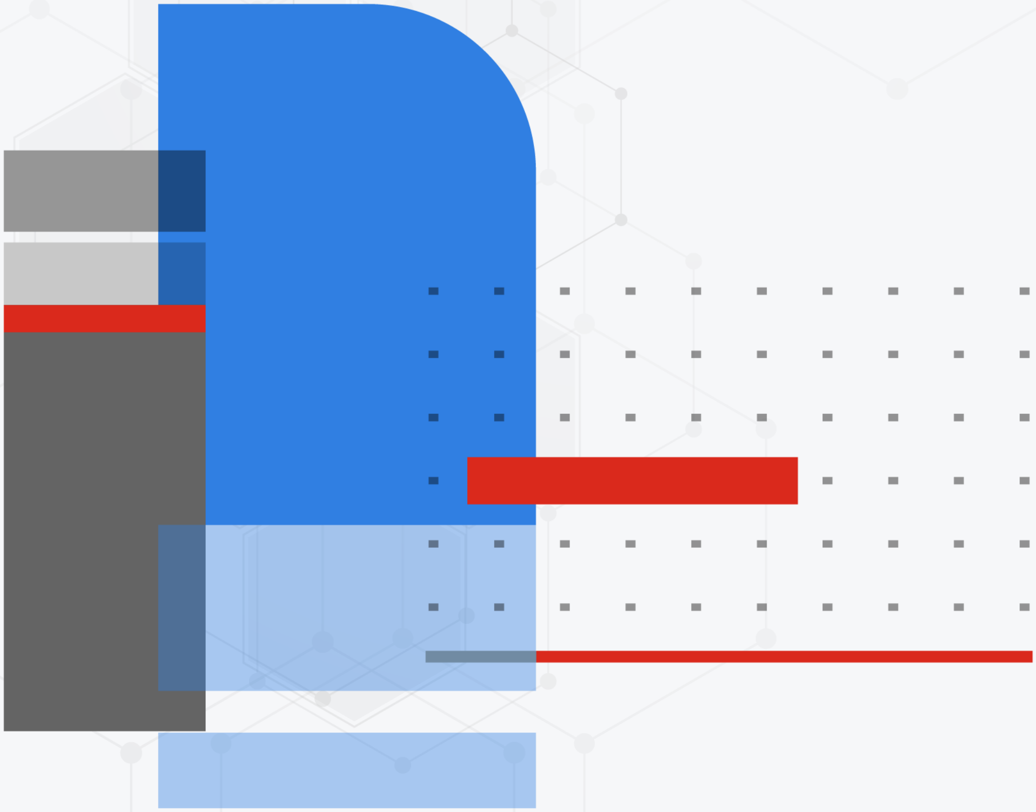
FORTINET

User Guide

FortiSIEM Version 7.0.2



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE

https://training.fortinet.com

FORTIGUARD CENTER

https://fortiguard.com/

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

FORTINET®
04/17/2024
FortiSIEM - User's Guide

TABLE OF CONTENTS

Overview

FortiSIEM is an advanced Security Information and Event Management (SIEM) solution that combines advanced log and traffic analysis with performance/availability monitoring, change analysis, and accurate knowledge of the infrastructure to provide accurate threat detection, remediation, incident response and compliance reporting.

FortiSIEM can be deployed as a hardware appliance, a virtual appliance, or as a cluster of virtual appliances to scale-out to large infrastructure deployments.

Scale-Out Architecture

FortiSIEM scales seamlessly from small enterprises to large and geographically distributed enterprises and service providers.

For smaller deployments, FortiSIEM can be deployed as a single all-in-one hardware or virtual appliance that contains full functionality of the product. The virtual appliance can run on most common hypervisors including VMware ESX, Microsoft Hyper-V, and RedHat KVM, and can be deployed on premise or in Amazon AWS Cloud. For larger environments needing greater event handling throughput and storage, FortiSIEM can be deployed in cluster mode. There are three types of FortiSIEM nodes – Collector, Worker and Supervisor.

Collectors are used to scale data collection from various geo-separated network environments potentially behind a firewall. Collectors communicate to the devices, collect the data, parse the data, and send it to the Worker nodes over a compressed secure HTTP(S) channel. Supervisor and Worker nodes reside inside the data center and perform data analysis functions using distributed co-operative algorithms. For scalable event storage, FortiSIEM provides two solutions – FortiSIEM NoSQL event database with data residing on a NFS Server and Elasticsearch.

As compute or storage needs grow, you can add Collector nodes, Worker nodes, disks on the NFS server and Elasticsearch Data Nodes.

FortiSIEM also provides Windows Agents that enable log collection from a large number of Windows Servers. Windows Agents can be configured to send events to Collectors in a highly available load balanced manner.

Multi-tenancy

FortiSIEM allows you to manage multiple groups of devices and users (Organizations) within a single FortiSIEM installation. Devices and IP addresses can overlap between Organizations. FortiSIEM provides strict logical separation between organizations at the application layer. Users of one Organization cannot see another Organization’s data including devices, users and logs. Users belonging to a Manage Service Provider Organization can see all Organizations.

Infrastructure Discovery and Automated CMDB

For complete situational awareness, the user needs to know the network and server infrastructure in depth. FortiSIEM’s inbuilt discovery engine can explore an IT infrastructure (on premise and cloud, physical and virtual), discover and categorize network devices, servers, users and applications in depth. A wide range of information is discovered including hardware information, serial numbers and licenses, installed software, running applications and services, and device configurations. Some special topological relationships can be discovered, for example - WLAN Access Points to WLAN Controllers, and VMware guests to physical hosts. This rich information populates an integrated configuration management database (CMDB), which is kept up to date through scheduled rediscoveries.

A novel aspect of FortiSIEM discovery is that the system automatically discovers what can be monitored and which log can be pulled using the provided credentials. This approach reduces human error, since FortiSIEM autonomously learns the true network configuration state.

High Performance Log Collection and Flexible Parsing

FortiSIEM has a flexible distributed log collection and parsing architecture. For logs pushed to FortiSIEM (such as Syslog), devices can load balance the logs across various Workers or Collectors. For logs pulled by FortiSIEM (such as Windows WMI or Cloud services via REST API), the pulling functionality is automatically load balanced across Workers and Collectors. Logs are immediately parsed at the point at which they are received. This distributed processing speeds up log collection and analysis.

FortiSIEM has a patented XML based log parsing language that is both flexible and computationally efficient. Flexibility comes from the fact that users can easily write their own parsers (XML files) or edit system provided ones using the FortiSIEM GUI. The parser XML files are compiled at run-time and executed as an efficient code. This makes log parsing very efficient, almost as efficient as writing code in native programming languages.

Performance and Availability Monitoring

Zero-day malware can create performance issues on a server, for example, malware can consume large memory, or ransomware scanning and encrypting files can slow the performance of other applications. By shutting down certain services and creating excessive network traffic, malware can cause availability issues. To properly detect and remediate security issues, an investigator needs to know the performance and availability trends of critical infrastructure services. Powered by its discovery capabilities, FortiSIEM can seamlessly collect a rich variety of performance and availability metrics to help the investigator hunt for threats. FortiSIEM can also alert users when it receives metrics outside a normal profile, correlating such violations with security issues to create high fidelity alerts.

Network Configuration and File Integrity Monitoring

Unauthorized or inadvertent changes to key system configuration files (such as httpd.conf) or router/firewall configuration can lead to security issues. Malware can modify key system files. Bad actors (for example, insider threats) can steal forbidden files. It is important to maintain control of key files and directories.

FortiSIEM provides mechanisms for tracking and detecting key file changes. It can monitor start-up and running configuration of network devices via SSH. It can monitor configuration files on servers. FortiSIEM agents can efficiently monitor large server infrastructures. An alert is created when a file changes from one version to another or deviates from a blessed hardened configuration.

Custom Device and Application Support

While FortiSIEM provides turnkey support for a large number of devices and applications, users can build their own full-fledged support from the GUI. System log parsers, performance monitors, and configuration change detectors can be modified. New device and application types, performance monitors, and configurations change detectors can be defined, and new log parsers can be integrated to work with FortiSIEM.

User Identity and Location Tracking

By combining DHCP logs, VPN logs, WLAN logs, and Domain Controller logon events, FortiSIEM is able to maintain an audit trail for IP address to user and geo-location mappings over time. While IP address to User mapping is important for look-up purposes by its own right, this feature enables FortiSIEM to detect stolen credentials as they tend to get used from distant locations over a short period of time.

External Threat Intelligence Integration

External websites can provide cyber threat information in terms of:

- Malware IP
- Malware Domain
- Malware hash
- Malware URL
- Anonymity Networks

FortiSIEM has a flexible framework to connect to a wide variety of threat sources (both free and paid), efficiently downloading this information and find matches in real-time in the environment it is running. Some threat sources can have a large number (millions) of bad IPs and URLs. FortiSIEM’s distributed search and rule engines find matches with such large sets of data at a very high event rate.

Distributed Event Correlation and Threat Detection - the Rule Engine

FortiSIEM has a distributed event correlation engine that can detect complex threats in near real-time. Threats are users or machine behavioral anomalies and can be specified in terms of event patterns sequenced over time. A threat can be alternatively looked at as a SQL query evaluated in a streaming mode. FortiSIEM has an inbuilt profiling engine that can handle threats defined using statistical thresholds, using mean and standard deviation.

What makes the FortiSIEM rule engine powerful is (a) the ability to include any data in a rule, for example: performance and change metrics along with security logs, (b) distributed in-memory computation (patent-pending) involving Supervisor and Worker nodes for near real-time performance with high event rates, (c) the ability for a rule to generate a dynamic watch list which can be used recursively in a new rule to create a nested rule hierarchy, (d) use of CMDB Objects in Rule definition, and (e) unified XML based language for rules and reports which makes it easy to convert a report into a rule and vice-versa.

Several machine learning based UEBA models are part of the FortiSIEM inbuilt rule library – (a) detection of simultaneous logins from two different countries, (b) detection of simultaneous logins from two improbable geo-locations,

(c) login behavior anomaly – logins to servers at times that one does not typically log on, etc., (d) detection of traffic to dynamically generated domains.

FortiSIEM has a large number of in-built behavioral anomaly rules that work out of the box, but can also be adapted by the user for their own environment. A framework is provided where the user can write new rules via the GUI, test them with real events, and then deploy in the system.

Device and User Risk Scoring

By combining with asset criticality, user role and importance, incident severity, frequency of occurrence and vulnerabilities found, FortiSIEM assigns a risk score to users and machines. This score is displayed in a dashboard with drill-down capabilities to identify the underlying factors.

Incident Response and Mitigation

FortiSIEM provides a number of mitigation scripts that can run an action when an incident happens. The scripts can be invoked automatically when an incident happens or can be invoked on-demand. Some examples include blocking an IP or a MAC, deactivating a user from active directory, removing an infected file, putting a user into a watch list, restarting a process or rebooting a server, and so on. You can also write your own mitigation scripts and deploy on a running system.

Search, Threat Hunting, Compliance Reports and Dashboards

FortiSIEM provides a flexible and unified search framework. The user can search data based on keywords or in a structured way using FortiSIEM parsed attributes. In real-time mode, the matched data streaming in from devices is displayed. In Historical mode, events in the event database are searched. Supervisor and Worker nodes perform search in a distributed manner.

A large number of inbuilt reports (search templates) are provided, based on the device type, and functionality, such as availability, performance, change and security.

Two novel aspects of FortiSIEM search are event unification and drill-down or threat hunting capabilities. With event unification, all data is analyzed and presented the same way, whether it is presentation aspects (real-time search, reports, rules) or context (performance and availability metrics, change events or security logs). Using drill-down, you can start from a specific context, such as Top Authentication Failed Users, and select attributes to further analyze data and iteratively, get to the root cause of a problem. As an example, the investigation of 'Top Authentication Failed users' could be followed by picking a specific user from the list and selecting Destination IP, and Ports to see which machines the user communicated with, followed by selecting the raw logs for real evidence.

FortiSIEM contains a wide selection of compliance reports out of the box – PCI, COBIT, SOX, ISO, ISO 27001, HIPAA, GLBA, FISMA, NERC, GPG13, SANS Critical Control, NIST800-53, and NIST800-171.

FortiSIEM provides a wide variety of visual dashboards for the data it collects and for incidents that have triggered - Summary dashboards, Widget dashboards, Business Service dashboard, Incident dashboard, and Identity and Location dashboard.

Internal Ticketing System and Two-way Third-party Ticketing Integration

FortiSIEM has a built-in ticketing system for managing incidents via tickets. It supports the full ticket life cycle of opening, escalating, closing, reopening and creating cases with attachments for evidence.

FortiSIEM can also integrate with third-party ticketing systems. When an incident occurs in FortiSIEM, a ticket can be created in the external ticketing system and linked to an existing device or a new device can be created in the external system. You can customize various FortiSIEM incident fields to the external ticketing system field. When the ticket is closed in the external ticketing system, the ticket is closed in FortiSIEM.

Several third-party external ticketing systems are supported out of the box, for example, ServiceNow, Salesforce, ConnectWise and Remedy. An API is provided so that other integrations can be built.

Business Service Analytics

Business Service enables you to prioritize incidents and view performance/availability metrics from a business service perspective. A Business Service is defined within FortiSIEM as a smart container of relevant devices and applications serving a common business purpose. Once defined, all monitoring and analysis are presented from a business service perspective.

FortiSIEM enables you to easily define and maintain a Business Service. Since FortiSIEM automatically discovers the applications running on the servers as well as the network connectivity and the traffic flow, you can easily choose the applications and respective servers and be intelligently guided to choose the rest of components of the Business Service.

FortiSIEM Releases

The following sections provide release specific information about new features, enhancements, and resolved issues:

What's New in 7.0.2

- Key Enhancement
- Bug Fixes and Minor Enhancements
- Important Notes

Key Enhancement

Storage Space Reduction for ClickHouse Based Deployments

This release reduces the storage space for storing events in ClickHouse based deployments. This is achieved in two ways:

- By removing a derived event attribute that included the list of all parsed attributes. This attribute was added to quickly show all parsed attributes in raw message queries, but required additional storage. Now GUI performs optimized adhoc queries to get this information from ClickHouse database.
- By changing the compression algorithm to Zstandard (ZSTD) level 6. Note that only new installations from 7.0.2 onwards can use the ZSTD level 6 compression. Existing customers will use the current LZ4 algorithm. See the ClickHouse Sizing Guide for new storage requirements.

Bug Fixes and Minor Enhancements

This release includes the following bug fixes:

- Several security related code improvements in Linux Agent area
- Fix for Bug 946202: FortiSIEM Supervisor and Worker makes excessive DNS lookups due to missing entries in `/etc/hosts` file. This bug was introduced in 7.0.0.
- Fix for Bug 934773: The runtime directory of `phAnomaly` process under `/tmp` would be deleted after certain time, resulting in `phAnomaly` process to not run after 10 days. This bug was introduced in 7.0.0.
- phAnomaly process to not run after 10 days. This bug was introduced in 7.0.0.
- Fix for Bug 921597: Reboot may be slow after upgrading to 7.0.0. This bug was introduced in 7.0.0.

- Fix for Bug 948701: Machine Learning Clustering job failed to handle inference output without `hostName` id attribute. This bug was introduced in 7.0.0.

This release includes Rocky Linux OS 8.8 updates until September 3, 2023. The list of updates can be found at https://errata.rockylinux.org/.

FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include fixes until September 3, 2023. Therefore, FortiSIEM customers in versions 6.4.1 and above, can upgrade only their Rocky Linux versions by following the procedures described in the FortiSIEM OS Update Procedure Guide.

Important Notes

1. For native Elasticsearch and Elastic Cloud deployments, FortiSIEM 7.0.0 or higher supports Elasticsearch versions 7.17 and 8.5. If you are running a lower Elasticsearch version and upgrade to FortiSIEM 7.0.0 or higher, then Elasticsearch Queries will not work. Follow these steps to properly upgrade your infrastructure.
    a. Upgrade FortiSIEM to 7.0.0 or higher.
    b. Upgrade Elasticsearch version to 7.17 or 8.5.
    c. In **Admin > Setup > Storage > Online**, redo **Test** and **Deploy**.
2. AWS Elasticsearch is not supported in FortiSIEM 7.0.0 or higher, since they only support Elasticsearch 7.10, which is lower than the required 7.17.
3. AWS Opensearch is not supported in FortiSIEM 7.0.0 or higher.
4. To support new analytical functions in Elasticsearch, the Painless scripting language is used. See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/modules-scripting-painless.html for reference. If you are running Elasticsearch, then add the following line to the `Elasticsearch.yml` file in every Elasticsearch node and restart the cluster for the changes to take effect. Otherwise, queries will fail.

    ```
    script.painless.regex.enabled: true
    ```

5. 5.x Collector will not work with FortiSIEM 6.7.2 or later. This step is taken for improved security. Follow these steps to make the 5.x Collectors operational after upgrade.
    a. Upgrade the Supervisor to the latest version: 7.0.0 or higher.
    b. Copy phProvisionCollector.collector from the Supervisor to all 5.x Collectors.
        i. Login to Supervisor.
        ii. Run the following command.

        ```
        scp /opt/phoenix/phscripts/bin/phProvisionCollector.collector
        root@<Collector_IP>:/opt/phoenix/bin/phProvisionCollector
        ```

    c. Update 5.x Collector password.
        i. SSH to the Collector.
        ii. Run the following command.

        ```
        phProvisionCollector --update <Organization-user-name> <Organization-
        user-password> <Supervisor-IP> <Organization-name> <Collector-name>
        ```

iii. Make sure the Collector ID and password are present in the file `/etc/httpd/accounts/passwds` on Supervisors and Workers.

d. Reboot the Collector.

6. FortiSIEM 7.0.0, 7.0.1 and 7.0.2 cannot be installed with FIPS option.
7. For Windows and Linux Agents monitoring host performance, **CMDB > Monitor Status** tab is not populated in GUI.
8. FortiSIEM 7.0.0 and later API documentation is transitioning to https://fndn.fortinet.net/index.php?/fortiapi/2627-fortisiem/. Fortinet recommends checking this link first for the latest API updates.

What's New in 7.0.1

- Important Notes
- Key Enhancements
- Bug Fixes

Important Notes

1. For native Elasticsearch and Elastic Cloud deployments, FortiSIEM 7.0.0 supports Elasticsearch versions 7.17 and 8.5. If you are running a lower Elasticsearch version and upgrade to FortiSIEM 7.0.0, then Elasticsearch Queries will not work. Follow these steps to properly upgrade your infrastructure.
    a. Upgrade FortiSIEM to 7.0.0.
    b. Upgrade Elasticsearch version to 7.17 or 8.5.
    c. In **Admin > Setup > Storage > Online**, redo **Test** and **Deploy**.
2. AWS Elasticsearch is not supported since they only support Elasticsearch 7.10, which is lower than the required 7.17.
3. AWS Opensearch is not supported.
4. To support new analytical functions in Elasticsearch, the Painless scripting language is used. See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/modules-scripting-painless.html for reference. If you are running Elasticsearch, then add the following line to the `Elasticsearch.yml` file in every Elasticsearch node and restart the cluster for the changes to take effect. Otherwise, queries will fail.

    ```
    script.painless.regex.enabled: true
    ```
5. 5.x Collector will not work with FortiSIEM 6.7.2 or later. This step is taken for improved security. Follow these steps to make the 5.x Collectors operational after upgrade.
    a. Upgrade the Supervisor to the latest version: 7.0.0 or higher.
    b. Copy phProvisionCollector.collector from the Supervisor to all 5.x Collectors.
        i. Login to Supervisor.
        ii. Run the following command.

```
scp /opt/phoenix/phscripts/bin/phProvisionCollector.collector
root@<Collector_IP>:/opt/phoenix/bin/phProvisionCollector
```

c. Update 5.x Collector password.

i. SSH to the Collector.

ii. Run the following command.

```
phProvisionCollector --update <Organization-user-name> <Organization-
user-password> <Supervisor-IP> <Organization-name> <Collector-name>
```

iii. Make sure the Collector ID and password are present in the file `/etc/httpd/accounts/passwds` on Supervisors and Workers.

d. Reboot the Collector.

6. This release cannot be installed with FIPS option.
7. For Windows and Linux Agents monitoring host performance, **CMDB > Monitor Status** tab is not populated in GUI.
8. FortiSIEM 7.0.0 and later API documentation is transitioning to https://fndn.fortinet.net/index.php?/fortiapi/2627-fortisiem/. Fortinet recommends checking this link first for the latest API updates.

Key Enhancements

- Rocky Linux 8.8
- Optimized Incident Trigger Event Lookup

Rocky Linux 8.8

This release updates Rocky Linux OS to 8.8 and includes published Rocky Linux OS updates until July 14, 2023. The list of updates can be found at https://errata.rockylinux.org/.

FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include fixes until July 14, 2023. Therefore, FortiSIEM customers in versions 6.4.1 and above, can upgrade only their Rocky Linux versions by following the procedures described in https://docs.fortinet.com/document/fortisiem/7.0.0/fortisiem-os-update-procedure/574280/fortisiem-os-update-procedure.

Optimized Incident Trigger Event Lookup

Incident Trigger Event lookup in GUI is optimized for long running Incidents. In previous releases, the trigger events are searched over the First Seen Time and Last Seen Time window, which can be very large, if the incident is constantly triggering and is not resolved. In such cases, GUI may fail to display trigger events. In the new design, for an Incident, the latest 100 trigger events are shown over a maximum 30-day period. For ClickHouse, in addition, the eventType field is stored for every trigger event and used in the queries. Since eventType is a ClickHouse Primary Index, queries are faster (https://help.fortinet.com/fsiem/7-0-0/Online-Help/HTML5_Help/appendix-clickhouse-index-design.htm), but the additional speedup will impact newer incidents. Consider these examples:

- If 100 trigger events occur in last 1 day, then only these trigger events are shown.
- If 50 trigger events occur in each of last 2 days, then only these trigger events over last 2 days are shown.

- If 1 trigger event occur on each of last 100 days, then 30 trigger events are shown.

Bug Fixes

This release contains the following fixes and enhancements.

Bug Id	Severity	Module	Description
929885	Major	App Server	Test Connectivity & Discovery may get stuck with Database update 0% when a few discoveries are running.
922978	Major	Report	`ReportWorker` on EventDB environments may be slow in processing events and sending summaries to `ReportMaster`.
914571	Minor	Agent Manager	`phAgentManager` process memory grows, while receiving Kafka events, caused by a memory leak in the 3rd party librdkafka module. In this release, librdkafka module has been upgraded to the latest version. Our tests show that a FortiSIEM Collector with 8 vCPU and 24GB memory, can collect up to 4K EPS from Kafka.
923024	Minor	App Server	In GUI, switching user from Super Global to a specific Organization does not work unless the user belongs to all Organizations.
921351	Minor	App Server	Multiple Incident REST API issues are fixed: • JSON APIs return error responses in JSON format, instead of XML format • POST API filtering allow these event attributes: `eventSeverity`, `eventSeverityCat`, `phIncidentCategory`, `incidentStatus`, `customer`, `phCustId`, `incidentReso`, `incidentId` • Two parameters are required for Trigger event queries - `timeFrom` and `timeTo`, to provide response to trigger event queries in reasonable time. These two parameters should not be more than 1 day apart. For details, see FortiSIEM REST API.
918854	Minor	App Server	`AppServer` incorrectly invalidates older log integrity XML data, resulting in these files not written to database.
917625	Minor	App Server	During CMDB Merge for Windows Agents, Windows GUID is considered for merging. This causes two different Windows Servers with different names but same IP or GUID to be merged into the same entry in CMDB.
921662	Minor	Data Purger	Excessive logging by `phDataPurger` when it hits a Value Group lookup error, fills up `/opt` disk.
921628	Minor	Elasticsearch	In Elasticsearch, the nesting of SUM and IF functions doesn't

Bug Id	Severity	Module	Description
			work when IF operator is (>,<,>= or <=). An example is SUM(IF((Event Severity >= 4),1,0)).
921451	Minor	Event Pulling Agents	Azure for US Govt does not work - (fails with correct credential).
928179	Minor	GUI	Machine Learning Report: Windows Process Interaction Ratio does not display correct data.
927794	Minor	GUI	If a nested function has aggregation but outer function is non-aggregate (e.g. LOG(SUM(X))), then whole function is treated as non-aggregate and included in GroupBY attribute list. This results in an invalid Query.
924367	Minor	GUI	New Entity Risk View in 7.0 shows only 10 Incidents in the time window. Now it shows all Incidents.
919768	Minor	GUI	Two issues are resolved for assigning Custom Design Templates assigned to a Report Folder under **Resources > Reports**: (a) If you are migrating from pre-7.0.0 release and you have Custom Design Templates assigned to a Report Folder under **Resources > Reports**, then Report Design Template migration process will not complete, (b) Cannot assign a custom Report Design Template to a Report Folder.
918931	Minor	GUI	Cannot execute FortiSOAR Playbook and run FortiSOAR Connector from Analytics page.
923667	Minor	Machine Learning	The Machine Learning algorithm fails to predict Incident Resolution for some new Incidents.
921060	Minor	Machine Learning	The Machine Learning algorithm to predict Incident Resolution does not work in Service Provider installations.
929009	Minor	Parser	The EPS in event `PH_SYSTEM_EPS_GLOBAL` is calculated incorrectly.
928414	Minor	Parser	`phParser` CPU may be high if event size is very large. This was noticed when receiving larger than 800KB events.
918150	Minor	System	Upgrade can fail when Rocky Linux OS repo DNS Name resolution fails.
918654	Enhancement	Parser	Make `phParser` EoL character recognition configurable for TLS syslog. The following `phoenix_config.txt` entry is added: `tcp_syslog_delimiter=0x0a # or 0x00,0x0a`
743793	Enhancement	Parser	Enable SASL_SSL (authentication plus encryption) for Kafka producer and consumer. In this release, there is no GUI support for this. Customer needs to choose SASL_PLAINTEXT on GUI and configure this in `phoenix_config.txt`.

Bug Id	Severity	Module	Description

			`sasl_ssl_ca_cert=/etc/pki/kafka/ca-cert`
			`sasl_ssl_cert_file=/etc/pki/kafka/client_client.pem`
			`sasl_ssl_key_file=/etc/pki/kafka/client_client.key`
			`sasl_ssl_password=`
			`sasl_ssl_verify=true`
			See the **Appendix > Configuration Notes > Editing phoenix_config.txt File** for guidance on changing the file. Specifically, on the Collector, you need to make the same change in 2 places:
			• Change the `/opt/config/phoenix_config.txt` file on the Collector and restart the Collector.
			• Make the same change on `/opt/phoenix/config/collector_config_template.txt`. This ensures that new Collectors registering will get the new parameters and the changes are preserved across upgrades.

914960	Enhancement	Systems	Reduce the number of CMDB backups to 1 per day to conserve space and facilitate upgrade.

What's New in 7.0.0

- Important Notes
- New Features
- Key Enhancements
- Bug Fixes and Enhancements
- Known Issues

Important Notes

1. For native Elasticsearch and Elastic Cloud deployments, FortiSIEM 7.0.0 supports Elasticsearch versions 7.17 and 8.5. If you are running a lower Elasticsearch version and upgrade to FortiSIEM 7.0.0, then Elasticsearch Queries will not work. Follow these steps to properly upgrade your infrastructure.
    a. Upgrade FortiSIEM to 7.0.0.
    b. Upgrade Elasticsearch version to 7.17 or 8.5.
    c. In **Admin > Setup > Storage > Online**, redo **Test** and **Deploy**.

2. AWS Elasticsearch is not supported since they only support Elasticsearch 7.10, which is lower than the required 7.17.
3. AWS Opensearch is not supported.
4. To support new analytical functions in Elasticsearch, the Painless scripting language is used. See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/modules-scripting-painless.html for reference. If you are running Elasticsearch, then add the following line to the `Elasticsearch.yml` file in every Elasticsearch node and restart the cluster for the changes to take effect. Otherwise, queries will fail.

   ```
   script.painless.regex.enabled: true
   ```

5. 5.x Collector will not work with FortiSIEM 6.7.2 or later. This step is taken for improved security. Follow these steps to make the 5.x Collectors operational after upgrade.
   a. Upgrade the Supervisor to the latest version: 7.0.0 or higher.
   b. Copy `phProvisionCollector.collector` from the Supervisor to all 5.x Collectors.
      i. Login to Supervisor.
      ii. Run the following command.

      ```
      scp /opt/phoenix/phscripts/bin/phProvisionCollector.collector
      root@<Collector_IP>:/opt/phoenix/bin/phProvisionCollector
      ```

   c. Update 5.x Collector password.
      i. SSH to the Collector.
      ii. Run the following command.

      ```
      phProvisionCollector --update <Organization-user-name> <Organization-
      user-password> <Supervisor-IP> <Organization-name> <Collector-name>
      ```

      iii. Make sure the Collector ID and password are present in the file `/etc/httpd/accounts/passwds` on Supervisors and Workers.
   d. Reboot the Collector.
6. In pre-7.0.0 releases, you can define a Report Design Template for an individual Report, a Report Bundle or a Report Folder under **Resources > Reports**. In this release, assigning a Report Design Template to a Report and a Report Bundle works correctly, but *assigning to a Report Folder does not work*. This means:
   - In 7.0.0, you cannot assign a custom Report Design Template to a Report Folder.
   - If you are migrating from an earlier release and you have Custom Design Templates assigned to a Report Folder under **Resources > Reports**, then the pre-7.0.0 -> 7.0.0 Template migration process will not complete. Note that Template migration happens under the hood, when user logs on to the system for the first time after upgrading to 7.0.0. In this case, you will see the following error message, "Another User is updating all Report Templates on this machine. Please try again later.".

   The following workaround is suggested:

   A. Before upgrading, check if you have any Custom Design Templates assigned to a Report Folder. This can be checked in one of two ways:

- Login to GUI, go to **Resources > Reports**, and visit each folder and see if there is a Custom Design Template defined.
- Alternatively, you can download a zip file with the bash script from here, SSH to the Supervisor as root, copy the script to `/tmp` and run the command:

  ```
  /tmp/GetCustomFolderReportDesignTemplate
  ```

  If you get "Permission denied" error while running the script, then run the following command as root.

  ```
  chmod 755 /tmp/GetCustomFolderReportDesignTemplate
  ```

- If there no Custom Design Template defined for a Report folder, then the script output will be "No Custom Folder Report Design Template Found. You may proceed to regular upgrade."
- If there are Custom Design Templates defined for a Report folder, then the script output will be something like:

  ```
  Found 2 Custom Folder Report Design Templates:

    testFolder1

    testFolder2
  ```

B. Before upgrading, if there are Custom Design Templates defined for a Report folder, then you need to delete them. This can be done in one of two ways:

- Login to GUI, Go to **Resources > Reports**, select each folder with Custom Folder Report Design Template, select **More > Report Design** and click "Revert to Default".
- Alternatively, you can download a zip file with the bash script from here, SSH to the Supervisor as root, copy the script to `/tmp` and run the command:

  ```
  /tmp/RemoveAllCustomFolderReportDesignTemplate
  ```

  The script output will be something like:

  ```
  Deleted 2 Custom Folder Report Design Templates:

    testFolder1

    testFolder2
  ```

You may proceed to regular upgrade. If you have already upgraded, then reload the GUI.

C. If you have already upgraded without doing the procedures 1 and 2 above, then there are two cases:

- If you do not have any Custom Design Templates assigned to a Report Folder, then the system will work normally.
- If you do have Custom Design Templates assigned to one or more Report Folders, then you will see the error when you visit Reports page: "Another User is updating all Report Templates on this machine. Please try again later." In this case, you can download a zip file with the bash script from here, SSH to the Supervisor as root, copy the script to `/tmp` and run the following command:

  ```
   /tmp/RemoveAllCustomFolderReportDesignTemplate
  ```

  The script output will be:

```
Deleted 2 Custom Folder Report Design Templates:
  testFolder1
  testFolder2
```

You may proceed to regular upgrade. If you have already upgraded, then reload the GUI.

After running the script, simply reload the GUI.

7. This release cannot be installed with FIPS option.
8. For Enterprise deployments, while creating a custom Report Bundle, you will see an Error: *NumberFormat Exception: For input string: "undefined"*. You can close this error and proceed to create the report bundle. The error has no impact.
9. The Report Design Templates from pre-7.0.0 releases will be migrated to the new format as required by the new Visual Report Design Editor in 7.0. If your pre-7.0.0 Report Design Template contained a PDF attachment in the middle of the template, then after migration, the PDF attachment will be moved to the end of the PDF document.
10. For Windows and Linux Agents monitoring host performance, **CMDB > Monitor Status** tab is not populated in GUI.
11. FortiSIEM 7.0.0 and later API documentation is transitioning to https://fndn.fortinet.net/index.php?/fortiapi/2627-fortisiem/. Fortinet recommends checking this link first for the latest API updates.

New Features

This release contains the following new features:

- Visual Report Designer
- New Query Functions
- Machine Learning Workbench
- Incident Investigation Workspace
- Built-in Machine Learning Models
- ClickHouse Event Integrity
- Fortinet Security Fabric Discovery
- FortiEMS Discovery
- FortiEMS Endpoint Tagging
- Windows Agent 5.0.0
- Linux Agent 7.0.0

Visual Report Designer

This release provides a report design editor that shows how the report will look in the PDF document. This is often referred to as a WYSIWYG (What you see is what you get) editor. All the features in the current report designer are available with the following exceptions:

- Sub-section from earlier versions is not supported in 7.0.0
- An image/text can be placed side-by-side with another item (image/chart/text) in 7.0.0

For details on creating and editing reports using the Visual Report Designer, see Designing a Report Template.

When a user logs in for the first time to an upgraded FortiSIEM 7.0.0, existing pre-7.0.0 report and report bundle templates will be automatically converted to the new format. The new format will be identical to the old format except in one case: if a user chose 2 charts for the same report in the pre-7.0.0 template, then the charts will be placed next to each other with a shared legend, in the new 7.0.0 format. If there are 4 or more charts for the same report in the pre-7.0.0 template, then the new 7.0.0 format will display multiple rows of charts, with 2 charts in one row, and a common legend at the end.

New Query Functions

The following enhancements are provided for querying events:

1. **Aggregation Functions**: COUNT, MEDIAN, MODE, PCTILE, STDDEV, and VARIANCE. These compute specific functions in group-by queries and provide additional insights compared to existing aggregation functions: SUM, AVG, MIN, MAX.
2. **Time Window Functions**: SMA, EMA. These compute simple and exponential moving averages over a time window.
3. **String Manipulation Functions**: LEN, TO_UPPER, TO_LOWER, REPLACE, TRIM, LTRIM, RTRIM, SUB_STR, URL_DECODE. These do various string manipulations and may be needed to regularize string valued event attributes.
4. **Conversion Functions**: TO_INTEGER, TO_DOUBLE, TO_STRING, LOG
5. **Extraction Function**: EXTRACT. This can extract a value from an event attribute, in case the parser missed this attribute in historical data.
6. **Evaluation Function**: IF. This function can be used to set a new variable based on whether a logical condition based on event attributes is true or false.
7. Allow functions to be nested up to 5 levels, e.g. COUNT DISTINCT (TO_UPPER(user)))

These functions are only available for ClickHouse and Elasticsearch Queries. See the full description link below for limitations of nesting operations.There is no support for EventDB queries and rules.

For full description of the functions and examples, see Functions in Analytics.

Machine Learning Workbench

This release provides a workflow for users to create machine learning tasks based on the events stored in FortiSIEM. You can run a report to create a dataset for a machine learning task, and then train FortiSIEM to create a machine learning model. Then you schedule an inference job to run periodically, which can detect deviations from the model and create incidents, or send emails. The model can be re-trained periodically or on demand. 4 machine learning tasks are supported: Regression, Classification, Anomaly Detection and Forecasting. Classification will only work if there is a labeled field in the event. For Forecasting jobs, email is sent instead of creating incidents.

Four machine learning jobs can be run locally on the Supervisor/Worker cluster, or on AWS. Each platform supports different machine learning tasks and algorithms. When run locally, machine learning jobs are distributed across the Supervisor/Worker cluster - this means that any of Supervisor or Worker nodes can do the training and inference jobs. In each mode, the user can choose a specific machine learning algorithm or run in Auto mode, where FortiSIEM tries to choose the best algorithm with the optimal parameters. Auto mode takes longer to train as various algorithms and parameter sets are attempted during the optimization process.

For details on how to create a machine learning job, see Machine Learning.

Incident Investigation Workspace

Currently, users investigate an Incident within the List View. It is not easy in this view to correlate this Incident with other related Incidents and the entities involved. In this release, a separate Incident Investigation workspace is provided in **Analytics > Investigation**. Starting with a root Incident, the user can build a link graph relating that Incident to involved entities (IP, Host, user, process, file) and then recursively to other incidents and related entities. The user can view the timeline of these Incidents and play them in a time ordered fashion to visualize how an attack kill chain is developing. Context is provided for every entity based on information in CMDB, external lookups and events in the FortiSIEM Event Database. It is also possible to run reports, run FortiSOAR playbooks and Connectors to gain further insight into an investigation. Finally, the user can also take a remediation action, create a case locally or in an external ticketing system and clear the Incident. In summary, this Workspace enables the user to stay on this page and fully investigate an Incident and take it to closure.

For details on working with Incident Investigation Workspace, see Investigating Incidents.

Built-in Machine Learning Models

The following specialized Machine Learning models are provided:

1. **Login Anomaly Detection via Bipartite Graph Edge Anomaly Algorithm**

   This release includes a proprietary Machine Learning algorithm that detects login anomalies by learning the user-to-workstation login patterns and forming dynamic peer user groups with similar login patterns. Users and Workstations are represented using a Bipartite graph. In a Bipartite graph, the sets of nodes can be split into two disjoint sets, in such a way that there are no edges between the nodes within the same set. In this example, Users and Workstations form a Bipartite graph, the edge between a User and a Workstation represents a login, and the edge weight represents the number of logins during a time interval.

   This algorithm is part of the FortiSIEM Machine Learning Workbench, introduced in this release. A system defined Machine Learning job including a login report and the Bipartite Graph Edge Anomaly algorithm, is included in this release. The user needs to train the algorithm using the login data from their environment and then schedule the job to run at periodic intervals to detect anomalies. An Incident triggers when an anomaly is detected, along with a visualization of the anomaly.

   For details on the Bipartite Graph Edge Anomaly algorithm, see Anomaly Detection Algorithms for Local Mode.

   For details on how to train and schedule the Login anomaly detection job, see Running Anomaly Detection Local Mode.

2. **Incident Resolution Recommendation**

   FortiSIEM provides 2 attributes to record Incident status

   - **Incident Resolution**: None, True Positive, False Positive
   - **Incident Status**: Active, System Clear and Manually Cleared

   When an Incident triggers, **Incident Status** is Active and **Incident Resolution** is None. There are 3 ways an Incident can get resolved:

a. If the Incident turns out to be a false positive, then the user can set **Incident Resolution** to False Positive and **Incident Status** to Manually Cleared.

b. The Incident may clear itself because of a clearing condition in the rule. In that case, **Incident Resolution** is set to True Positive and **Incident Status** is set to System Cleared.

c. The Incident may be a real issue. In that case, after working through the Issue, the user can set **Incident Resolution** to True Positive and **Incident Status** to Manually Cleared.

In this release, FortiSIEM uses a Machine Learning Classification algorithm to learn the **Incident Resolution** set by the user for Incidents over the last 2 days, and recommends **Incident Resolution** for new Incidents as they happen. The algorithm runs daily at midnight (12AM) to cover Incidents over the last 2 days. Recommendation is done only for new incidents in real time:

- **Incident Resolution** is set to True Positive or False Positive.
- A new Incident attribute called **Confidence** (between 0 and 100) is set, with a higher confidence number implying high confidence on the result.
- **Incident Comment** is updated with the comment "Resolution set by Machine Learning".

Notes:

1. Only **Incident Resolution** is set and **Incident Status** is not modified.
2. This algorithm always runs in the background, and cannot be disabled. It uses a set of Incident attributes as features (including Event Receive Time, Event Type, Reporting Device, Source, Target, Category and MITRE Attack Technique) to make its recommendation.

ClickHouse Event Integrity

This release provides a mechanism to check if event data in ClickHouse has been altered after it is first written to database. This feature is resource intensive and turned off by default. When turned on, checksums are computed per shard and per partition from that day onwards and stored in PostgreSQL database. From **Admin > Settings > Database > Event Integrity**, the user can check the various checksums and ask FortiSIEM to validate them. If some changes were made to the event data, the on-demand checksum would not match the checksum stored in PostgreSQL database.

For details about configuring and validating ClickHouse Event Integrity, see here.

A tool is provided to calculate checksum for historical data. The tool will compute checksums and store them in PostgreSQL database.

Fortinet Security Fabric Discovery

In earlier releases, FortiSIEM can discover a FortiGate firewall via REST API. The attached FortiSwitches, FortiAPs along with the FortiGate firewall and its configuration are discovered. In this release, this discovery is enhanced to a Security Fabric Discovery, where the following *additional* items are also discovered:

- Security Risk Rating for the entire Fabric, if the discovered FortiGate firewall is a Fabric root firewall.
- FortiClient User Store for the discovered FortiGate firewall, which is the list of FortiClient devices passing through the firewall.
- Shallow discovery of other FortiGate firewalls in the Fabric. Shallow discovery includes basic information about the firewall and does not include detailed information such as FortiClient User Store, configuration, etc.

In this release, the recommended way to discover the full Security Fabric is to *individually discover each FortiGate firewall via REST API*. The information from various discoveries is merged and displayed in CMDB.

For details about Security Fabric Discovery, see Fortinet FortiGate Firewall in the External Systems Configuration Guide.

FortiEMS Discovery

In this release, FortiSIEM can discover FortiEMS Servers, managed FortiClient endpoint devices and detailed vulnerabilities for each managed FortiClient endpoint. The vulnerability information is normalized to similar information found by vulnerability scanners.

For details about FortiEMS Discovery, see FortiClient EMS in the External Systems Configuration Guide.

FortiEMS Endpoint Tagging

When an Incident triggers in FortiSIEM and it involves a FortiClient endpoint managed by FortiEMS, then user can associate a tag to the FortiClient endpoint in FortiEMS. A tag can be associated with a rule or manually defined. Tagging/Untagging is done via the remediation framework and can be done Adhoc or automated via the notification policy framework. For automation to work correctly, Fortinet Security fabric Discovery must be performed to associate FortiClient endpoint to the FortiEMS that it is registered to.

For details about FortiEMS endpoint tagging, see the Appendix - FortiEMS Endpoint Tagging.

Windows Agent 5.0.0

1. In previous releases, discovery and performance monitoring for Windows Servers had to be performed via WMI/OMI only, which needed an account to be created on the server for FortiSIEM use. In this release, Windows Agent can perform discovery and performance monitoring, this feature has parity with WMI/OMI based discovery and performance monitoring.

   For configuring discovery and performance monitoring for Windows Agent, see Configuring Windows Agent - Monitor settings.

2. DNS Analytical logs are now collected via real time Events Tracing for Windows (ETW) provider. This is done to overcome an issue with the old design where DNS analytical logs can stop when the log size is full, requiring the agent to restart in order to pick up new analytical logs.

Linux Agent 7.0.0

In previous releases, discovery and performance monitoring for Linux Servers had to be performed via SNMP and SSH only, which needed configuration changes on the server for FortiSIEM to setup SNMP and SSH connections. In this release, Linux Agent can perform discovery and performance monitoring, this feature has parity with SNMP and SSH based discovery and performance monitoring.

For configuring discovery and performance monitoring for Linux Agent, see Configuring Linux Agent - Monitor settings.

Key Enhancements

- Enhanced Entity Risk View
- External Threat Intelligence Integration Enhancements
- Elasticsearch 8.5.3 Support

- FortiGate VDOM Based Mitigation
- Rule Enhancements
- GUI Inactivity Timeout Enforcement
- Miscellaneous Enhancements

Enhanced Entity Risk View

The Risk Page is re-designed to provide more context for impacted entity (user or host) along with an activity timeline. See Risk View for more information on the Risk Page.

External Threat Intelligence Integration Enhancements

Two enhancements are included in this release.

1. A python-based framework that can be used to integrate new threat intelligence sources. For details see Python Threat Feed Framework in the Appendix.
2. GUI to show the health of threat intelligence integrations. Information includes Status, Feed, Last Updated, Pulling Schedule, Integration Type, Action and missed data polls because of errors. This enables users to make sure that integrations are running correctly.

Elasticsearch 8.5.3 Support

This release adds support for Elasticsearch 8.5.3.

FortiGate VDOM Based Mitigation

The FortiGate mitigation scripts now work if FortiGate has Virtual Domains (VDOMs) defined. User provides VDOM information and the script uses the VDOM during execution. See step 4 in Creating a Remediation Action for more information.

Rule Enhancements

1. Ability to compare event attributes within the same event, e.g. Source IP = Destination IP or Source IP != Destination IP.
2. Allow expression on the Right hand side of query/rule operator.

GUI Inactivity Timeout Enforcement

GUI inactivity time out is specified in **CMDB > User > Idle Timeout**. This is correctly enforced in this release. Unless the user is in **Dashboard**, the user is automatically logged out after the specified timeout if the user does not move the mouse or press a key.

Miscellaneous Enhancements

1. Create a CMDB entry for Cloud Service in CMDB and alert when logs are not being received. Host name is used as the IP Address in the logs. Merge discovered Cloud Services in the CMDB if the IP addresses of the service changes.
2. Show Collector ID in the Org Definition screen.
3. Expand AWS S3 Generic Log ingestion to handle multi-line JSON events (if extension is .json.gz or .json).

4. Support SMTP over SSL on ports 587 and 465.
5. Incident and Case PDF Export content improvements.
6. Added heads up display for **CMDB > Users** and **CMDB > Applications** to show the most prevalent users and applications.
7. Create a default **CMDB > Users** group called "FortiSIEM Users" containing administrative users defined locally in FortiSIEM.

Bug Fixes and Enhancements

Bug ID	Severity	Module	Description
885349	Major	App Server	FortiGuard Malware URL entries with special characters may result in App Server exceptions, which may fill up disk and the Supervisor may stop.
885206	Major	App Server	User may not be able to login to FortiSIEM Manager, due to excessive incident updates from instances.
880937	Major	App Server	When customer has user defined parsers, parser order may change unexpectedly after content update or regular upgrade.
891289	Minor	App Server	In notification email, Identity and Location lookup data is merged across organizations.
879916	Minor	App Server	Unable to view adhoc queries from the Query Status tab when the online storage is Elasticsearch.
877909	Minor	App Server	In **CMDB > Device**, items cannot be sorted globally.
869411	Minor	App Server	Schedule CMDB Report is blank, if Copy to remote host option is chosen and email setting is not configured.
865069	Minor	App Server	For a user defined via AD Group Role, the manually added Contact information will be deleted after user logs out.
859557	Minor	App Server	Unable to delete user defined Dashboard Slideshow in super/global and orgs.
851691	Minor	App Server	CMDB Report: Sometimes the returned number of rows may depend on the combination of display columns used.
843342	Minor	App Server	Incident Title and name are empty for auto clear incidents triggered by OSPF Neighbor Down Rule.
840694	Minor	App Server	AGENT method disappears from CMDB Discovery Method column when SNMP discovery is re-ran.
803284	Minor	App Server	Customer defined Default email sender in Notification Email gets overwritten after upgrade.
797247	Minor	App Server	A user that logs in via AD Group Role config cannot change the Date Format.

Bug ID	Severity	Module	Description
795247	Minor	App Server	A CMDB Device Groups can be deleted if there are devices belonging to this group.
749788	Minor	App Server	Delete/Edit CMDB AD User groups with 100k users fails with 'Undefined' error.
799463	Minor	Data Purger	Detect when Elasticsearch Alias is not created, and then try to create again.
817151	Minor	Disaster Recovery	When removing Disaster Recovery (DR) from cluster, cloud health page is not cleaned up; it contains the old cluster data.
876027	Minor	Discovery	FortiGate discovery API fails due to missing 'status' parameter on one of the API calls.
801608	Minor	Discovery	SNMP SysObjectId cannot be applied when a system defined 'Device Type' is used.
892781	Minor	Event Pulling Agents	Failed to Pull ELB forwarded logs using AWS-S3-WITH-SQS.
862020	Minor	Event Pulling Agents	Generic HTTPS Advanced Poller incorrectly sets lastPollTime window to local time instead of UTC.
788696	Minor	Event Pulling Agents	Azure Compute not working to government cloud; No Azure instance found.
690309	Minor	Event Pulling Agents	Unable to receive logs from Cloud-based Endpoint Solutions such as Bitdefender GravityZone via API.
912165	Minor	GUI	Interface Usage Dashboard: Wrong interface values are mapped when selecting interfaces from second table.
897192	Minor	GUI	When sorting a column in a Resource folder, then going to another Resource folder without that column, a Query Exception will occur.
895959	Minor	GUI	Searching function in Parser XML Editor does not work properly.
885293	Minor	GUI	Users are incorrectly redirected to 'Password reset page' even though password is still valid.
881317	Minor	GUI	Some UEBA tags are not applied.
862834	Minor	GUI	Application Monitoring does not show the correct message when you click on Monitor from CMDB.
860518	Minor	GUI	In Incident List View, switching incidents before trigger event query finishes will show the old incident's triggered events.
847236	Minor	GUI	Kafka Configuration - GUI shows an error when hostname is being saved as a Kafka broker.

Bug ID	Severity	Module	Description
845231	Minor	GUI	Elasticsearch Query that uses 'CONTAIN' with value ending with '\' will not complete.
807427	Minor	GUI	Incident HTTP notification test fails due to ':' in protocol string.
806694	Minor	GUI	Collector health page does not update 'collector type' column when the value has changed.
796076	Minor	GUI	In org level, **Admin > Device Support > Device Apps** -> Group list shows natural ID of custom group instead of Display names.
792520	Minor	GUI	Bar color in **CMDB> Devices> Summary> Health Overview** does not match with thresholds.
791298	Minor	GUI	VirusTotal connector does not complete when adding 'relationship to include' drop down.
853461	Minor	Linux Agent	Linux Agent fails to start up when IPv6 is disabled on Ubuntu 20.04.5.
905514	Minor	Parser (Data)	FortiGateParser stopped recognizing some FGT messages because of unexpected devid format in log.
893761	Minor	Parser (Data)	WinOSWmiParser parses different 'Process Name' for Security 4624 event.
889725	Minor	Parser (Data)	PaloAltoParser does not parse Source IP, Reason & User for PAN-OS-SYSTEM-generic.
886338	Minor	Parser (Data)	FortiGate parser update because of new devid format.
884941	Minor	Parser (Data)	FortiNAC parser needs to be extended.
877268	Minor	Parser (Data)	Event Type 'Google_Apps_moderator_action_add_user' needs to have more attributes to be parsed.
869873	Minor	Parser (Data)	FortiWeb Event Types contains incorrect description.
865141	Minor	Parser (Data)	Microsoft NPS event not fully parsed.
863302	Minor	Parser (Data)	3 Event Types have severity above 10.
846007	Minor	Parser (Data)	Parsed event type 'SentinelOne-EPP-Generic' missing event attributes.
842119	Minor	Parser (Data)	File Name' attribute incorrect or blank for FortiSandbox Syslog.
840182	Minor	Parser (Data)	WinOSWmiParser does not parse events with id 18456, if there is no user defined at the raw event log.
811131	Minor	Parser (Data)	CiscoIOS Parser has an unknown event.
809815	Minor	Parser (Data)	Palo Alto Threat ID 34261 miscategorized. Should be for cobalt strike, not a benign definition.

Bug ID	Severity	Module	Description
798684	Minor	Parser (Data)	Parse Cisco AMP for Endpoints API V0 raw logs for more information.
754074	Minor	Parser (Data)	Update Microsoft Network Policy Manager Parser for Windows Agent Collection.
907902	Minor	Performance Monitoring	Custom Perf Monitors always returns numerical data as DOUBLE, even when it is specified to be of a different data type.
898371	Minor	Performance Monitoring	Fail to monitor WebLogic 12c memory.
871853	Minor	Query	PctChange function is not working.
861224	Minor	RuleWorker	phRuleWorker randomly crashes due to possible memory corruption.
876849	Minor	System	For Disaster Recovery in EventDB based deployments, if NFS takes a long time to respond, replication health page responds incorrectly.
874222	Minor	System	FortiSIEM install fails since Red Hat hypervisor is not explicitly supported in install scripts.
867999	Minor	System	Changing the IP of the Supervisor using configFSM.sh will cause svn_url to change to repos/cmdb/.
857752	Minor	System	Include all cert formats during the Upgrade certificate backup and restore procedures.
729023	Minor	System	SQLite header and source version mismatch causes upgrade failure.
881225	Minor	Windows Agent	Unable to collect Windows DHCP logs with traditional Chinese characters in DhcpSrvLog-Mon.log.
799857	Minor	Windows Agent	XML key is truncated in Windows security events 1202/1203.
856691	Enhancement	Data	For the scenario - Administrator is added to FortiGate, the event type should be properly parsed and a rule should be created.
814287	Enhancement	DataPurger	Enhance Elasticsearch Event Export tool phExportESEvent to include org ID as an argument.
814145	Enhancement	Event Pulling Agents	Support Gzip compressed files on HTTP POST feature.
813609	Enhancement	Event Pulling Agents	Support Tenable Nessus Security Scanner via Nessus10 API.
796857	Enhancement	GUI	Support LookupTableGet() and event attribute on right side of Filter condition.

Bug ID	Severity	Module	Description
796453	Enhancement	GUI	Azure EventHub integration missing mapping to organization.
878826	Enhancement	Linux Agent	Add support for Ubuntu 22.04 LTS.
868661	Enhancement	Linux Agent	Add support for CentOS 9, RHEL 9 and Rocky Linux 9.
871607	Enhancement	Parser (Data)	Extend FortiDeceptor parser to include MITRE ATTACK TTP information.
845671	Enhancement	Parser (Data)	Event Severity' is not being parsed and evaluated properly in the KasperskyParser.
811438	Enhancement	Parser (Data)	Add support for cronyd events.
802206	Enhancement	Parser (Data)	Add parser for TSV formatted Zeek log.
845685	Enhancement	System	Unable to update FortiSandbox Malware Hash and URL In STIX v2 format.

Known Issues

- General
- ClickHouse Related
- Discovery Related
- Elasticsearch Related
- EventDB Related
- HDFS Related
- High Availability Related

General

See issues mentioned in Important Notes.

ClickHouse Related

1. If you are running ClickHouse event database and want to do Active-Active Supervisor failover, then your Supervisor should not be the **only** ClickHouse Keeper node. In that case, once the Supervisor is down, the ClickHouse cluster will be down and inserts will fail. It is recommended that you have 3 ClickHouse Keeper nodes running on Workers.
2. If you are running ClickHouse, then during a Supervisor upgrade to FortiSIEM 6.7.0 or later, instead of shutting down Worker nodes, you need to stop the backend processes by running the following command from the command line.

   ```
   phtools --stop all
   ```
3. If you are running Elasticsearch or FortiSIEM EventDB and switch to ClickHouse, then you need to follow two steps to complete the database switch.

   a. Set up the disks on each node in **ADMIN > Setup> Storage** and **ADMIN > License > Nodes**.
   b. Configure ClickHouse topology in **ADMIN > Settings > Database > ClickHouse Config**.

4. In a ClickHouse environment, Queries will not return results if none of the query nodes within a shard are reachable from Supervisor and responsive. In other words, if at least 1 query node in every shard is healthy and responds to queries, then query results will be returned. To avoid this condition, make sure all Query Worker nodes are healthy.

Discovery Related

Test Connectivity & Discovery may get stuck with Database update 0% when a few discoveries are running.

Elasticsearch Related

1. In Elasticsearch based deployments, queries containing "IN Group X" are handled using Elastic Terms Query. By default, the maximum number of terms that can be used in a Terms Query is set to 65,536. If a Group contains more than 65,536 entries, the query will fail.

   The workaround is to change the “max_terms_count” setting for each event index. FortiSIEM has been tested up to 1 million entries. The query response time will be proportional to the size of the group.

   Case 1. For already existing indices, issue the REST API call to update the setting

   ```
   PUT fortisiem-event-*/_settings
   {
     "index" : {
       "max_terms_count" : "1000000"
     }
   }
   ```

   Case 2. For new indices that are going to be created in the future, update fortisiem-event-template so those new indices will have a higher max_terms_count setting

   a. `cd /opt/phoenix/config/elastic/7.7`
   b. Add `"index.max_terms_count": 1000000` (including quotations) to the “settings” section of the `fortisiem-event-template`.

      Example:

      ...

      ```
            "settings": {
              "index.max_terms_count": 1000000,
      ```

      ...

   c. Navigate to **ADMIN > Storage > Online** and perform **Test** and **Deploy**.
   d. Test new indices have the updated terms limit by executing the following simple REST API call.

   ```
   GET fortisiem-event-*/_settings
   ```

2. FortiSIEM uses dynamic mapping for Keyword fields to save Cluster state. Elasticsearch needs to encounter some events containing these fields before it can determine their type. For this reason, queries containing `group by` on any of these fields will fail if Elasticsearch has not seen any event containing these fields. Workaround is to first run a non-group by query with these fields to make sure that these fields have non-null haves.

EventDB Related

Currently, Policy based retention for EventDB does not cover two event categories: (a) System events with phCustId = 0, e.g. a FortiSIEM External Integration Error, FortiSIEM process crash etc., and (b) Super/Global customer audit events with phCustId = 3, e.g. audit log generated from a Super/Global user running an adhoc query. These events are purged when disk usage reaches high watermark.

HDFS Related

If you are running real-time Archive with HDFS, and have added Workers after the real-time Archive has been configured, then you will need to perform a **Test** and **Deploy** for HDFS Archive again from the GUI. This will enable `HDFSMgr` to know about the newly added Workers.

High Availability Related

If you make changes to the following files on any node in the FortiSIEM Cluster, then you will have to manually copy these changes to other nodes.

1. FortiSIEM Config file (`/opt/phoenix/config/phoenix_config.txt`): If you change a Supervisor (respectively Worker, Collector) related change in this file, then the modified file should be copied to all Supervisors (respectively Workers, Collectors).
2. FortiSIEM Identity and Location Configuration file (`/opt/phoenix/config/identity_Def.xml`): This file should be identical in Supervisors and Workers. If you make a change to this file on any Supervisor or Worker, then you need to copy this file to all other Supervisors and Workers.
3. FortiSIEM Profile file (`ProfileReports.xml`): This file should be identical in Supervisors and Workers. If you make a change to this file on any Supervisor or Worker, then you need to copy this file to all other Supervisors and Workers.
4. SSL Certificate (`/etc/httpd/conf.d/ssl.conf`): This file should be identical in Supervisors and Workers. If you make a change to this file on any Supervisor or Worker, then you need to copy this file to all other Supervisors and Workers.
5. Java SSL Certificates (files `cacerts.jks`, `keyfile` and `keystore.jks` under `/opt/glassfish/domains/domain1/config/`): If you change these files on a Supervisor, then you have to copy these files to all Supervisors.
6. Log pulling External Certificates: Copy all log pulling external certificates to each Supervisor.
7. Event forwarding Certificates define in FortiSIEM Config file (`/opt/phoenix/config/phoenix_config.txt`): If you change on one node, you need to change on all nodes.
8. Custom cron job: If you change this file on a Supervisor, then you have to copy this file to all Supervisors.

Windows Agent Releases

Some Windows Agent 5.x.x, Windows Agent 4.4.x, Agent 4.3.x and 4.2.x features are only supported on FortiSIEM 6.4.0 or later.

Windows Agent 5.0.1

This Windows Agent release resolves the following issue:

If the Windows Agent loses network connection to the Collector for a period of time, then the performance monitoring events can have unknown event type. This can result in high Collector CPU (Bug 947196).

Windows Agent 5.0.0

This release contains the following features and enhancements:

1. In previous releases, discovery and performance monitoring for Windows Servers had to be performed via WMI/OMI only, which needed an account to be created on the server for FortiSIEM use. In this release, Windows Agent can perform discovery and performance monitoring, this feature has parity with WMI/OMI based discovery and performance monitoring.

   For configuring discovery and performance monitoring for Windows Agent, see Configuring Windows Agent - Monitor settings.
2. DNS Analytical logs are now collected via real time Events Tracing for Windows (ETW) provider. This is done to overcome an issue with the old design where DNS analytical logs can stop when the log size is full, requiring the agent to restart in order to pick up new analytical logs.

Windows Agent 4.4.1

This release includes the following bug fix.

For French locale, Windows Security, System and Application Event logs are incorrectly formatted, leading to important fields not being parsed (Bug 901252).

Windows Agent 4.4.0

This release contains the following new feature and bug fix.

Support for Virtual Desktop Infrastructure (VDI) Environment

Windows Agents can work in VDI environments using the following steps:

1. The administrator first installs the Windows Agent onto the VDI Golden image. See Installing Windows Agent in VDI Environment for details.
2. When user logs on to the VDI environment and downloads a VM from the VDI Server, the VM contains a VDI transient image (containing the Windows Agent). The agent automatically registers to the FortiSIEM Supervisor node, with host name set to <DOMAIN>__<USERNAME> in CMDB.
3. When user logs off from the VDI environment, the agent automatically unregisters to the FortiSIEM Supervisor node. The agent's status is decommissioned, so that it does not consume an agent license.

Bug Fix

Command line arguments in 'new process created' events are lowercased affecting base64 decoding of command line arguments (Bug 873700).

Windows Agent 4.3.0

This release provides the following features and improvements.

Software Installer Improvements

In earlier versions, FortiInsight User Entity Behavior Analysis (UEBA) was installed as a separate package and installer and showed up as a separate Windows service. Starting with this release, FortiInsight runs as an integrated module within FortiSIEM Windows Agent. This also means that FortiInsight will no longer be running in the background when the UEBA license, and template associations are not enabled.

Three installation options are provided: x86 MSI, x64 MSI and a bundled exe that automatically detects the correct MSI to use.

Installation paths, log files and registries have been renamed from AccelOps to FortiSIEM:

- Installation path has been updated from C:/Program Files/AccelOps to **C:/Program Files/Fortinet/FortiSIEM**
- ProgramData paths have been updated from C:/ProgramData/AccelOps to **C:/ProgamData/FortiSIEM/**
- Registry entries have been moved from HKLM/Software/AccelOps to **HKLM/Software/Fortinet/FortiSIEM**
- Log files have been added to **C:/Program Files/Fortinet/FortiSIEM/logs**
- ProxyTrace.log has been updated to **C:/ProgramData/FortiSIEM/logs/Trace.log**
- All libraries have been renamed from AccelOps to FortiSIEM.
  - AccelOps.Common > FortiSIEM.Common
  - AccelOps.Security > FortiSIEM.Security
  - AccelOps.Utilities > FortiSIEM.Utilities
  - AccelOps.WebProxy > FortiSIEM.WebProxy

Robust Detection of Event Log Restart (Event ID 1100)

In previous versions, Event Log restart was detected by tracking the Process ID (PID) of the Windows Event Log service. The assumption is that when Windows Event Log service restarts, the PID gets recycled. In some cases, however, the Windows Event Log “restart” does not recycle the PID, but just invalidates the handles.

This release adds a robust restart check by looking for the security Event ID 1100, which indicates a restart has occurred.

Restart Event Collection from Last Position

In previous versions, event collection starts from Agent startup time. This causes the Agent to miss events, especially in case of restart. In this release, the Windows Agent will store its last processed event and on restart, will begin event collection from that point. Restart will not result in Event loss.

Monitor Software Installed via Microsoft Apps

In previous versions, FortiSIEM Windows Agent would detect installed software when the user installed via standard installation mechanisms such as Control Panel or MSIs. This release adds support for the Microsoft App store, which has become more the standard for installing, and distributing Microsoft software. FortiSIEM Windows Agent 4.3 can now detect installed/removed software when the user installs software via the Microsoft App store.

Windows Agent 4.2.7

This release fixes the following issue.

Windows Agent process stops after enabling UEBA on Windows OS French language pack version (Bug 821479).

Windows Agent 4.2.6

This release fixes the following issue.

Virtual Collector configuration in Windows Agent Host to Template Association does not work correctly. Agent does not send events to the configured Virtual Collectors (Bug 812009).

Windows Agent 4.2.5

This release fixes the following issue.

Windows security logs with XML keyword are truncated. Examples are Windows Security Event ID 1202, 1203 for Active Directory Federation Service (ADFS) (Bug 799857).

Windows Agent 4.2.4

This release resolves the following issue.

Allow the following characters in the Windows Agent user name during registration: space, dollar, plus, minus, dot, at the rate of, underscore, left parenthesis, right parenthesis, in other words, these characters between double quote “ $*+-.@_()” (contains space) (Bug 790304).

Windows Agent 4.2.3

This release provides a way to install FortiSIEM Windows Agent so that the Administrator can stop the Agent Service if needed. To accomplish this, the user must install the Agent via the command line with the `UNPROTECT = 1` option. For details, see Installing with the Ability to Stop Agent Service in the Windows Agent Guide.

Windows Agent 4.2.2

This release adds support for the full special characters set in specifying Windows Agent passwords. Supported character set is specified at this website:

https://owasp.org/www-community/password-special-characters

Specifically, it includes (between double quotes): " !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~"

These characters can be input both via the Windows Agent command line and the GUI.

Windows Agent 4.2.1

This release fixes the following three issues for FortiSIEM Windows Agent.

1. The Agent may not capture Windows Event Forwarding (WEF) logs when WEF is configured to write forwarded logs to any folder other than the Forwarded Events folder on the forwarded server. In addition, the Agent's performance of WEF log handling is improved. (Bug 766939)
2. The Agent limits the Collectors' name to only 50 characters, which may not work in AWS where FQDN can be long. (Bug 770632)
   Note: The name is now 253 characters.
3. The Agent stops sending logs after killing or restarting Windows Event Log Process. (Bug 744891)

Windows Agent 4.2.0

This release contains two enhancements.

1. A GUI is provided for installing the Agent. See Installing FortiSIEM Windows Agent 4.2.x in the Windows Agent 4.x.x Installation Guide.
2. Ability to upgrade multiple agents in parallel from the Supervisor. See here.

Windows Agent 4.1.6

This release fixes the following three issues for FortiSIEM Windows Agent.

1. The Agent may not capture Windows Event Forwarding (WEF) logs when WEF is configured to write forwarded logs to any folder other than the Forwarded Events folder on the forwarded server. In addition, the

Agent's performance of WEF log handling is improved. (Bug 766939)

2. The Agent limits the Collectors' name to only 50 characters, which may not work in AWS where FQDN can be long. (Bug 770632)
   Note: The name is now 253 characters.
3. The Agent stops sending logs after killing or restarting Windows Event Log Process. (Bug 744891)

Windows Agent 4.1.5

This release resolves two security issues:

1. The log file contains plain text password used to register the agent to the Supervisor. This password is not used for any other purposes. (Bug 749499)
2. An authenticated windows user can run arbitrary Powershell scripts with Admin permissions. (Bug 749499)

Windows Agent 4.1.4

This release resolves two issues:

1. File handle leak while interfacing with local SQLite database. This can cause Windows Agent memory usage to grow overtime. (Bug 746978)
2. File handle leak while interfacing with Windows registry. This can cause Windows Agent memory usage to grow over time. (Bug 748252)

Windows Agent 4.1.3

This release resolves two issues:

1. When FortiSIEM monitors DNS Analytical logs, Windows EventLog service memory utilization maybe high. (Bug 723147)
2. Windows Agent may stop sending events if both the Supervisor and Collector go down for more than 10 minutes and then come up. (Bug 727842)

Windows Agent 4.1.2

This release adds the ability to work with FortiSIEM Management Extension Application (MEA) Collector released as part of FortiSIEM 6.3.0.

Windows Agent 4.1.1

This release fixes the following issues:

1. Windows Agent does not generate events when a monitoring template is chosen with a large set of comma separated eventIDs. Previous limit of 50 eventIDs or 250 characters is now extended to 1200 characters including comma separating characters. If you need more than this limit, you can always create multiple monitoring templates. (Bug 702090)
2. When Windows Event Forwarding is configured, FortiSIEM Agent running on the forwarded server may sometimes fail to get the message in Security Events. A new API is now used to collect the events from the Windows Forwarded Events folder. (Bug 710074)

Windows Agent 4.1.0

This release adds the following enhancements.

1. Agent will restart automatically after 1 minute if it is killed.
2. Service protection – user cannot Stop, Restart or Pause the agent from Windows Service Manager.
3. Users can change the logging level without restarting service by changing the registry key. Registry key instructions follow:
   A. Open HKEY_LOCAL_MACHINE\SOFTWARE\AccelOps\Agent key
   B. To update with trace logging, set “LogLevel” value to “2”
   C. To update with debug logging, set “LogLevel” value to “1”
4. Agent Database is used to store Agent configuration parameters and to store events when connectivity to collectors is lost. The default size for your Agent Database is 1GB. This can be changed by modifying the MaxDBSizeInMB entry in your Registry Editor.

Details are in the Windows Agent Guide.

Windows Agent 4.0.1

This release fixes three issues:

1. Agent status became disconnected on Windows server 2012R2. (Bug 672660)
2. The log file contains plain text password used to register the agent to the Supervisor. This password is not used for any other purposes. (Bug 749499)
3. An authenticated windows user can run arbitrary Powershell scripts with Admin permissions. (Bug 749499)

Windows Agent 4.0.0

This release provides User Entity Behavior Analysis (UEBA) by embedding a Kernel Agent that detects anomalies on these 10 user activities.

- Log on and log off
- Machine on and off

- File create
- file delete
- file read
- file write
- file rename
- file move
- file upload
- file download
- drive mount
- drive un-mount

Windows Agent 3.3.1

This release resolves two security issues:

1. The log file contains plain text password used to register the agent to the Supervisor. This password is not used for any other purposes. (Bug 749499)
2. An authenticated windows user can run arbitrary Powershell scripts with Admin permissions. (Bug 749499)

Windows Agent 3.3.0

This release fixes the following issue:

Windows Agent fails to send events to Collector after service restart or machine reboot. (Bug 659782)

Windows Agent 3.2.3

This release resolves two security issues:

1. The log file contains plain text password used to register the agent to the Supervisor. This password is not used for any other purposes. (Bug 749499)
2. An authenticated windows user can run arbitrary Powershell scripts with Admin permissions. (Bug 749499)

Windows Agent 3.2.2

This release fixes the following issue:

Windows Agent on certain platforms, including Windows10 Pro, may crash while doing File Integrity Monitoring checks. This can cause Agents to get disconnected from FortiSIEM GUI and cause events to stop coming. (Bug 653943)

Windows Agent 3.2.1

This release fixes the following issue:

Windows Agent service stops after a while with File Integrity Monitoring (FIM) turned on. (Bug 636060)

Windows Agent 3.2.0

This release includes several enhancements for File Integrity Monitoring (FIM) when using Windows Agents:

- Detect File Permission and Ownership changes.
- Ability to push monitored files from agents to the FortiSIEM Supervisor where an audit trail of file changes are kept in SVN. The user can then examine the differences between the files.
- Ability to detect file changes from a baseline.

Windows Agent 3.1.3

This release resolves two security issues:

1. The log file contains plain text password used to register the agent to the Supervisor. This password is not used for any other purposes. (Bug 749499)
2. An authenticated windows user can run arbitrary Powershell scripts with Admin permissions. (Bug 749499)

Windows Agent 3.1.2

This release adds the following new features and enhancements:

- Signed Agent binary: Windows Agent binaries are now cryptographically signed by Fortinet.
- Ability to specify host name: The user can specify a host name during Windows Agent installation. The Agent will register to the Supervisor with that host name. CMDB will show that host name.
- Virtual Collector Support: Agents can send events to a Virtual Collector (such as an F5 Load balancer) located between Agents and Collectors. Virtual Collectors can be defined in the Agent definition on the Supervisor.
- Agent fails to install if there is a file or folder named Program under C:\.

Windows Agent 3.1.0

This release contains the following Windows Agent specific enhancements, in addition to the ability to work without Agent Manager functionality described earlier.

- Support for Windows Event Forwarding: Windows can forward logs using Windows mechanisms to a Central Windows Server. A FortiSIEM agent on the central server can then bring all the events from the various windows servers to FortiSIEM. This is an alternative to running FortiSIEM agent on every Windows server. The disadvantage of this approach is that Windows (Security, application and system) event logs can be collected in this way, while FortiSIEM agent can collect other information such as FIM, Custom log, Sysmon etc. This release is able to parse the forwarded Windows events so that actual reporting Windows server is captured and all the attributes are parsed as sent by native agents.

- Support of Windows FIPS enabled mode: In earlier releases, the agent did not work properly if FIPS mode was turned on. This issue is addressed in this release.
- File hash for File Integrity Monitoring computed using SHA256: The file hash value for file/folder monitoring is now reported using SHA256 algorithm instead of MD5. This enables direct match with external threat intelligence malware file hashes.

Content Pack Updates

This document provides details about Content updates for various 7.0.x releases.

- Content Updates for 7.0.0, 7.0.1, 7.0.2 and 7.0.3
- Content Updates for 7.0.0, 7.0.1 and 7.0.2
- Content Updates for 7.0.0 and 7.0.1
- Content Updates for 7.0.0
- Initial Included Content Updates

Deployment Notes

Content Pack Updates require the use of FortiSIEM version 6.4.0 or later. Procedures related to Content Updates can be found here.

7.0.0 content pack updates release begin with Content Update 501, and increments.

Content Pack Updates must be done in the following order:

1. Update FortiSIEM Manager.
2. Update FortiSIEM Supervisor.
3. Update FortiSIEM Worker.

Content Updates for 7.0.0, 7.0.1, 7.0.2 and 7.0.3

- Content Update 514
- Content Update 513
- Content Update 511
- Content Update 510

Note: There is no Content Update 512.

Content Update 514

Published April 17, 2024

This content update contains the following:

1. 5 x Outbreak Rules and Reports:
   - Outbreak: Nice Linear eMerge Command Injection Vuln Detected on Network
   - Outbreak: Sunhillo SureLine Command Injection Attack Detected on Network
   - Outbreak: Sunhillo SureLine Command Injection Attack Detected on Host

  - Outbreak: PAN OS GlobalProtect Command Injection Vuln Detected on Network
  - Outbreak: PAN OS GlobalProtect Command Injection Vuln Detected on Host
2. Enhancements to Proofpoint and Unix parsers.
3. Latest GeoDB updates.

Content Update 513

Published March 25, 2024

This content update contains the following:

1. Updated Windows Agent Parser for Agent 7.1.4.
2. 2 Outbreak Rules and Reports:
   - Outbreak: ConnectWise ScreenConnect Attack Detected on Network
   - Outbreak: ConnectWise ScreenConnect Attack Detected on Host
3. Updated Ransomware Rule to prevent false positives.
   - Ransomware detected on a host
4. Updated Rule and Watchlist for Windows dormant users.
   - Windows Dormant Account Detected
5. Enhancements to FortiGate, DellNSeries, and Unix parsers.
6. Latest GeoDB updates.

Content Update 511

Published February 08, 2024

This content update contains the following:

1. Updated GenericJSON parser

Content Update 510

Published February 05, 2024

This content update contains the following:

1. 1 x Outbreak Rules and Reports:
   - Outbreak: Ivanti Connect Secure and Policy Secure Attack Detected on Network
2. New parser for Microsoft Graph API Platform
3. Updated FortiDeceptor and WinOSWmi parsers
4. For 7.0.3, this content update also contains Rollup of Content Updates 501-509. See Content Updates for 7.0.0, 7.0.1 and 7.02 (Content Updates 504-509), Content Updates for 7.0.0 and 7.0.1 (Content Update 503), and Content Updates for 7.0.0 (Content Updates 501-502) for more information.

Content Updates for 7.0.0, 7.0.1 and 7.0.2

Content Update 509

Published January 25, 2024

This content update contains the following:

1. 6 x Outbreak Rules and Reports:
    - Outbreak: Microsoft SharePoint Server Elevation of Privilege Vuln Detected on Network
    - Outbreak: Microsoft SharePoint Server Elevation of Privilege Vuln Detected on Host
    - Outbreak: Adobe ColdFusion Access Control Bypass Attack Detected on Network
    - Outbreak: Adobe ColdFusion Access Control Bypass Attack Detected on Host
    - Outbreak: Androxgh0st Malware Attack Detected on Network
    - Outbreak: Androxgh0st Malware Attack Detected on Host
2. Updated FortiGate and FortiProxy event types.
3. Latest GeoDB updates.

Content Update 508

Published December 20, 2023

This content update contains the following:

1. 4 x Outbreak Rules and Reports:
    - Outbreak: Lazarus RAT Attack Detected on Network
    - Outbreak: Lazarus RAT Attack Detected on Host
    - Outbreak: JetBrains TeamCity Authentication Bypass Attack Detected on Network
    - Outbreak: JetBrains TeamCity Authentication Bypass Attack Detected on Host
2. Enhancements to WinOSWmi and CiscoFTD parsers.
3. Latest GeoDB updates.

Content Update 507

Published November 29, 2023

This content update contains the following:

1. 3 Outbreak Rules and Reports:
   - Outbreak: Citrix Bleed Attack Detected on Network
   - Outbreak: Apache ActiveMQ Ransomware Attack Detected on Network
   - Outbreak: Apache ActiveMQ Ransomware Attack Detected on Host
2. Dedicated rules to detect admin user addition/deletion via console.
   - FortiGate: Admin User Added via Console
   - FortiGate: Admin User Deleted via Console
3. Added FortiEDR specific rules.
   - FortiEDR: Malicious Process Detected
   - FortiEDR: Malicious Process Blocked
   - FortiEDR: Suspicious Process Detected
   - FortiEDR: Suspicious Process Blocked
   - FortiEDR: Inconclusive or PUP Process Detected
   - FortiEDR: Inconclusive or PUP Process Blocked
   - FortiEDR: Likely Safe Process Detected
   - FortiEDR: Likely Safe Process Blocked
   - FortiEDR: Safe Process Detected
   - FortiEDR: Safe Process Blocked
4. Enhancements to FortiGate, CarbonBlackCEF, WinOSWmi, AOWUA_Win, PaloAlto, FortiEDR, FortiDeceptor, and FortiAuthenticator parsers.
5. New parser for ZScaler JSON logs - ZScalerNSSParser.
6. Fixed Application Server dashboard report and Netflow dashboards.
7. Latest GeoDB updates.

Content Update 506

Published November 1, 2023

This content update contains the following:

1. 3 Outbreak Rules and Reports:
   - Outbreak: Cisco IOS XE Web UI Attack Detected on Network
   - Outbreak: HTTP2 Rapid Reset Attack Detected on Network
   - Outbreak: HTTP2 Rapid Reset Attack Detected on Host
2. Latest GeoDB updates.

Content Update 505

Published October 11, 2023

This content update contains the following:

1. 2 Outbreak Rules and Reports:
   - Outbreak: Google Chromium WebP Vuln Detected on Network
   - Outbreak: Google Chromium WebP Vuln Detected on Host
2. Dedicated rules for detecting FortiMail Malicious URL/File attachments.
   - FortiMail: Malicious URL found
   - FortiMail: Malicious Spam File Attachment Found
3. Updated Malware rule to detect FortiGate IPS events.
   - Malware found by firewall but not remediated
4. Updated Windows Sigma rule to prevent false positives.
   - Windows: Possible DCShadow
5. Enhancements to FortiGate, FortiEDRRest, FortiMail, PulseSecure, McAfeeWebGwCEF, and PaloAlto parsers.
6. Latest GeoDB updates.

Content Update 504

Published September 21, 2023

This content update contains the following:

1. 6 Outbreak Rules and Reports:
   - Outbreak: Adobe ColdFusion Deserialization of Untrusted Data Vuln Detected on Network
   - Outbreak: Adobe ColdFusion Deserialization of Untrusted Data Vuln Detected on Host
   - Outbreak: WooCommerce Payments Improper Authentication Vuln Detected on Network
   - Outbreak: WooCommerce Payments Improper Authentication Vuln Detected on Host
   - Outbreak: Agent Tesla Malware Attack Detected on Network
   - Outbreak: Agent Tesla Malware Attack Detected on Host
2. New parser for FortiWeb Cloud
3. Enhancements to FortiClient, FortiWeb, FortiAuthenticator, FortiManager, WinOSWmi, GenericDHCP, and Sourcefire2 parsers
4. Latest GeoDB updates
5. For 7.0.2, this content update also contains Rollup of Content Updates 501-503. See Content Updates for 7.0.0 (Content Updates 501-502) and Content Updates for 7.0.0 and 7.0.1 (Content Update 503) for more information.

Content Updates for 7.0.0 and 7.0.1

- Content Update 503

Content Update 503

Published August 24, 2023

This content update contains the following:

1. 5 Outbreak Rules and Reports:
   - Outbreak: Microsoft Office and Windows HTML RCE Vuln Detected on Network
   - Outbreak: Microsoft Office and Windows HTML RCE Vuln Detected on Host
   - Outbreak: Zyxel Router Command Injection Attack Detected on Network
   - Outbreak: Ivanti Endpoint Manager Mobile Authentication Bypass Vuln Detected on Network
   - Outbreak: Ivanti Endpoint Manager Mobile Authentication Bypass Vuln Detected on Host
2. New parser for Armis Asset Intelligence Platform.
3. New parser for Hillstone Firewall.
4. Enhancements to FortiEDRParser, GitlabLogParser, FortiClientParser and UbiquityParser.
5. Latest GeoDB updates.
6. For 7.0.1, this content update also contains Rollup of Content Updates: 501-502. See Content Updates for 7.0.0 (501-502) for more information.

Content Updates for 7.0.0

- Content Update 502
- Content Update 501

Content Update 502

Published July 13, 2023

This content update contains the following:

1. Enhanced FortiGateParser, McAfeeXmlParser, and WinOSWmiParser.
2. 3 x Outbreak Rules and Reports:
   - Outbreak: VMware Aria Operations for Networks Command Injection Vuln Detected on Network
   - Outbreak: Apache RocketMQ RCE Vuln Detected on Network
   - Outbreak: SolarView Compact Command Injection Vuln Detected on Network
3. Added the following Dragos threatfeed rules and reports:

- Traffic to Dragos Worldview Malware IP List
- Permitted Traffic from Dragos Worldview Malware IP List

4. Latest GeoDB updates.

Content Update 501

Published June 16, 2023

This content update contains the following:

1. 9 x Outbreak Rules and Reports:
   - Outbreak: Multiple Vendor Camera System Attack Detected on Network
   - Outbreak: TP-Link Archer AX-21 Command Injection Attack Detected on Network
   - Outbreak: TP-Link Archer AX-21 Command Injection Attack Detected on Host
   - Outbreak: Zyxel Multiple Firewall Vuln Detected on Network
   - Outbreak: Zyxel Multiple Firewall Vuln Detected on Host
   - Outbreak: Progress MOVEit Transfer SQL Injection Vuln Detected on Network
   - Outbreak: Progress MOVEit Transfer SQL Injection Vuln Detected on Host
   - Outbreak: CosmicEnergy Malware Detected on Network
   - Outbreak: CosmicEnergy Malware Detected on Host
2. Latest GeoDB updates.

Initial Included Content Updates

The following content updates from FortiSIEM 6.x are included with FortiSIEM 7.0.0.

Content Update

Published May 16, 2023

This content update contains the following:

1. FortiNAC parser enhancement.
2. PaloAlto parser enhancement.
3. 4 x Outbreak Rules and Reports:
   - Outbreak: PaperCut MF/NG Improper Access Control Vulnerability Detected on Network
   - Outbreak: PaperCut MF/NG Improper Access Control Vulnerability Detected on Host
   - Outbreak: TBK DVR Authentication Bypass Attack Detected on Network
   - Outbreak: Oracle WebLogic Server Vuln Detected on Network
4. Latest GeoDB updates.

Content Update

Published April 27, 2023

This content update contains the following:

1. Fixed several dashboard reports for FortiDeceptor and FortiGate
2. Fixed FortiGate Parser issue for some models
3. 5 x Outbreak Rules and Reports:
    - Outbreak: Zoho ManageEngine RCE Vulnerability Detected on Network
    - Outbreak: ThinkPHP Remote Code Execution Vulnerability Detected on Network
    - Outbreak: ThinkPHP Remote Code Execution Vulnerability Detected on Host
    - Outbreak: Realtek SDK Attack Detected on Network
    - Outbreak: Realtek SDK Attack Detected on Host
4. Latest GeoDB updates.

Content Update

Published April 04, 2023

This content update contains the following:

1. 10 x Outbreak Rules and Reports:
    - Outbreak: IBM Aspera Faspex Code Execution Vulnerability Detected on Network
    - Outbreak: IBM Aspera Faspex Code Execution Vulnerability Detected on Host
    - Outbreak: Joomla! CMS Improper Access Check Vulnerability Detected on Network
    - Outbreak: Teclib GLPI Remote Code Execution Vulnerability Detected on Network
    - Outbreak: Progress Telerik UI Attack Detected on Network
    - Outbreak: Progress Telerik UI Attack Detected on Host
    - Outbreak: Microsoft Outlook Elevation of Privilege Vulnerability Detected on Network
    - Outbreak: Microsoft Outlook Elevation of Privilege Vulnerability Detected on Host
    - Outbreak: 3CX Supply Chain Attack Detected on Network
    - Outbreak: 3CX Supply Chain Attack Detected on Host
2. Latest GeoDB Updates.

Content Update

Published March 14, 2023

This content update contains the following:

1. FortiGateParser update.
2. 5 x Outbreak Rules and Reports:
    - Outbreak: VMware ESXi Server Ransomware Attack Detected on Network
    - Outbreak: Cacti Server Command Injection Attack Detected on Network
    - Outbreak: Cacti Server Command Injection Vulnerability Detected on Host
    - Outbreak: Fortra GoAnywhere MFT RCE Vulnerability Detected on Host
    - Outbreak: Fortra GoAnywhere MFT RCE Vulnerability Detected on Network
3. All outbreak network rules updated to not trigger when source is public and is blocked by a firewall.
4. Latest GeoDB Updates.

Content Update

Published February 7, 2023

This content update contains the following:

1. 4 x Outbreak Rules and Reports
    - Outbreak: Control Web Panel Login Exploit Detected on Host
    - Outbreak: Control Web Panel Login Exploit Detected on Network
    - Outbreak: Router Malware Attack Detected on Host
    - Outbreak: Router Malware Attack Detected on Network
2. Latest GeoDB Updates

Content Update

Published January 12, 2023

This content update contains the following:

- Windows Parsing Enhancements
- 9 x Outbreak Rules and Reports
    - Outbreak: Atlassian Pre-Auth Arbitrary File Read Vuln detected on Network
    - Outbreak: Atlassian Pre-Auth Arbitrary File Read Vuln detected on Host
    - Outbreak: BURNTCIGAR MS Signed Driver Malware detected on Network
    - Outbreak: BURNTCIGAR MS Signed Driver Malware detected on Host
    - Outbreak: FortiWeb detected VMware Spring Cloud Func RCE Vulnerability on Network
    - Outbreak: VMware Spring Cloud Func RCE Vulnerability on Network
    - Outbreak: FortiWeb detected Zerobot Botnet Activity on Network

  - Outbreak: Zerobot Botnet Activity Detected on Host
  - Outbreak: Zerobot Botnet Activity Detected on Network
- UnixParser support for Chronyd events
- Dedicated rules for detecting FortiGate admin user creation/deletion
  - FortiGate: Admin User Added
  - FortiGate: Admin User Deleted
- PaloAlto Parser updated to parse additional attributes for some log types
- Latest GeoDB Updates

Content Update

Published December 20, 2022

This content update contains Outbreak rules and reports, and the latest GEO database updates.

Note: 6.4.2 begins with Content Update 118 being available. It contains content from prior updates for 6.4.2, so older Content Updates do not need to be downloaded.

Added Rules

- Outbreak: VMWare Workspace ONE Vulnerability - CVE-2022-22954 on Network
- Outbreak: Redigo Malware Detected on Network
- Outbreak: Redigo Malware Detected on Host
- Outbreak: FortiOS SSLVPN Heap Buffer Overflow Attack - CVE-2022-42475 Detected on Network

Added Reports

- Outbreak: VMWare Workspace ONE Vulnerability - CVE-2022-22954 on Network
- Outbreak: Redigo Malware Detected on Network
- Outbreak: Redigo Malware Detected on Host
- Outbreak: FortiOS SSLVPN Heap Buffer Overflow Attack - CVE-2022-42475 Detected on Network

Content Update

Published November 30, 2022

This content update contains Outbreak rules and reports, updated FortiGate and FortiProxy regular IPS signatures, updated FortiGate and FortiProxy Industrial Operational Technology (OT) IPS signatures, and the latest GEO database updates.

Added Rules

- Outbreak: ABB Flow Computer Path Traversal Vulnerability Detected on Network
- Outbreak: Sandbreak vm2 sandbox module RCE Vulnerability Detected on Network

- Outbreak: Hive Ransomware Detected on Network
- Outbreak: Hive Ransomware Detected on Host
- Outbreak: X.509 Email Address Buffer Overflow in OpenSSL 3.0.0 to 3.0.6 detected on Network
- Outbreak: X.509 Email Address Buffer Overflow in OpenSSL 3.0.0 to 3.0.6 detected on Host
- Outbreak: CISA Top 20 Vulnerability detected on Host
- Outbreak: FortiGate detected CISA Top 20 Vulnerability on Network
- Outbreak: FortiWeb detected CISA Top 20 Vulnerability on Network

Added Reports

- Outbreak: ABB Flow Computer Path Traversal Vulnerability Detected on Network
- Outbreak: Sandbreak vm2 sandbox module RCE Vulnerability Detected on Network
- Outbreak: Hive Ransomware Detected on Network
- Outbreak: Hive Ransomware Detected on Host
- Outbreak: X.509 Email Address Buffer Overflow in OpenSSL 3.0.0 to 3.0.6 detected on Network
- Outbreak: X.509 Email Address Buffer Overflow in OpenSSL 3.0.0 to 3.0.6 detected on Host
- Outbreak: CISA Top 20 Vulnerability detected on Host
- Outbreak: FortiGate detected CISA Top 20 Vulnerability on Network
- Outbreak: FortiWeb detected CISA Top 20 Vulnerability on Network

Content Update

Published October 26, 2022

This content update contains rules and reports for Prestige Ransomware, Apache Commons Text RCE (CVE-2022-42889, CVE-2022-33980), and an enhanced FortiSandbox parser.

Added Rules

- Prestige Ransomware Detected on Network
- Prestige Ransomware Detected on Host
- Apache Commons Text RCE Vulnerability Detected on Network
- Apache Commons Text RCE Vulnerability Detected on Host

Added Reports

- Prestige Ransomware Detected on Network
- Prestige Ransomware Detected on Host
- Apache Commons Text RCE Vulnerability Detected on Network
- Apache Commons Text RCE Vulnerability Detected on Host

Parser Update

- FortiSandboxParser - Parse sha1 checksum

Content Update

Published October 14, 2022

This content update contains a rule and report for FGT Auth Bypass on Administrative Interface (CVE-2022-40684), enhanced parsers, and the latest GEO database updates.

Added Rule

- FortiGate Authentication bypass on Administrative Interface

Added Report

- FortiGate Authentication bypass on Administrative Interface Detected

Parser Updates

- AOWUA_DNSParser - Parse event severity
- FortiGate- Detection for CVE-2022-40684
- FortiProxy - Detection for CVE-2022-40684

Content Update

Published October 6, 2022

This content update contains rules and reports for Microsoft Exchange ProxyNotShell RCE Vulnerability (CVE-2022-41040, CVE-2022-41082), enhanced parsers, an enhanced "Concurrent VPN Authentications To Same Account From Different Cities" rule, and the latest GEO database updates.

Added Rules

- Microsoft Exchange Autodiscover RCE ProxyNotShell Detected on Host
- Microsoft Exchange Autodiscover RCE ProxyNotShell Detected on Network

Added Reports

- Microsoft Exchange Autodiscover RCE ProxyNotShell Detected on Host
- Microsoft Exchange Autodiscover RCE ProxyNotShell Detected on Network

Modified Rules

- Concurrent VPN Authentications to same account from different cities, excluded user “N/A” seen in some FortiGate VPN logs

Parser Updates

- ImpervaParser – Event types generalized to reflect that SecureSphere does more than just DB monitoring
- FireEyeParsers – Test modified/corrected events
- FortiSandbox – Enhanced to handle additional fields, and re-structured to allow ease of expansion

Content Update

Published September 23, 2022

This content update contains rules and reports for Apache Path Traversal Vulnerability (CVE-2021-42013, CVE-2021-41773), Wordpress WPGateway Plugin Vulnerability (CVE-2022-3180), an added parser, and latest GEO database updates.

Rules

- Apache Path Traversal Vuln Detected on Network
- Apache Path Traversal Vuln Detected on Host
- Wordpress WPGateway Plugin Vuln Detected on Network
- Wordpress WPGateway Plugin Vuln Detected on Host

Reports

- Apache Path Traversal Vuln Detected on Network
- Apache Path Traversal Vuln Detected on Host
- Wordpress WPGateway Plugin Vuln Detected on Network
- Wordpress WPGateway Plugin Vuln Detected on Host

Parser Update

- MSDefAdvancedHuntingParser

  Note: This update corrects an issue by re-adding this missing parser.

Content Update

Published September 12, 2022

This content update contains rules and reports for Hikvision Command Injection Vulnerability (CVE-2021-36260), and FortiDeceptor parser updates.

Rules

- Hikvision IP Camera Command Injection Vulnerability CVE-2021-36260 on Network

Reports

- Hikvision IP Camera Command Injection Vulnerability CVE-2021-36260 on Network

Parser Updates

- FortiDeceptorParser

Content Update

Published August 30, 2022

This content update contains rules and reports for Zimbra Collaboration Mboximport Vulnerability (CVE-2022-27925, CVE-2022-37042) and several parser updates.

Rules

- Zimbra Collaboration Mboximport Vulnerability Detected on Host
- Zimbra Collaboration Mboximport Vulnerability on Network

Reports

- Zimbra Collaboration Mboximport Vulnerability Detected on Host
- Zimbra Collaboration Mboximport Vulnerability on Network

Parser Updates

- AwsSecurityHubParser
- BarracudaCloudGenFWParser
- BitdefenderGravityZoneParser
- BroadcomSSLParser
- CheckpointCEFParser
- CiscoAMPParser
- CiscoIOSParser
- CiscoMerakiParser
- CiscoNxOSParser
- ClarotyParser
- ExtremeSwitchParser
- F5Big-IP-LTMParser
- FalconDataRepParser
- FalconStreamingParser
- FortiGateParser
- FortiInsightAPIParser
- FortiInsightNativeParser

- FortiMailParser
- FortiNDRParser
- FortiWebParser
- FoundryIronwareParser
- GeneralPatternDefinitions
- GoogleGCPParser
- H3CComwareParser
- HPProCurveParser
- HuaweiVRPParser
- InfoBloxAppParser
- InfoBloxAuditParser
- IPswitchWS_FTPParser
- IronportMailParser
- JenkinsParser
- JunipNSM-IDP
- JunipSSGFirewallLog
- MikroTikFirewallParser
- MotorolaWiNGParser
- MSDefAdvancedHuntingParser
- NCircleVAParser
- NginxParser
- OracleAuditParser
- OracleCASBParser
- PacketFence2Parser
- PaloAltoCEFParser
- parserOrder.csv
- PCAPPacketsDataParser
- PHBoxParser
- PHGenericLogParser
- PostfixParser
- RadiusParser
- ReconnextLogParser

- RSAAuthenticationServerParser
- SAPEnterpriseThreatDetectionParser
- SnortParser
- SophosUTMParser
- UbiquityParser
- UnixParser
- VeeamBackupParser
- VMwareVCenterParser
- WatchGuardFirewallParser
- WinDefATPParser
- WinOSPullParser
- WinOSWmiParser
- WinSyslogParser
- ZyxelUSGParser

Content Update

Published August 25, 2022

This content updates contains an added parser, several parser updates, and latest GEO database updates.

Added Parser

- BarracudaWebSecGWParser.xml

Parser Updates

- ApacheParser.xml
- AOWUA_WinParser.xml
- AwsSecurityHubParser.xml
- BitdefenderGravityZoneParser.xml
- CiscoASAParser.xml
- CiscoIOSParser.xml
- CiscoISEParser.xml
- CloudTrailParser.xml
- FireAMPCloudParser.xml
- Office365Parser.xml
- PHBoxParser.xml

- Rapid7InsightVMVulnParser.xml
- RuckusParser.xml
- WinDefATPParser.xml
- WinOSWmiParser.xml

Content Update

Published June 7, 2022

This content update contains 2 new rules and reports for detecting Atlassian Confluence Vulnerability (CVE-2022-26134).

Rules

- Atlassian Confluence CVE-2022-26134 Vuln Detected on Host
- Atlassian Confluence CVE-2022-26134 Vuln Detected on Network

Reports

- Atlassian Confluence CVE-2022-26134 Vuln Detected on Host
- Atlassian Confluence CVE-2022-26134 Vuln Detected on Network

Content Update

Published June 3, 2022

This content update contains 2 new rules and reports for detecting Microsoft Office Follina Vulnerability (CVE-2022-30190), ExtremeSwitch Parser updates, and latest Geo database updates.

Rules

- Microsoft Office Follina Vuln Detected on Host
- Microsoft Office Follina Vuln Detected on Network

Reports

- Microsoft Office Follina Vuln Detected on Host
- Microsoft Office Follina Vuln Detected on Network

Parser Update

- ExtremeSwitch

Content Update

Published May 19, 2022

This content update contains 2 new rules and reports for detecting Sysrv-K Botnet Activity which exploits CVE-2022-22947 and other vulnerabilities in the Spring Framework and WordPress plugins.

Rules

- Sysrv-K Botnet Activity Detected on Network
- Sysrv-K Botnet Activity Detected on Host

Reports

- Sysrv-K Botnet Activity Detected on Network
- Sysrv-K Botnet Activity Detected on Host

Content Update

Published April 18, 2022

This content update contains 2 new rules and reports for detecting Microsoft Driver RCE vulnerability (CVE-2022-26809). In addition, Geo database updates are also included.

Rules

- Microsoft Driver RCE vulnerability - CVE-2022-26809 Detected on Network
- Microsoft Driver RCE vulnerability - CVE-2022-26809 Detected on Host

Reports

- Microsoft Driver RCE vulnerability - CVE-2022-26809 Detected on Network
- Microsoft Driver RCE vulnerability - CVE-2022-26809 Detected on Host

Content Update

Published April 1, 2022

This content update contains rules and reports for detecting Spring4Shell zero day remote code execution vulnerability (CVE-2022-22965). The detection is currently based on Fortinet products.

Rules

- Spring4Shell Malware Detected on Host
- Spring4Shell Malware Detected on Network

Reports

- Spring4Shell Malware Detected on Host
- Spring4Shell Malware Detected on Network

Content Update

Published March 07, 2022

This content update contains rules and reports for detecting HermeticWiper-FoxBlade malware (CVE_2021_44228). The detection is currently based on Fortinet products. The content update also includes the latest Fortinet GeoDB update.

Rules

- HermeticWiper-Foxblade Malware Detected on Host
- HermeticWiper-Foxblade Malware Detected on Network

Reports

- HermeticWiper-Foxblade Malware Detected on Host
- HermeticWiper-Foxblade Malware Detected on Network

GeoDB

- FortiGuard latest GeoDB updates

Content Update

Published February 23, 2022

15 Parser Updates

- CheckpointCEFParser
- DragosParser
- F5Big-IP-LTMParser
- ForeScoutCounterACTParser
- FortiAnalyzerParser
- FortiWebParser
- HPProCurveParser
- JunOSParser
- NozomiParser
- PaloAltoParser
- PHGenericLogParser
- SAPEnterpriseThreatDetectionParser
- VMwareVCenterParser
- WinOSWmiParser
- WinSyslogParser

7 New Parsers

- CybereasonCEFParser
- HitachiVSPParser
- MSDefAdvancedHuntingParser
- NutanixParser
- SAPEnterpriseThreatDetectionParser
- TrendMicroWorryFreeParser
- VMwareNSXvSphereParser

11 New Reports

- MS Defender for Endpoint Alerts
- MS Defender for Endpoint Events
- Nutanix: API Requests Audit
- Nutanix: Top Dropped Traffic Flows
- Nutanix: Top Dropped Traffic Flows by Destination
- Nutanix: Top Dropped Traffic Flows by Source
- Nutanix: Top Permitted Traffic Flows
- Nutanix: Top Permitted Traffic Flows by Destination
- Nutanix: Top Permitted Traffic Flows by Source
- Nutanix: Top Consolidated Audit Events by User
- Nutanix: Top Consolidated Audit Events by Count

14 New Rules

- FortiAnalyzer: No logs received from a device in 4 hours
- MS Defender for Endpoint Alert - Generic
- LSASS Memory - Credential Access Alert from MS Defender for Endpoint
- Process Injection - Defense Evasion Alert from MS Defender for Endpoint
- Suspicious Process Discovery - Discovery Alert from MS Defender for Endpoint
- System Network Configuration Discovery - Discovery Alert from MS Defender for Endpoint
- System Service Discovery - Discovery Alert from MS Defender for Endpoint
- Ingress Tool Transfer - Execution Alert from MS Defender for Endpoint
- Masquerading - Execution Alert from MS Defender for Endpoint
- Suspicious PowerShell command line - Execution Alert from MS Defender for Endpoint

- Suspicious Task Scheduler activity - Persistence Alert from MS Defender for Endpoint
- OS Credential Dumping - Suspicious Activity Alert from MS Defender for Endpoint
- Windows Logging Service Shutdown
- Windows Security Log is Full

22 Bugs Fixes

- 782926 – Add Parsing, Rules, and Reports for MS Defender AdvancedHunting Events forwarded to Azure Event Hub
- 773036 – Checkpoint CEF Parser didn’t properly handle URL filtering logs
- 762065 – Add parsing support for Cybereason CEF log format
- 754611 – Update Dragos Parser to support events with MITRE data
- 598590 – Update F5Big-IP-LTM Parser to extract GEO location information from some logs
- 762424 – Update ForeScoutCounterACT Parser to handle additional log format
- 776027 – Update FortiAnalyzer Parser to not set Reporting Device Name if the value is “.self”, observed when forwarding local system logs
- 770842 – Update FortiWeb Parser to handle logs from legacy hardware models
- 762419 – Add syslog parser for Hitachi VSP logs
- 754088 – Update HP Procurve Parser to handle additional log format
- 769325 – Update JunOS Parser to handle additional event type formats
- 769317 – Update Nozomi Parser to handle MITRE data in syslog
- 645109 – Add Nutanix syslog parser, reports, and dashboard
- 770908 – Palo Alto event type PAN-OS-THREAT-virus-100000-deny is not parsed correctly
- 781393 - Set correct phEventCategory of system PH_GENERIC_DEBUG events
- 765158 – Update VMwareVCenter Parser to handle additional generic event types
- 777847 – Update WinOSWmiParser and WinSyslog parsers to better handle Terminal Services events
- 770195 – Update WinOSWmiParser to categorize Active Directory Federated Services events
- 745940 – Update WinOSWmiParser to parse relative target name correctly for some events
- 706296 – Add missing windows security event types and rules corresponding to Windows Logging Service Shutdown and Windows Security Log is full
- 771691 – Add support for Trend Micro Worry-Free Business Security Services (WFBS-SVC) via syslog
- 762384 – Add parser for VMware NSX-V appliance, the logging format is distinct from NSX-T appliances

Content Update

Published on February 15, 2022

2 New Rules to detect CVE-2022-21882

- Win32k Elevation of Privilege Vulnerability Detected on Network
- Win32k Elevation of Privilege Vulnerability Detected on Host

2 New Reports for CVE-2022-21882

- Win32k Elevation of Privilege Vulnerability Detected on Host
- Win32k Elevation of Privilege Vulnerability Detected on Network

Content Update

Published on January 24, 2022

4 New Rules

- Active Directory Privilege Escalation Exploit Detected on Host
- Active Directory Privilege Escalation Exploit Detected on Network
- Windows HTTP Protocol Stack RCE Detected on Host
- Windows HTTP Protocol Stack RCE Detected on Network

4 New Reports

- Active Directory Privilege Escalation Exploit Detected on Host
- Active Directory Privilege Escalation Exploit Detected on Network
- Windows HTTP Protocol Stack RCE Detected on Host
- Windows HTTP Protocol Stack RCE Detected on Network

Key Concepts

This section describes several key concepts used in FortiSIEM.

Clustering Architecture

FortiSIEM scales seamlessly from small enterprises to large and geographically distributed enterprises and service providers.

- For smaller deployments, FortiSIEM can be deployed as a single all-in-one hardware or virtual appliance that contains full functionality of the product. This is the Supervisor node.
- For larger environments that need greater event handling throughput, FortiSIEM can be deployed in a cluster of Supervisor and Worker Virtual Appliances. Collector nodes are also used to distribute event collection to Collectors for performance and also architecture reasons such as collecting events from remote networks and different network segments.
- For larger distributed environments where there are multiple instances of FortiSIEM, the FortiSIEM Manager can be used to monitor separate FortiSIEM instances and manage Incidents. FortiSIEM Manager is a separately licensed product to FortiSIEM. Unless there is a requirement to manage multiple FortiSIEM Instances (Supervisors), then please begin with installing the Supervisor which will manage Worker nodes, Collector nodes and Agents.

There are four types of FortiSIEM nodes – Collector, Worker, Supervisor and Manager. Collectors are used to scale data collection from various geographically separated network environments potentially behind firewalls. Collectors communicate to the devices, collect, parse and compress the data and then send this information to the Worker nodes over a secure HTTP(S) channel in a load balanced manner. Supervisor and Worker nodes reside inside the data center and perform data analysis functions using distributed co-operative algorithms.

A FortiSIEM instance consists of Supervisor, multiple Workers and Collectors. A FortiSIEM Manager can be used to monitor and manage multiple FortiSIEM instances over HTTPS REST API channel. Incidents, License and Health information are forwarded from each FortiSIEM instance to the FortiSIEM Manager. From FortiSIEM Manager, you can Clear/Resolve/Change Severity/Add comments to one or more Incidents, disable one or more rules and change their severity, run FortiSOAR Playbooks and Connectors to update Incident Status and Comments. A one-click operation to log you into the appropriate FortiSIEM instance where an Incident occurred. This enables you quickly to investigate an Incident in depth.

There are five primary data analysis tasks:

1. Data indexing and storing in an event database
2. Data searching
3. Correlating data in streaming mode to trigger rules (behavioral anomalies)
4. Creating a user identity and location database to add context for data
5. Creating baselines for anomaly detection

For scalability, each of these tasks is divided into a heavyweight Worker component executed by the Worker nodes and a lightweight Master component executed by the Supervisor node. The Supervisor nodes, accessible via the GUI is comprised of a self-contained three-tier model – the GUI, the Application Server containing the business logic, and a relational database for holding the FortiSIEM application state.

For scalable event storage, FortiSIEM provides three options:

- Local disk
- FortiSIEM NoSQL event database with data residing on an NFS Server
- Elasticsearch distributed database

Hardware appliance and All-in-one virtual appliance solutions use the local disk option while the NoSQL or Elasticsearch options can be exploited by a FortiSIEM cluster of Supervisor and Workers.

The NoSQL event database option is a purpose built FortiSIEM proprietary solution. The Supervisor and Worker nodes create and maintain the database indices. To scale event insertion and search performance in this mode requires (a) a fast communication network between the Supervisor/Worker nodes and the NFS Server and (b) high NFS IOPS that can be achieved using fast RAID disk or tiered SSD and magnetic disks.

Elasticsearch provides a true distributed, redundant columnar database option for scale-out database performance at the expense of higher storage needs. In this option, FortiSIEM Worker nodes push the data in real time to Elasticsearch cluster, which maintains the event database. FortiSIEM has developed an intermediate adaptation layer, so that the same GUI can run seamlessly on both Elasticsearch and FortiSIEM NoSQL event database.

Licensing

FortiSIEM is licensed based on the following:

- Number of devices FortiSIEM monitors or receives logs from
- Number of Windows Agents and Linux Agents
- Aggregate Events per Second (EPS) it receives

Note that FortiSIEM licensing is not based on storage - you can store and query the data as needed for your compliance needs without any concern regarding licensing. The license parameters can be perpetual or subscription based. Maintenance and FortiGuard Threat Intelligence are subscription based.

You can have unlimited devices in CMDB. However, the total number of devices that send logs to FortiSIEM or are monitored by FortiSIEM cannot exceed the device license. The devices under license are called 'Managed' while the remaining devices are called 'Unmanaged'. If you do a discovery and the number of newly discovered devices combined with Managed CMDB devices exceed the license, then the extra devices are tagged in CMDB as 'Unmanaged'. You can either buy more device license or exchange an Unmanaged device with a Managed device.

FortiSIEM calculates Events per Second (EPS) over a 3-minute period as the total number of events received over a 3-minute period divided by 180. FortiSIEM is a distributed system where events can be received at any node - Collector, Worker, or Supervisor. The EPS licensing is enforced as follows:

At the end of every 3-minute interval, Incoming EPS is calculated at each event entry node (Collector, Worker, or Supervisor) and the value is sent to the central decision-making engine on the Supervisor node.

1. The Supervisor node takes all Incoming EPS values and based on the Licensed EPS, computes the Allocated EPS for the next 3-minute interval for every node and communicates those values to every node.
2. For the next 3-minute interval, each node accepts up to (Allocated EPS * 180) events. It also reports Incoming EPS for the current interval to the Supervisor node.
3. The continuous EPS reallocation process continues.

FortiSIEM includes some additional refinements to EPS enforcement as follows:

- Each Collector has a Guaranteed EPS. The Allocated EPS for this Collector is always greater than the Guaranteed EPS.
- FortiSIEM keeps track of Unused EPS as the sum of positive differences of Allocated EPS and Incoming EPS over all nodes. At the beginning of the day (12:00 am), Unused EPS is set to 50% of previous day’s Unused EPS and then Unused EPS accumulates throughout the day before maxing out at five times Licensed EPS. Unused EPS can be used for bursting during attacks or other event surge periods, beyond Licensed EPS.

For more details on License Enforcement, see here.

Multi-tenancy and Organizations

Multi-tenancy enables you to manage multiple groups of devices (Organizations) within a single installation. FortiSIEM provides logical separation between Organizations at an application layer. The users of one Organization cannot see another Organization’s data, which includes devices, users and logs.

You have to choose the Service Provider Installation type when you first install FortiSIEM. Organizations can be defined in two ways:

- *By adding a Collector to an Organization* – all devices sending logs to a Collector or all devices monitored by a Collector are automatically assigned to the Organization to which the Collector belongs. Device Names and IP Addresses can overlap between two Organizations. This situation can be used to model Remote Managed Service Providers.
- *By assigning IP ranges to Organizations* – there are no Collectors and devices will be discovered from Supervisor node and send logs to Supervisor or Worker nodes. If the IP addresses of ALL interfaces of a device are wholly included within the IP range for an Organization, then the device is assigned to that Organization. Else, the device is assigned to the Super/Local Organization (see below).

In addition to user-defined Organizations, FortiSIEM creates two Organizations for ease of management:

- **Super/Local Organization** – this can be used to model a Service Provider’s own network.
  - For Organizations with Collectors, if a device sends logs directly to Supervisor or Worker nodes or is discovered from the Supervisor node, then it belongs to the Super/Local Organization.
  - For Organizations without Collectors, if all the IP addresses of a device (being discovered or sending logs) are not wholly included within the IP range for any Organization, then that device is assigned to the Super/Local Organization.
- **Super/Global Organization** – this is a virtual Organization that can 'see' all the other Organizations. This is useful for Service Provider administrative users.

FortiSIEM Multi-tenancy principles are as follows:

1. Users belonging to Super/Global Organization can see other organizations and their data.
2. Users belonging to Super/Local Organization and user-defined Organizations can only see their own Organization.
3. Devices and events are automatically tagged by FortiSIEM with the Organization Id and Name.
4. Rules can be written at a Global level or for a specific Organization. Incidents trigger when rule conditions are met and they trigger independently for each organization. Each Incident is labeled with Customer Id and Name.
5. Searches/Reports can be executed from Super/Global Organization for any combinations of Organizations.
6. From a specific user-defined Organization or Super/Local Organization, Searches/Reports can run on that Organization.
7. Viewing Incidents is simply a specific Search and follows the same principles as specified in 5 and 6.

Role-based Access Control

After installation, FortiSIEM automatically creates an admin user with Full Admin rights for Super/Global and Super-/Local Organization. When the user creates a new Organization, FortiSIEM creates an admin user for that Organization. These are accounts with Full Admin rights. FortiSIEM users with Full Admin rights can create Roles and then create users and assign them a role.

A FortiSIEM role is based on the following aspects:

- What the user can see:
  - Restrict GUI visibility by hiding parts of the GUI
  - Restrict some Organizations for Service Provider installations
  - Restrict data by writing filters on device type, event type and any parsed event attribute
- What the user can do:
  - Restrict or even hide Admin tab where most of the configuration takes place
  - Restrict any other GUI tab
  - Restrict write capability on certain parts of the GUI

FortiSIEM has a few built-in roles that the users can customize to meet their own needs.

Discovery and CMDB

Discovery is a key differentiator for FortiSIEM as it enables users to seamlessly discover their infrastructure (the 'truth') and auto-populate the CMDB, which can then be used to facilitate analytics.

Discovery can be of two types:

- **Simple LOG discovery** – FortiSIEM has mappings for device type to parse logs for all its in-built log parsers. When it sees a log that matches a parser, it associates the corresponding device type to that device and creates a CMDB entry.
- **Detailed device discovery** – LOG discovery is very basic since only the Vendor and Model can be guessed (for example: Cisco IOS, Fortinet FortiGate, Microsoft Windows, Generic Linux). It is not possible to deduce more details about the device, for example: Operating System version, hardware model, installed patches, installed software, running processes, network device configurations, interfaces, monitor-able performance metrics, etc. In addition to discovering all of the above, FortiSIEM can also discover certain inter-device relationships, for example, Virtualization Guest to Host mappings, WLAN AP to Controller mappings, Multi-context device to physical device mappings, network topology etc. Devices in the AWS Cloud and MS Azure Cloud can be discovered as well.

Discovered information is used to automatically populate a CMDB. As new devices get added or deleted from the infrastructure, scheduled rediscoveries can keep FortiSIEM CMDB up to date. The user can also define some rules to map certain groups of devices to certain CMDB device groups.

The key advantages of FortiSIEM Discovery and CMDB are as follows:

1. The customer has an *accurate picture of the infrastructure* and its relationships from a simple discovery. If a new rogue device is added to the network, FortiSIEM rediscovery learns immediately of the new device and can send an alert of this potential security issue. If an inadvertent configuration change to a key file is made, FortiSIEM rediscovery or configuration monitoring also detects and alerts.
2. *Performance and availability monitoring is automated* since FortiSIEM simply learns what can be monitored and starts monitoring immediately. This approach eliminates human error from the process.
3. *Certain key CMDB Objects such as Business Services can remain up to date against infrastructure changes* as they can be auto-populated by discovery.
4. *CMDB Objects make rules and reports easy to create*. First, no long explicit list of IP addresses or host names are needed for rules or reports. Secondly, rules do not need to be rewritten as devices get added or deleted.
5. *Discovery enables configuration change detection* for both day-to-day changes and changes to golden versions.

Windows and Linux Agents

Some logs and performance metrics can be collected remotely from Windows servers via WMI and by running the Winexe command. Some key performance metrics and file monitoring on Linux servers can be done via SSH. However, the following limitations exist:

For Windows Servers:

- Not all metrics can be collected from a FortiSIEM Linux platform via WMI (for example: Sysmon, Generic Event Logs in the Event Log navigation tree, Registry changes). WMI can be used to collect only Windows Event logs.
- *File Integrity Monitoring Data collected via Windows Security logs is very verbose* (~8 logs per file operation) and creates unnecessary noise in FortiSIEM.
- Remotely running *some programs such as Winexe start services on the servers* may trigger security alerts in certain environments.
- A domain account is required to collect certain logs. A regular account does not provide all logs.
- WMI Service often creates CPU load on the servers when a large number of logs are pulled via WMI.

- *Collecting logs via polling from thousands of servers is not efficient.* If a server is not responsive or slow, you have to wait for the connection to timeout and this wastes resources.

Linux Servers send log via syslog. However, if you want to collect File Integrity Monitoring Data, then a certain configuration is required for this to be done remotely.

Agents provide a clean and efficient way to collect exactly the data that is needed. FortiSIEM Agents are very lightweight and do not consume more than 5% of system CPU and memory. FortiSIEM Windows Agents have the following functionality:

- Collect any Windows Event log including Security, Application and Performance event logs, DHCP/DNS logs, Sysmon logs, etc.
- Collect Custom log files
- Detect registry changes
- Detect File read, write and edits (FIM) with added user context
- Run any PowerShell command and send the output as logs – this allows users to capture any data at periodic intervals and send it to FortiSIEM.
- Detect removable media insertion, deletion, read and write

FortiSIEM can manage a large number of FortiSIEM Windows Agents using configuration templates. The user needs to create a template and associate it with servers. Windows Agents can be configured to send logs to FortiSIEM collectors in a round robin fashion. If one collector is not available, the Agent can send it to the next Collector in the list. This provides a robust and scalable way to collect logs from a large number of servers.

Linux Agents can be used to detect file reads, writes, and edits (FIM functionality) with added user context.

Business Services

A Business Service provides a collection of devices and applications serving a common business purpose. You can define a Business Service in FortiSIEM either manually or by the Dynamic CMDB Group framework that adds it to the Business Service once a device matching certain criteria appears in CMDB.

The primary objective of a Business Service is to assist in incident triage. Once a Business Service is defined, every incident is tagged with the impacted Business Services. A Business Service dashboard provides a top-level Incident-centric view of Business Services. The user can take care of incidents for critical Business Services and ensure that they stay up.

Parsers and Monitors

The ability to parse any log to any depth is a key SIEM functionality. FortiSIEM comes inbuilt with over 2,500 event attributes, 175,000 event types and 250 parsers for various device types and applications. In addition, it has a flexible GUI based framework for customers to enhance existing log parsers, and create completely new device types, event attributes, event types and log parsers. The user can test parser changes on a live system and apply them to become effective immediately on all nodes – so changes take effect without any downtime. Parsers can also be exported out of one system and imported into another system. In Service Provider environments, a parser change can be created at a global level and deployed to all organizations.

FortiSIEM also comes with a number of built-in performance monitors and configuration pulling scripts for device types and applications. Discovery automatically enables the applicable monitors and the user can adjust some parameters, such as polling intervals. Similar to log parsers, the user can create and test performance monitors on a live system and apply them to become effective immediately on all nodes – so changes take effect without any downtime. Performance Monitors can also be exported out of one system and imported into another system.

FortiSIEM tracks changes to installed software and network device configuration. If a new configuration file needs to be monitored and can be obtained via a script, then the user can add them to the system. FortiSIEM monitors changes from a current version to a previous version, deviation from a blessed file, and changes between running config and startup config for certain devices.

Entity Risk Score

FortiSIEM displays devices and users (entities) ranked by risk, providing entity risk scores in Risk View. An entity risk score is calculated based on triggering incidents using a proprietary algorithm that incorporates asset criticality, incident severity, frequency of incident occurrence, and vulnerabilities found. In addition, scores are color coded to quickly identify high risk (red), medium risk (yellow) and low risk (green), and also show occurrence trends, such as whether a risk has gone up or down. Each entity can be selected to show a more detailed risk score trend, along with timeline incident data.

User Identity and Location

FortiSIEM creates an Audit trail of User Identity and Location data in real time by associating a network identity (for example: an IP address, or MAC address) to user identity (for example: a user name, computer name, or domain or Cloud logon) and tying that to a location (like a wired switch port, a wireless LAN controller, or VPN gateway or geo-location for VPN logins). The associations are generated by piecing together various pieces of information from Windows Active Directory events, DHCP events, WLAN and VPN logon events and various Cloud service logon events, with discovery results.

FortiSIEM Supervisor and Worker nodes collaborate in a distributed manner to create User Identity and Location records. The IdentityWorker module on Worker nodes keep a partial User Identity and Location in-memory database based on the events that they see. Whenever the IdentityWorker module on a specific Worker sees new information, for example: a new IP address to User association, it updates the database and communicates to the IdentityMaster module on the Supervisor node. The global User Identity and Location database is created by the IdentityMaster module on the Supervisor node by combining information from all IdentityWorker modules. Whenever the IdentityMaster module sees new information, it sends a signal to parser modules in all nodes, which then gets the latest updates from the Supervisor node. The parser module injects IP to User meta-data into events in real time so that this information can be searched without complicated database join operations.

Searches, Reports and Compliance

FortiSIEM provides a unified way to search the data it collects from various devices. All data whether it is system logs, performance metrics, or configuration changes, is converted to an event with parsed event attributes to make it easy to search.

Searches can be done for real-time data or historical data. In real time mode, search occurs in a streaming node on incoming data without touching the event database. In historical mode, the user specifies a time period and data residing in the event database is searched for that time period. Searches can be specified on raw logs or parsed attributes. A rich variety of grouping and aggregation constructs are supported to display data at various granularity. The raw log data is saved into the same event database as the parsed attributes and any attributes added via enrichment are also added to the event and stored in the event database.

FortiSIEM comes pre-built with a large number of reports that can be used as starting points. The user can customize these reports and save them as their own reports for later use. Reports can be scheduled to run at specified times and be delivered in various formats, such as PDF and CSV, via email. FortiSIEM provides a large number of compliance reports, each with reference to specific compliance mandates. To run these reports, the user simply needs to add devices to the specific compliance device group (Business Service) and then run the report.

All searches run in a distributed fashion in FortiSIEM. For deployments with FortiSIEM NoSQL database, the Supervisor node distributes each search query to Worker nodes and summarizes the partial results sent back from the Worker nodes. Assuming you have sufficient NFS IOPS, searches can be made faster up by adding Worker nodes. Worker nodes can be added to a live system. Since event data is centrally stored in NFS, newly added Workers can participate in queries.

For deployments with Elasticsearch, the Supervisor node sends each search query to the Elasticsearch Coordinating node, which then distributes each search query to Elasticsearch Data Node and summarizes the partial results sent back from the Data Node to the Supervisor node. Adding Elasticsearch Data Nodes can make up searches faster. Since each Data Node has its own storage, it takes some time for data to be distributed to the newly added Data Node. However, since data is stored locally on each Data Node, this solution scales horizontally.

Rules and Incidents

Rules detect bad behavioral anomalies for machines and users in real time. FortiSIEM has developed SQL-like XML based rule specification language. The user creates a rule from the GUI, tests it using real events, and then deploys the rule. The XML language is quite powerful and uses CMDB Objects (e.g. Device, Network and Application Groups, Event Type Groups, Malware Objects, Country groups, Watch Lists) to keep the rules concise.

A rule specification involves multiple sub-patterns of events connected by temporal operators (AND, OR, AND NOT, FOLLOWED BY, and NOT FOLLOWED BY). Each sub-pattern is like a SQL Query with filters, group by attributes and thresholds on aggregates. The thresholds can be static or dynamically specified based on statistics. A rule can be nested, meaning a rule can be set to trigger another rule. A rule can also create a watch list that, like a CMDB Object, can be used in another rule.

Rule computation happens in a streaming mode using distributed in-memory computation involving Super and Worker nodes. Latest rule definitions are distributed to Super and Worker nodes. Worker nodes evaluate each rule based on the events it sees and periodically sends partial rule results to the Supervisor node. The Supervisor node keeps the global rule state machine and creates an incident when rule conditions are met. When a rule involves a statistical attribute (for example: mean or standard deviation), a baseline report is created which computes the statistics and updates the rule conditions. The baseline report also runs in a streaming mode using in-line distributed computation. When a CMDB Object changes, an App Server module on the Supervisor node sends a change signal to the Worker nodes, which then downloads the changes. This distributed in-memory computation enables FortiSIEM to scale to near real time performance with high EPS and a large number of rules.

Since FortiSIEM analyzes all data including logs, performance and availability metrics, flows and configuration changes, the rule engine can detect suspicious behavior. This ability to cross correlate across different functional IT domains is what makes the FortiSIEM rule framework powerful.

Incident Notification Policy

Once an incident triggers, the user may want to take an action, for example: send an email, create a ticket or initiate a remediation action. Rather than attaching an action to an incident, which does not scale, FortiSIEM takes a policy-based approach. You can write Incident Notification policies involving Time Of Day, Incident Severity, Affected Items, and Affected Organization and attach actions to policies. This allows you to create corporate wide policies on who works on what and on which time of day. Affected items are specified using CMDB Groups and Assigned Users can be specified using CMDB Users – this makes incident notification policies easy to specify and maintain.

Remediation Library

You may want to remediate an incident by running a script. In FortiSIEM, this amounts to creating an Incident Notification Policy and attaching the Remediation Script as an Action to the Notification Policy. The remediation script may run on the Supervisor node or on the Collectors since the enforced devices may be behind a firewall.

When an incident triggers and a Remediation Action has to be taken, the App Server sends a signal to the involved enforcement points (Supervisor and Collectors). The enforcement point first retrieves necessary information (such as enforced on device IP or Host name, enforced on device credentials and incident details) from the Supervisor node and passes that information to the Remediation Script. After the script executes, the Remediation results are attached to the Incident.

FortiSIEM provides a wide collection of inbuilt Remediation Scripts. The user can create new Remediation Scripts in FortiSIEM.

External Ticketing System Integration

This feature allows you to manage a FortiSIEM incident in an external ticketing system. Several API based built-in integrations are available – ServiceNow, Salesforce and ConnectWise. A Java based framework is available for the user to create integrations to other ticketing systems.

There are four types of integrations available – Device or Incident and Inbound or Outbound.

- *Incident Outbound Integration* is used to create a ticket in an external ticketing system.
- *Incident Inbound Integration* is used to update the external ticket status in FortiSIEM of a ticket opened previously using Incident Outbound Integration. If a ticket is closed in external ticketing system, the ticket status is also updated in FortiSIEM.
- *Device Outbound Integration* is used to update CMDB in an external ticketing system from FortiSIEM CMDB. Every ticketing system needs a CMDB.
- *Device Inbound Integration* is used to update FortiSIEM device attributes from an external CMDB.

To use built-in *Incident Outbound* and *Device Outbound Integrations*, define an appropriate integration and attach it as an Action to an Incident Notification Policy. You can use extensive field mappings to customize how the ticket will appear in the external ticketing system. Incident Inbound and Device Inbound integrations have to be scheduled to run at periodic intervals.

Dashboards

FortiSIEM offers various types of dashboards for the user to understand the data it collects and the incidents that are triggering in the system:

- Summary Dashboards
- Widget Dashboards
- Business Service Dashboards
- Identity and Location Dashboards
- Incident Dashboards
- Interface Usage Dashboards
- PCI Logging Dashboards

Summary Dashboards

Summary dashboards show a near real time view of health, up-time, incidents and other key performance metrics of many devices in a single spreadsheet format – each row is a device and each column is a metric. Cells are color-coded (Red, Yellow, Green) to highlight the values when they cross certain customizable limits. The advantage of this type dashboard is that user can simultaneously compare many metrics of many devices from a single view and instantaneously spot issues. The user can customize the groups of devices and the corresponding metrics. Additionally, the user can build multiple Summary dashboards. FortiSIEM has developed an in-memory database that powers this dashboard – continuous querying event database does not scale. For more information, see Summary Dashboards.

Widget Dashboards

Widget dashboards offer the more traditional Top N dashboard view – one chart for one metric. A wide variety of chart types are available and are described in FortiSIEM Charts and Views.

Any FortiSIEM Report – whether it is reported on Events or on CMDB – can be added to a Widget dashboard. FortiSIEM Widget Dashboards have these distinct advantages.

- Color Coding – Items in each widget can be color coding based on thresholds – this can quickly help the user to spot problems
- Dynamic Search – The user can filter the entire dashboard by Host Name or IP Address to quickly locate what they're searching for
- Streaming Computation – The reports in the widget dashboard are computed in a streaming mode without making repeated queries to the event database. This makes the dashboards fast to load.

For more information, see Widget Dashboards.

Business Service Dashboards

Business Service Dashboards provide a top-down view of Business Service health. The user can see the incidents related to each Business Service and then drill down on the impacted devices and incidents. For more information, see Business Service Dashboards.

Identity and Location Dashboards

Identity and Location dashboards provide a tabular view of network identity to user identity mappings. For more information, see Identity and Incident Dashboards.

Incident Dashboards

FortiSIEM provides two Incident Dashboards – Overview and Risk View.

- The Overview dashboard shows a top-down view into Incidents By Category, Top Incidents and where they are triggering, and Top Impacted Devices and what Incidents they are triggering.
- The Risk View dashboard organizes devices and users by Risk.

For more information, see Overview and Risk View.

Interface Usage Dashboards

This dashboard provides an overview of individual interface usage for Router and Firewall devices. You can obtain metrics at three levels:

device level, interface level and application level. For more information, see Interface Usage Dashboards.

PCI Logging Dashboards

A PCI Logging Status dashboard provides an overview of which devices in PCI are logging. The devices are displayed by CMDB Device Groups (for example Windows, Linux, Firewalls and so on) and by Business Units. For more information, see PCI Logging Dashboards.

Getting Started

Following are the basic steps for getting started with FortiSIEM:

Step 0 - Pre-Install Considerations

FortiSIEM can run in the following modes:

- Single node all in one Virtual Appliance (Supervisor node) running on a wide variety of Hypervisors with local event database storage
- Virtual Appliance Cluster – Supervisor and Worker nodes - external event database storage
- Dedicated hardware appliances – single node with local event database storage or cluster with external event database storage

Before starting the installation process, make the following decisions:

- Installation type: Hardware appliance or Virtual appliance
- If Virtual Appliance, then decide:
  - Hypervisor type – ESX, KVM, Hyper-V, AWS, Azure, Nutanix, Google Cloud Platform
  - Enterprise version or Service Provider version
  - Single node (All-in-one Supervisor) or a Cluster (single Supervisor and multiple Workers)
  - Local event database or External storage (cluster requires external storage)
  - External storage type - FortiSIEM event database or Elasticsearch
  - Whether Collectors are needed
- If hardware appliance, then decide:
  - Enterprise version or Service Provider version
  - Single node (All-in-one Supervisor Appliance) or a Cluster (single Supervisor Appliance e.g. 3500F and multiple Workers e.g. 2000F)
  - Local event database or External storage (cluster requires external storage)
  - External storage type - FortiSIEM event database or Elasticsearch
  - Whether Collectors are needed

Step 1 - Install the Virtual or Hardware Appliance

You can choose to use all-in-one FortiSIEM Hardware Appliance or a Virtual Appliance based solution.

To install FortiSIEM Hardware Appliance (FSM-2000F, FSM-2000G, FSM-3500F, FSM-3500G, FSM-500F, FSM-500G), see here.

To install a FortiSIEM Virtual Appliance based solution:

- Select the hypervisor (VMWare ESX, AWS, Azure, Hyper-V, KVM, Nutanix, Google Cloud Platform) on which FortiSIEM is going to run
- Select event database storage – local or NFS or Elasticsearch or ClickHouse.
  Note: ClickHouse is recommended for most deployments. Please see ClickHouse Reference Architecture for more information.
- Set up external storage if needed: NFS and Elasticsearch
  See *NFS Storage Guide* and *Elasticsearch Storage Guide*
- Install FortiSIEM Virtual Appliance (see the installation guides here.)

Step 2 - Install License

Apply the license provided by Fortinet. Note that for Virtual appliance install, the UUID of the Supervisor node must match the license while for hardware appliance, the hardware serial numbers must match the license.

After applying the license, the system will reboot and provide a login page.

Login with the following default values:

- **USER ID** - admin
- **PASSWORD** - admin*1
- **CUST/ORG ID** - super
- **DOMAIN** - LOCAL

For more information about FortiSIEM Licensing, see the *Licensing Guide* here.

Step 3 - Specify Event Database Storage

If you chose Virtual Appliances, then specify storage option (see here – **ADMIN** > **Setup** > **Storage**).

Hardware appliances only support local disk event database storage.

Step 4 - Check System Health and License

Ensure that:

- All the system components are up and in good health (**ADMIN** > **Health** > **Cloud Health** – see here)
- The license matches your purchase by visiting the **ADMIN** > **License** > **License** page – see here

Step 5 - (Optional) Create Organizations for Service Provider Deployments

A Service Provider would consist of multiple Organizations.

These Organizations can be defined in two ways:

- **Case 1** - By associating one or more collectors to an Organization – any log received by those Collectors or any devices discovered by those collectors will belong to that Organization. This typically makes sense for remote management scenarios.
- **Case 2** - By associating an IP range to an Organization – this typically makes sense for hosted scenarios

In both cases, create organizations by visiting **ADMIN** > **Setup** > **Organizations** (see here).

The system will create default system users with Full Admin functionality for each created organization.

Step 6 - (Optional) Check Full Admin Organization Users for Service Provider Deployments

FortiSIEM will automatically create a Super-global Full Admin user and one Full Admin user for each Organization. Ensure that you are able to log in to:

- each Organization using the system created Full Admin users
- Super-Global mode using Super-global Full Admin user and then switch to any Organization

Step 7 - Add Email Gateway

FortiSIEM will send notifications for incidents via email. Setup the email gateway by visiting **ADMIN** > **Settings** > **System** > **Email** (see here for details).

Step 8 - (Optional) Add Collector

If your monitored devices are behind a firewall or in a distant location across the Internet, then you will need a Collector to collector to collect logs and performance metrics from that location.

FortiSIEM Collectors can be Hardware Appliances or Virtual Appliances. Hardware Appliances are easiest to install.

- For FSM-500F

See *500F Collector Configuration Guide* for the installation above.

Install the FortiSIEM Collector Virtual appliance based on the Hypervisor of your choice:

- VMWare ESX
- AWS
- Azure
- KVM
- Microsoft Hyper-V
- Nutanix
- Google Cloud Platform

See the specific Installation Guides here for the installations above.

Register the Collector to the FortiSIEM Supervisor node.

See the section *Registering Collectors* for the registration process.

Step 9 - (Optional) Set Event Upload Destination for the Collector(s)

You must specify the FortiSIEM nodes where the Collector will upload events to, in **ADMIN** > **Settings** > **System** > **Worker Upload** (see here). There are three options:

- In a simple setup with one Supervisor node, specify the Supervisor node. This is not recommended in larger setups as this will make the Supervisor node busy.
- You may want to specify one or more Worker nodes, listed by Worker IP addresses. The Collectors will load balance across the specified Worker nodes. In this manner, streaming analytics like inline reports and rule are distributed over Worker nodes.
- You may specify a load balancer name that sits in front of the Worker nodes. Note that in this case, you have to carefully tune the load balancing configuration to get optimum performance.

The second option works the best in most cases.

Step 10 - (Optional) Check Collector Health

You want to make sure that Collectors are up and running properly. Go to **ADMIN** > **Health** > **Collector Health** to check (see here for details).

At this point, the system is ready to receive events or perform discovery.

Step 11 - Receive Syslog and Netflow

First check the list of supported devices whose logs are parsed by FortiSIEM out of the box. The list is **ADMIN** > **Device Support** > **Parsers**. See also the external device support document for further details (see here). If your device is in that list, then FortiSIEM will likely parse your logs out of the box.

Note that with every new version, vendors add new log types or sometimes, even change the log format in a non-backward compatible manner. In that case, the built-in parser may need to be adjusted (this topic will be covered in Advanced Operations). If your device is not on the list of built-in parsed devices, then a custom parser needs to be written. This topic will be covered in Advanced Operations.

Configure your device to send logs to FortiSIEM. If your device is behind a Collector, then the logs will be sent to the Collector. Otherwise, logs can be sent to Supervisor or Worker node. For devices with high event rates, it is recommended to add a Worker node (Step 19) and send logs directly to Worker node. Most vendors have straightforward methods to send syslog to external systems – see here but be aware that the information may be a little out of date. Consider your vendor's manual in that case.

FortiSIEM automatically receives Netflow variations of well-defined ports.

Step 12 - Check CMDB Devices and Run Searches for Received Events

If the logs in Step 11 are received correctly in FortiSIEM, then you should see the sending devices in the correct CMDB device and application group.

You can also search for the logs and see how they are parsed. Go to **ANALYTICS** > **Shortcuts** from the folder drop-down and run 'Raw Messages', 'Top Reporting Devices' or 'Top Event Types' queries (see here for details).

Step 13 - Discover Devices

Some systems (for example, Linux based servers) have generic log patterns – so logs cannot precisely identify the Operating system. If you want to get accurate information from such systems, then you must discover them via protocols such as SNMP, SSH. For Windows servers, if you want to collect logs via WMI, then you must discover them via WMI only or SNMP and WMI.

To perform discovery first go to **ADMIN** > **Setup** > **Credentials** and set up credentials and then go to **ADMIN** > **Setup** > **Discovery** and run discoveries. For Service Provider deployments with collectors, do the discoveries from each organization because IP addresses and names can be overlapping.

You can run the discovery in the foreground or in the background. If you run in the foreground, then you will know when it finishes. If you run in the background, then you must go to Tasks section to see the discovery completion percentages and status. Note that ill-defined discoveries can take a long time to complete – see here for guidelines.

To see the benefits of discovery, see the *External Systems Configuration Guide* here and search your device type.

Step 14 - Check CMDB and Performance Monitors for Discovered Devices

After discovery is complete, you will see the CMDB populated with the discovered devices in the correct device, application and network segment folders.

Note the following:

- If the number of devices is within your license limits, then the discovered devices will be in managed and Pending state. Otherwise, a set of (randomly chosen) devices exceeding license limit will be in the Unmanaged state. FortiSIEM will not receive logs from unmanaged devices, nor they can be monitored. You can flip a device from Unmanaged to Managed and vice-versa. You can also buy additional licenses to rectify this situation.
- If devices have overlapping IP addresses, then they will be merged. Check for this incident “PH_RULE_DEVICE_MERGED_OVERLAP_IP” to look for merged devices. To correct this situation, you have two choices:
  - Change the overlapping IP address on the device, delete the device from CMDB and rediscover.
  - If the overlapping IP is a Virtual IP (VIP), then add this IP to the VIP list in **ADMIN** > **Settings** > **Discovery**. Delete the device from **CMDB** and re-discover.

After you have corrected the situation, make sure that devices are not merged and appear correctly in **CMDB**.

Note that in the enterprise mode, discoveries are done by the Supervisor node. In the Service Provider version, there are two possibilities, depending on how organizations are defined (see Step 5)

- For Organizations defined by IP addresses, discoveries are done by the Supervisor node. After discovery, the devices should belong to the correct organization.

  - If all interfaces of a device belong to the specified Organization IP range, then the device belongs to that Organization.
  - On the other hand, if at least one IP does not belong to specified Organization IP range, then the device belongs to the Super/local Organization (representing the Hosting Service Provider Organization).
- For Organizations with Collectors, discoveries are done by the associated Collector node. Check **CMDB** to see that the devices are marked with the correct Organization and Collector.

As part of discovery, FortiSIEM also discovers which performance metrics it can collect and which logs it can pull. See **ADMIN** > **Setup** > **Pull Events** and **ADMIN** > **Setup** > **Monitor Performance** tabs (see here for details). You can turn off log/performance metric collection or tune the polling intervals.

Performance monitoring and log collection is a continuous process. If you tested the credentials before running discoveries (**ADMIN** > **Setup** > **Credentials** > **Test Connectivity**) and fixed the errors showing up in Discovery error tab, then the metric/log collection should not have errors. After running for some time, there can be errors – some reasons being (a) network connectivity issues from FortiSIEM to the devices, (b) someone changed the credentials or access policies on the device, (c) the device can have performance issues. Please check for errors in the **ADMIN** > **Setup** > **Pull Events** and **ADMIN** > **Setup** > **Monitor Performance** tabs (see here for details) and fix them. If credentials have changed, then you must change the credentials in **ADMIN** > **Setup** > **Credentials** and rediscover the corresponding devices.

Step 15 - Check Monitored Device Health

You can watch the current health of a device in CMDB by selecting the device and choosing the Device health option from the menu. To see the performance metrics in real time, select the device in CMDB and choose the Real time performance option from the menu.

Step 16 - Check Incidents

FortiSIEM provides a large number of built-in machine and user behavior anomalies in the form of rules. These rules are active by default and will trigger incidents. See here on how to navigate incidents. Advanced Operations describes how to tune these rules for your environment.

Step 17 – Notify an Incident via Email

You may want to notify users via email when an incident trigger. This is achieved in one of two ways.

- Create an Incident Notification Policy and specify the incident matching criteria and the receiver email address. See here for details.
- Select an incident from **INCIDENTS** > **List** view, go to **Actions** and select **Notify via Email**. See here for details.

Note that many other advanced actions are possible such as:

- Customizing the email template
- Remediating the incident by running a script
- Opening a ticket in an external ticketing system and so on.

See Advanced Operations for details.

Step 18 – Create a Ticket in FortiSIEM

You can use FortiSIEM built-in ticketing system to handle tickets. Currently, this is handled outside of the notification policy concept (Step 17).

To create a FortiSIEM ticket, select one or more incidents from **INCIDENTS** > **List** view, go to **Actions** and select **Create Ticket**.

Step 19 - View System Dashboards

FortiSIEM provides several built-in dashboards:

- Incident Dashboard – Overview and Risk View
- Incident Location View - (see here for details)
- Incident and Location Dashboard – select **DASHBOARD** > Incident and Location Dashboard (this requires you to collect DHCP, Active Directory logon events – see here for details

Go to **DASHBOARD** and select the dashboard of your choice.

Step 20 - (Optional) Add Worker

For larger software based deployments that involve multiple collectors or large number of monitored devices or devices with high event rates, it is highly recommended to deploy one or more Workers to distribute the Supervisor node's workload. Note that Workers cannot be added to Hardware-based appliances.

Workers can be added by visiting **ADMIN** > **License** > **Nodes** - see here for details.

After adding the Worker(s), remember to add the workers to the collect event upload destination list (**ADMIN** > **Settings** > **System** > **Worker Upload** - see here for details).

Step 21 - (Optional) Check Worker Health

Check the health of the Workers by visiting **ADMIN** > **Health** > **Cloud Health**.

- The health of all nodes should be Normal, load average should be within bounds (typically less than the number of cores), CPU should not be pegged at 99%, and little swap should be used.
- Click on any node and check the health of individual processes running on that node in the bottom pane. Status should be Up with large Up times and reasonable CPU and memory usage.

Step 22 - Check License Usage

Check whether the system is operating within licensed parameters (Monitored device count and EPS) by visiting **ADMIN** > **License** > **Usage** (see here for details).

Step 23 - Set Home Page and Complete Your User Profile

Click the **User Profile** icon (🪪) in the upper right corner of the UI. The dialog box contains three tabs:

Basic - Use the **Basic** tab to change your password into the system.

Contact - Use the **Contact** tab to enter your contact information.

UI Settings - Use the **UI Settings** tab to set the following:

Settings	Guidelines
Home	Select the tab which opens when you log in to the FortiSIEM UI.

Settings	Guidelines
Incident Home	Select the Overview, List, Risk, or Explorer display for the **INCIDENTS** tab.
Dashboard Home	Select the Dashboard to open by default under the **DASHBOARD** tab from this drop-down list.
Dashboard Settings	Select the type of dashboards to be visible/hidden using the left/right arrows. The up/-down arrows can be used to sort the Dashboards.
Language	Specify which language will be used for the UI display. Many UI items have been translated into the languages in the drop-down list, including buttons, labels, top-level headings, and breadcrumbs. Items that are data-driven are not translated.
Theme	Select Dark or Light theme for FortiSIEM UI. Save and refresh the browser to view the change.

Step 24 - Log On to the Console and Check Status

In rare situations when the GUI is not responding, you may need to SSH in to the system console of Supervisor, Worker and Collector nodes and issue some commands. The list of node IP addresses are available in **ADMIN > License > Nodes**, **ADMIN > Health > Cloud Health** and **ADMIN > Health > Collector Health**.

You can login as root for the first time using the password: `ProspectHills`. After the first login, you are forced to change this password.

The following commands are available:

`phstatus`: shows the status of all FortiSIEM processes

`phstatus -a`: shows the detailed status of all FortiSIEM processes along with events per second and local I/O rates

The following Linux commands can be useful:

`top`: shows the CPU, memory usage of all Linux processes

`iostat -x 2`: shows the I/O statistics for local disk

`nfsiostat -x 2`: shows the NFS I/O statistics for Supervisor and Worker for NFS based deployments

`tail -300f /opt/phoenix/log/phoenix.log`: See the C++ module log

Step 25 - Set up Automated CMDB Disk Space Management

If the CMDB disk partition becomes full, then the system may not work correctly. To prevent this from happening, 6.3.2 introduced a CMDB disk space management framework.

Three parameters are introduced in `phoenix_config.txt`.

- `month_retain_limit`: Number of months for which incidents on the Supervisor node should be retained (default value 6 months).

- `cmdb_disk_space_low_threshold` (in MB): When free CMDB disk space falls below this defined threshold, disk management kicks in (default value 50MB).
- `cmdb_disk_space_high_threshold` (in MB): When disk management kicks in, incidents are purged until CMDB disk space reaches this defined threshold (default value 100MB).

Two audit events are introduced.

- `PH_AUDIT_CMDB_DISK_PRUNE_SUCCESS`: This event indicates that free CMDB disk space fell below the low threshold (`cmdb_disk_space_low_threshold`) and old incidents and identity / location data were pruned to bring the free CMDB disk space above the high threshold (`cmdb_disk_space_high_threshold`).
- `PH_AUDIT_CMDB_DISK_PRUNE_FAILED`: This event indicates that free CMDB disk space fell below the low threshold (`cmdb_disk_space_low_threshold`) and in spite of pruning older incidents and identity / location data, free CMDB disk space stays below the high threshold (`cmdb_disk_space_high_threshold`). To remedy this situation, the user must reduce the number of months of incidents and identity / location data in CMDB (`month_retain_limit`).

Two system defined rules are included.

- FortiSIEM: CMDB Disk space low - Prune successful.
- FortiSIEM: CMDB Disk space low - Prune failed to keep free disk space above high threshold.

Adjust the CMDB disk management values if necessary.

Step 26 - Create Retention Policy

After the event database has been set up, if you haven't done so already, you may want to create retention policies to optimize how your storage is managed. To do so, follow the steps in Creating a Retention Policy.

Advanced Operations

FortiSIEM enables you to perform advanced operations for the following:

CMDB Advanced Operations

FortiSIEM enables you to perform the following CMDB advanced operations.

- Discovering Users
- Creating FortiSIEM Users
- Setting Eternal Authentication
- Setting 2-Factor Authentication
- Assigning FortiSIEM Roles to Users
- Creating Business Services
- Creating Dynamic DMDB Groups
- Setting Device Geo-Location
- Creating CMDB Reports

Discovering Users

Users can be discovered via LDAP, OpenLDAP, or they can be added manually. Discovering users via OpenLDAP or OKTA are similar.

To discover users in Windows Active Directory, discover the Windows Domain Controller:

1. Go to **ADMIN** > **Setup** > **Credentials**.
2. Click **New** to create an LDAP discovery credential by entering the following in the Access Method Definition dialog box:
   a. **Name** for the credential
   b. **Device Type** as "Microsoft Windows Server 2012 R2"
   c. **Access Protocol** as "LDAP"
   d. **Used For** as "Microsoft Active Directory"
   e. Enter the **Base DN** and **NetBios Domain**
3. Test the LDAP Credentials.

4. Run discovery.
5. Go to **CMDB** > **Users**.
6. Click the "Refresh" icon on left panel and see the users displayed on the right panel.

To add users manually:

1. Go to **CMDB** > **Users**.
2. Click **New** and add the user information.

For details about Discovering Users, see here (Refer to the table by searching: Credentials for Microsoft Windows Server)

For details about Adding Users, see here.

Creating FortiSIEM Users

To create users that access FortiSIEM:

1. Login as a user with "Full Admin" rights.
2. Create the **user** in CMDB.
3. Set a password – after logging in, the user can set a new password.
4. Select the user and click **Edit**.
5. Select **System Admin** and enter the following:
   a. **Authentication Mode** - "Local" or "External"
   b. **Enterprise case** - select the Role
   c. **Service Provide Case** - select the Role for each Organization

For details about creating users, see here.

To change the password:

1. Login as the user.
2. Click the "User Profile" icon on the top-right corner.
3. Click **Save**.

Setting External Authentication

FortiSIEM users can be authenticated in two ways:

- **Local** authentication – user credentials are stored in FortiSIEM
- **External** authentication – user credentials are stored in an external database (AAA Server or Active Directory) and FortiSIEM communicates with the external database to authenticate the user

Step 1: Set up an Authentication Profile

1. Login as a user with **Full Admin** rights.
2. Create an authentication profile by visiting **ADMIN** > **Settings** > **General** > **External Authentication**.
3. Click **New**.
4. Provide the following information in the External Authentication Profile dialog box:
   a. Enter a Name for the profile
   b. Select an **Organization** from the drop-down list

   c. Set **Protocol** appropriately (for example, LDAP, LDAPS, or LDAPTLS for Active Directory)
   d. Enter the **IP/Host** and **Port** number
5. Make sure the credentials are defined in **ADMIN** > **Setup** > **Credentials**.
6. Select the entry and click **Test** to ensure it works correctly.

Step 2: Attach the Authentication Profile to the user

1. Select the user under **CMDB** > **User** and click **Edit**.
2. Select **System Admin** and click the edit icon.
3. Set **Mode** to "External" and set the Authentication Profile created.

For details about Setting up Authentication Profiles, see here.

For details about Editing Users, see here.

Setting 2-Factor Authentication

FortiSIEM supports Duo as 2-factor authentication for FortiSIEM users:

Step 1: Set up an Authentication Profile

1. Login as a user with **Full Admin** rights.
2. Create an authentication profile by visiting **ADMIN** > **Settings** > **General** > **External Authentication**:
   a. Set **Protocol** to "Duo"
   b. Make sure the credentials are defined in **ADMIN** > **Setup** > **Credentials**
   c. Select the entry and click **Test** to make sure it works correctly

Step 2: Attach the Authentication Profile to the user

- Select the user **CMDB** > **Users** and click **Edit**
- Select **System Admin** and click the edit icon
- Set **Mode** to "External" and set the Authentication Profile created

For details about Setting up Authentication Profiles, see here.

For details about Editing Users, see here.

Assigning FortiSIEM Roles to Users

FortiSIEM allows the admin user to create Roles based on what data the user can see what the user can do with the data. To set up Roles:

Step 1: Create a Role of your choice

1. Login as a user with **Full Admin** rights.
2. Go to **ADMIN** > **Settings** > **Role** > **Role Management**.
3. Make sure there is a Role that suits your needs. If not, then create a new one by clicking **New** and entering the required information. You can also Clone an existing Role and make the changes.

Step 2: Attach the Role to the user

1. Select the user **CMDB** > **Users** and click **Edit**.
2. Select **System Admin** and click the edit icon.
3. Set **Default Role**:
    a. Enterprise case – select the **Role**
    b. Service Provide Case – select **Role** for each Organization

For details about Setting up Roles, see here.

For details about Editing Users,see here.

Creating Business Services

Business Service is a smart grouping of devices. Once created, incidents are tagged with the impacted Business Service(s) and you can see business service health in a custom Business Service dashboard.

For details about creating a Business Service, see here.

For details about setting up Dynamic Business Service, see here.

For details about viewing Business Service health, see here.

Creating Dynamic CMDB Groups and Business Services

CMDB Groups are a key concept in FortiSIEM. Rules and Reports make extensive use of CMDB Groups. While inbuilt CMDB Groups are auto-populated by Discovery, user-defined ones and Business Services are not. You can use the Dynamic CMDB Group feature to make mass changes to user-defined CMDB Groups and Business Services.

To create Dynamic CMDB Group Assignment Rules:

1. Login as a user with **ADMIN** tab modification rights.
2. Go to **ADMIN** > **Settings** > **Discovery** > **CMDB Group**.
3. Click **New**.
4. Enter CMDB Membership Criteria based on **Vendor**, **Model**, **Host Name** and **IP Range**.
5. Select the CMDB group (**Groups**) or Business Services (**Biz Services**) to which the Device would belong if the criteria in Step 3 is met.
6. Click **Save**.

You can now click **Apply** to immediately move the Devices to the desired CMDB Groups and Business Services. Discovery will also honor those rules – so newly discovered devices would belong to the desired CMDB Groups and Business Services.

For details about Setting up Dynamic CMDB Groups and Business Services, see here.

Setting Device Geo-Location

FortiSIEM has location information for public IP addresses. For private address space, you can define the locations as follows:

1. Login as a user with **ADMIN** tab modification rights.
2. Go to **ADMIN** > **Settings** > **Discovery** > **Location**.
3. Click **New**.
4. Enter **IP/IP Range**.

5. Specify the Corresponding **Location** for the IP address Range.
6. Select **Update Manual Devices** if you want already discovered device locations to be updated.
7. Click **Save**.
   You can now click **Apply** to set the geo-locations for all devices matching the IP ranges.

For details about Setting Device Location, see here.

Creating CMDB Reports

If you want to extract data from FortiSIEM CMDB and produce a report, FortiSIEM can run a CMDB Report and display the values on the screen and allows you to export the data into a PDF or CSV file.

For details about Creating CMDB Reports, see here.

Incidents and Cases Advanced Operations

FortiSIEM enables you to perform the following advanced operations:

- Changing the Home Country
- Searching Incidents
- Tuning Incidents via Exceptions
- Tuning Incidents via Modifying Rules
- Tuning Incidents via Drop Rules
- Tuning Incidents by Adjusting Thresholds
- Clearing Incidents
- Adding Comments or Remediation Advice to an Incident
- Remediating an Incident
- Notifying an Incident via Email
- Creating New Rules
- Creating a FortiSIEM Ticket
- Creating a Ticket in External Ticketing System

Additional Incident related information: Automated Incident Resolution Recommendation

Changing the Home Country

Many rules and reports use the My Home CMDB Object as defined in **RESOURCES** > **Country Groups** > **My Home**. By default, it is set to United States of America.

For details on changing this, see here.

Searching Incidents

If you want to search for specific incidents, go to **INCIDENTS** > **List** > **Actions** > **Search**. A Search Windows appears on left. First, select the Time Window of interest. Then by clicking on any of the criteria, you can see the current values. You can select values to see matches incidents in the right pane.

For details about Searching Incidents, see here.

Tuning Incidents via Exceptions

If you do not want a rule to trigger for a specific Incident Attribute, then you can create an exception.

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident (**Actions > Search**) or make sure that Incident shows in the right pane.
3. Highlight the Incident.
4. Click **Actions** > **Edit Rule Exception**.
5. Enter the exception criteria – attribute based or time-based.

For details about Tuning Incidents via Exceptions, see here.

Tuning Incidents via Modifying Rules

Sometimes modifying the rule is a better idea than creating exceptions. For example, if you do not want a rule to trigger for DNS Servers, simply modify the rule condition by stating something like “Source IP NOT CONTAIN DNS Server”. To do this:

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident (**Actions > Search**) or make sure that Incident shows in the right pane.
3. Highlight the Incident.
4. Click **Actions** > **Edit Rule**.
5. Edit the Rule.
   If it is a System Rule, then you must save it as a User Rule. Deactivate the old System Rule and activate the new User Rule.

For details, see here.

Tuning Incidents via Drop Rules

Sometimes the rule can be prevented from triggering by dropping the event from rule considerations. There are two choices - (a) store the event in database but not trigger the rule or (b) drop the event completely.

To do this:

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident (**Actions > Search**) or make sure that Incident shows in the right pane.
3. Highlight the Incident.
4. Click **Actions** > **Create Event Dropping Rule**.
5. Specify event drop criteria and action. Events can be dropped on certain parsed fields (like Reporting/Source/Destination IP and Regex filter on the content).

For details, see here.

Tuning Incidents by Adjusting Thresholds

Some performance rules are written using global thresholds, for example - the Rule “High Process CPU: Server” uses the global threshold “Process CPU Util Critical Threshold” defined in **ADMIN** > **Device Support** > **Custom Property**.

You have two choices – (a) modify the global threshold or (b) modify the threshold for a specific device or a group of devices. If you change the global threshold, then the threshold will change for all devices.

To modify the global threshold, follow these steps:

1. Go **ADMIN** > **Device Support** > **Custom Property**.
2. Select the property and click **Edit**.
3. Enter the new value and click **Save**.

For details, see here.

To modify the threshold for one device, follow these steps:

1. Go to **CMDB**.
2. Select the device and click **Edit**.
3. In the **Properties** tab, enter the new value and click **Save**.
   To modify the threshold for a group of devices, repeat the above step for all devices.

Clearing Incidents

In some cases, the Incident may not be happening anymore as the exception condition was corrected.

To clear one or more Incidents:

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident (**Actions > Search**) or make sure that Incidents show in the right pane.
3. Highlight the Incidents.
4. Click **Actions** > **Clear Incident**.
5. Enter **Reason** and click **OK**.

For details, see here.

Adding Comments or Remediation Advice to an Incident

To add a comment to an Incident:

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident or make sure that Incidents show in the right pane.
3. Highlight the Incidents.
4. Click **Actions** > **Edit Comment**.
5. Enter the **Comment** and click **OK**.

For details, see here.

Sometimes, it is necessary to add Remediation advice for the recipient of an Incident, so he can take some action to remediate the Incident. This has to be done by editing the Rule.

1. Go to **RESOURCES** > **Rules**.
2. Select a Rule and click **Edit**.
3. Enter **Remediation Note** text and click **Save**.

For details, see here.

The Remediation text can be added to the Incident Notification email template.

For details, see here.

Remediating an Incident

You can use the following commands to enable Windows Remote Management (WinRM) and set authentication on the target Windows Servers. See Remediations for information on adding, editing, and deleting a remeditation from the FortiSIEM UI.

In the remediation script:

1. When you initiate the WinRM session, set `transport` parameter to `ssl`.
2. Set the `server_cert_validation` option accordingly. If you do not need to validate the certificate, set to `ignore`.
   For example:
   ```
   session = winrm.Session(enforceOn, auth = (user, password), transport="ssl",
   server_cert_validation = "ignore")
   ```

In the target Windows server:

Note: You might need to disable Windows Firewall before running remediation.

1. Create the self-signed certificate in the certificate store, for example:
   ```
   New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName
   "mySubjectName.lan"
   ```
   where `Cert:\LocalMachine\My` is the location of the certificate store and `mySubjectName.lan` is the subject alternate name extension of the certificate.
2. Create an HTTPS listener, for example:
   ```
   winrm create winrm/config/Listener?Address=*+Transport=HTTPS '@{Port
   ="5986";Hostname="{your host name}"; CertificateThumbprint="{Cer-
   tificateThumbprint}"}'
   ```
3. Start the WinRM service and set the service `startup` type to `auto-start`. The `quickconfig` command also configures a listener for the ports that send and receive WS-Management protocol messages using either HTTP or HTTPS on any IP address.
   ```
   winrm quickconfig -transport:https
   ```
4. Validate the WinRM service configuration and Listener.
   a. Check whether basic authentication is allowed, for example:
      ```
      winrm get winrm/config/service
      ```
   b. Check whether a listener is running, and verify the default ports, for example:
      ```
      winrm get winrm/config/listener
      ```

Remediation can be done either on an ad hoc basis (for example, user selects an Incident that has already occurred to Remediate) or using a Notification Policy where the system takes the Remediation action when Incident happens. First, make sure the Remediation script for your scenario is defined. Check the existing Remediation scripts in **ADMIN** > **Settings** > **General** > **Notification Policy** > Remediation settings. If your device is not in the list, add the needed Remediation script.

To set ad hoc remediation:

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident (**Actions > Search**) or make sure that Incidents show in the right pane.
3. Highlight the Incident you want to remediate (you can remediate only one Incident at a time)..

4. Click **Actions** > **Remediate Incident**.
5. In the **Run Remediation** dialog box:
   a. Select the script in the **Remediation** drop-down list that you want to run.
   b. Select the role that the script will run on from the **Run On** drop-down list.
   c. Open the **Enforce On** drop-down list to choose which devices the remediation script will run on. In the **Run Remediation** dialog box, open the **Device** tree. Select individual devices and shuttle them to the **Selections** column. (You can choose only individual devices; you cannot choose device groups.)
6. Click **Run** in the **Run Remediation** dialog box.

For details, see here.

To set policy-based remediation:

1. Go to **ADMIN** > **Settings** > **General** > **Notification Policy**.
2. Click **New**.
3. Under **Action**, click the edit icon next to **Run Remediation/Script**.
4. In the **Notification Policy - Define Script/Remediation** dialog box click New.
5. In the dialog box tha topens click either **Legacy Script** or **Remediation**:
   - **Legacy Script**:
     - Enter the name and path to the script in the **Script** field.
     - Select the role the script will run on from the **Run On** drop-down list.
   - **Remediation**:
     - Select a remediation script from the **Script** drop-down list.
     - Select the role that the script will run on from the **Run On** drop-down list.
     - Open the **Enforce On** drop-down list to choose which devices the remediation script will run on. In the**Notification Policy - Define Script/Remediation - Enforce On** dialog box, open the **Device** tree. Select individual devices and shuttle them to the **Selections** column. (You can choose only individual devices; you cannot choose device groups.)
6. Click **Save**.

For details, see here.

To see the Notification history of an Incident:

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident (**Actions > Search**) or make sure that Incidents show in the right pane.
3. Highlight the Incidents.
4. Click **Actions** > **Show Notification History**.

For details, see here.

Notifying an Incident via Email

Notifying an Incident can be done either on ad hoc basis (for example - user selects an Incident that has already occurred to notify) or using a Notification Policy where the system takes the notification action when Incident happens.

First, make sure that Email Server has been properly defined in **ADMIN** > **Settings** > **Email** > **Email Settings**.

FortiSIEM has a built-in Incident Notification Email template. If you want a different one, please define it under **ADMIN** > **Settings** > **Email** > **Incident Email Template**.

For details, see here.

To set ad hoc notifications:

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident (**Actions > Search**) or make sure that Incidents show in the right pane.
3. Highlight the Incidents.
4. Click **Actions** > **Notify via Email**.
5. Choose Receive Email Address and Email Template.
6. Click **Send**.

For details, see here.

For Policy based Notification

To send policy-based notifications:

1. Go to **ADMIN** > **Settings** > **General** > **Notification Policy**.
2. Click **New**.
3. Specify the Incident Filter Conditions (**Severity**, **Rules**, **Time Range**, **Affected Items**, **Affected Organizations**) carefully to avoid excessive emails.
4. Under **Action**, click **Send Email/SMS to Target Users**.
5. Enter **Email Address** or Users from CMDB.
6. Click Save.

For details, see here.

To see the Notification history of an Incident:

- Go to **INCIDENTS** > **List** view.
- Search the Incident (**Actions > Search**) or make sure that Incidents show in the right pane.
- Highlight the Incidents.
- Click **Action** > **Show Notification History**

For details, see here.

Creating New Rules

Sometime, you may want to create a new rule from scratch.

For details, see here. Additional Incident related information available in Automated Incident Resolution Recommendation.

Creating a FortiSIEM Ticket

First make sure that:

- Ticket's assigned user is in CMDB
- Assigned user's Manager that is going to handle escalation is in CMDB
- A Ticket Escalation Policy is defined

For adding users see Advanced Operations > Creating System users.

For defining ticket escalation policy, see here.

To create a FortiSIEM ticket:

- Go to **INCIDENTS** > **List** view.
- Search the Incident (**Actions > Search**) or make sure that Incidents show in the right pane.
- Highlight the Incidents.
- Click **Actions** > **Create Ticket**.
- Click **Save**

Note that you can put multiple Incidents on one ticket or add an Incident to an existing ticket.

For details, see here.

Creating a Ticket in External Ticketing System

First, define an Incident Outbound Integration Policy by visiting **ADMIN** > **Settings** > **General** > **External Integration**.

For details, see here.

Then set the Incident Outbound Integration Policy in Notification Policy Action:

1. Go to **ADMIN** > **Settings** > **General** > **Notification Policy**.
2. Click **New**.
3. Specify the Incident Filter Conditions (**Severity**, **Rules**, **Time Range**, **Affected Items**, **Affected Organizations**) carefully to avoid excessive emails.
4. Under **Action**, click **Invoke an Integration Policy**.
5. Choose the Integration Policy.
6. Click **Save**.

For details, see here.

To update external ticket state in FortiSIEM:

1. Define an Incident Inbound Integration Policy by visiting **ADMIN** > **Settings** > **General** > **External Integration**.
2. Select the Policy and click **Schedule** to run the Incident Inbound Integration Policy.

For details, see here.

Device Support Advanced Operations

FortiSIEM enables you to perform the following advanced operations:

Checking Device Monitoring Status and Health

For Performance Monitoring scenarios, you would like to know:

- Is FortiSIEM is able to monitor the devices on time? Is FortiSIEM falling behind?
- Are there monitoring errors?
- What is the current health of monitored devices?

To check whether FortiSIEM is able to collect monitoring data on time:

1. Go to **CMDB**.
2. Search for the device and by typing in a string in the search window.
3. Check the **Monitor Status** column.
4. If Monitor Status Warning or Critical, then select the Device and check the Monitor sub-tab in the bottom pane to find out the reason.

FortiSIEM is an optimized multi-threaded solution. If one node is given too many devices to monitor, each device with many metrics, then it may not be able to keep up. If FortiSIEM is not able to keep up (e.g. polling interval is 1 minute and last poll was 3 minutes ago), then you can do one of the following:

1. Check the Monitored Device resources (CPU, memory) and the network between FortiSIEM and the Monitored Device. Many monitoring protocols such as SNMP, WMI will not operate under WAN type latencies (greater than 10 msec).
2. Increase the polling intervals by visiting **ADMIN** > **Setup** > **Monitor Performance** > **More** > **Edit Intervals**. **Note**: If you increase polling intervals, some performance monitoring rules that require a certain number of polls in a time window may not trigger. Please adjust those rules either by reducing the number of polls or increasing the time window. For example, if a rule needs 3 events (polls) for a 10 min time window with original polling interval as 3 min, the rule will not trigger if polling interval is changed to 4 min or higher. To make the rule trigger again, either reduce the number of events needed (for example, from 3 to 2) or increase the time window (for example, from 10 min to 15 min).
3. Turn off some other jobs by visiting **ADMIN** > **Setup** > **Monitor Performance** > **More** > **Edit Intervals**.
4. Deploy Collectors close to the Monitored Devices or deploy more Collectors and distribute performance monitoring jobs to Collectors by doing re-discovery.

To check for Monitoring errors:

- Go to **ADMIN** > **Setup** > **Monitor Performance** > **More** > **Errors**.

For details see here.

To see current health of a monitored device:

1. Go to **CMDB**.
2. Search for the device and by typing in a string in search window.
3. Choose **Actions** > **Device Health**.

For details, see here.

Setting Devices Under Maintenance

If a device will undergo maintenance and you do not want to trigger performance and availability rules while the device is in maintenance, then

1. Go to **ADMIN** > **Setup** > **Maintenance**.
2. Select the Maintenance Schedule.
3. Select the Group of Devices or Synthetic Transaction Monitors (STM) for maintenance.
4. Make sure the **Generate Incidents for Devices under Maintenance** is checked.

For details, see here

Creating Custom Monitors

Although FortiSIEM provides out of the box monitoring for many devices and applications, user can add monitoring for custom device types or add monitoring for supported device types.

1. Go to **ADMIN** > **Device Support** > **Monitoring**.
2. Click **Enter Performance Object** > **New** and enter the specification of the Performance Object.
3. Select the Performance Object and click **Test**.
4. Click **Enter Device Type to Performance Object Association** > **New** and choose a set of Device Types and associated Performance Objects.
5. Go to **ADMIN** > **Setup** > **Credentials** and enter the Device Credentials for a set of device types specified in Step 4.
6. Go to **ADMIN** > **Setup** > **Discovery** and discover these devices.
7. FortiSIEM will pick the customer monitors defined in Step 2 if the Tests in Step 3 succeeded.
8. Go to **ADMIN** > **Setup** > **Monitor Performance** and see the monitors
   From the same tab, Select one or more devices and Click **More** > **Report** and check whether the monitoring events are generated correctly.

Steps 1-4 are described here.

Steps 5 is described here.

Steps 6 is described here.

Step 8-9 are here.

Setting Important Interfaces and Processes

A network may have hundreds of interfaces and you have may have hundreds of network devices. Not all interfaces may not be interesting for up/down and utilization monitoring. For example, you may only want to monitor WAN links and trunk ports and leave out Access Ports. This saves you lots of CPU and storage. Similar logic applies to critical processes on servers.

Since FortiSIEM discovers interfaces and processes, it is easy to select Critical Interfaces and Processes for Monitoring.

1. Go to **ADMIN** > **Settings** > **Monitoring**.
2. Click **Important Interfaces**> **Enable** > **New** and select the Interfaces.
3. Click **Important Processes**> **Enable**> **New** and select the Processes.

Note that once you select Important Interfaces and Processes, only these Interfaces and Processes will be monitored for availability and performance.

For details, see here.

Modifying System Parsers

If you want to modify a built-in log parser, then do the following steps:

1. Go to **ADMIN** > **Device Support** > **Parsers**.
2. Select a Parser and click **Disable** since you have two parsers for the same device.
3. Select the same Parser and click **Clone**.
4. Make the required modifications to the parser.
5. Click **Validate** to check the modified Parser syntax.
6. Click **Test** to check the semantics of the modified Parser.
7. If both Validate and Test pass, then click **Enable** and then **Save**.
   The modified Parser should show **Enabled**
8. Click **Apply** to deploy the modified Parser to all the nodes.

For details, see here.

Creating Custom Parsers

If you want to create a completely new log parser, then do the following steps:

1. Go to **ADMIN** > **Device Support** > **Parsers**.
2. Parsers are evaluated serially from top to bottom in the list. Select the parser just before the current custom parser and click **New**.
3. Fill in the parser details – **Name**, **Device Type**, test Events and the parser itself.
4. Click **Validate** to check the syntax
5. Click **Test** to check the semantics of the modified parser.
6. If all passes, then click **Enable** and then click **Save**.
   The newly added parser should show **Enabled**.
7. Click **Apply** to deploy the change to all the nodes.

For details, see here.

Handling Multi-line Syslog

When devices send the same log in multiple log messages, you can combine them into one log in FortiSIEM to facilitate analysis and correlation.

1. Go to **ADMIN** > **Settings** > **Event Handling** > **Multiline Syslog**.
2. Click **New** to begin a multi-line syslog handling rule.
3. Enter a **Protocol** – TCP or UDP.
4. Enter a **Begin Pattern** and **End Pattern** regular expressions.
   All the logs matching a begin pattern and an end pattern are combined into a single log
5. Click **Save**.

For details, see here.

Creating Synthetic Transaction Monitors

You can define a Synthetic Transaction Monitor to monitor the health an application or a web service. To do this:

1. Go to **ADMIN** > **Setup** > **STM**.
2. **Step 1: Create a monitoring definition**, click **New** and enter the required fields. When the protocol is HTTP, then a Selenium script can be input. Specify the timeout values for detecting STM failures.
3. **Step 2: Apply the monitoring definition to a host**
4. **Step 3: Make sure it is working correctly** - click **Monitor Status**.

For details, see here.

Mapping Events to Organizations

In most cases, the events received by a Collector is tagged with the Organization to which the Collector belongs. In some cases, events for multiple Organizations are aggregated by an upstream device and then forwarded to FortiSIEM. In this case, FortiSIEM needs to map events to organizations based on some parsed event attribute. An example is the FortiGate VDOM attribute.

This is accomplished as follows:

1. Go to **ADMIN** > **Settings** > **Event Handling** > **Event Org Mapping**.
2. Click **New** to create an Event Org mapping definition.
3. Select a **Device Type** from the drop-down list.
4. Specify the **Event Attribute** that contains the Organization information.
5. Specify the **Collector** that will do this Event Org Mapping.
6. Specify an **IP** or **IP Range**.
7. Specify the mapping rules by clicking the edit icon next to **Org mapping**. In the Event Organization Mapping dialog box, map Event Attribute values to Organizations.

For details, see here.

Adding Windows Agents

FortiSIEM Windows Agents provides a scalable way to collect performance metrics, logs and other audit violations from a large number of Windows servers. Windows Agents (version 3.1 onwards) can be configured and managed from the FortiSIEM GUI. Windows Agent Manager is not required. As long as license is available, you can install Windows Agents and register to the FortiSIEM Supervisor node.

For details about Installing Windows Agents, see the latest Windows Agent Installation Guide.

For details about Configuring Windows Agent in FortiSIEM, see here.

Adding Linux Agents

Starting release 5.2.1, Linux Agent requires a license. Install a Linux Agent and register to the FortiSIEM Supervisor node. As long as the license is available, you can install Linux Agent and register to the FortiSIEM Supervisor node. Linux Agents can be configured and managed from the FortiSIEM GUI.

For details about Installing Linux Agents, see Linux Agent Installation Guide.

For details about Configuring Linux Agent in FortiSIEM, see here.

Forwarding Events to External Systems

Events received by FortiSIEM can be forwarded to external systems. FortiSIEM provides a flexible way to define forwarding criteria and forwarding mechanism such as syslog, Kafka and Netflow.

For details, see here.

Rules, Reports and Dashboards Advanced Operations

FortiSIEM enables you to perform the following advanced operations:

- Creating New Rules
- Creating New Reports
- Scheduling Reports
- Customizing Built-in Dashboards
- Creating Custom Dashboards
- Customizing Business Service Dashboards

Creating New Rules

To create new Rules, go to **RESOURCES** > **Rules**, choose a folder and click **New**. Remember to test and activate the rule.

For details, see here.

Rules can also be created from **ANALYTICS** tab. Once you have run a search, create a rule from it by clicking **Actions** > **Create Rule.**

For details, see here.

Creating New Reports

New Reports can be created from **RESOURCES** > **Reports** > Choose a Folder > Click **New**.

For details, see here.

Reports can also be created from **ANALYTICS** tab. Once you have run a search, you can save it as a Report by clicking **Actions** > **Save as Report**.

For details, see here.

Scheduling Reports

Reports can be scheduled to run at later time and contain data for a specific period of time. Go to **RESOURCES** > **Reports** > Choose a Report > **More** > **Schedule**.

For details, see here.

Customizing Built-in Dashboards

FortiSIEM Built-in Dashboards are organized in Folders with multiple Dashboards in each Folder. You can add dashboards to any Folder or modify the dashboards in any built-in folder. Dashboard modification can include – modifying chart layout, chart settings or even adding new widgets for widget dashboards.

For details, see here.

You can also choose to display only a set of Dashboard Folders by visiting **ADMIN** > **Settings** > **System** > **UI** > **Dashboard Settings**.

Creating Custom Dashboards

You can either create a new Dashboard Folder and move dashboards in it or add dashboards to an existing folder.

To create a new Dashboard folder:

1. Click **DASHBOARD**
2. Open the Dashboard Folder drop-down list.
3. Click **New**.

To create a new Dashboard for the folder:

1. Select the Dashboard Folder from the drop-down list.
2. Click **+** to the right of the selected folder.
3. Enter a **Name** and Dashboard **Type** from the drop-down list in the Create New Dashboard dialog box.
4. If you created a Widget Dashboard, click **+** beneath the folder name to add Widgets to the Dashboard.

For details, see here.

Creating Business Service Dashboards

After creating a new Dashboard, choose Type = Business Service Dashboard. Then select the Business Service Selector on the top right to add Business Services to the Dashboard.

For details, see here.

Advanced Health System Advanced Operations

FortiSIEM enables you to perform the following advanced operations:

- Monitoring System Health
- Monitoring Collector Health
- Monitoring Elasticsearch Health
- System Errors
- Monitoring User and Query Activity

Monitoring System Health

To see the system level health of every FortiSIEM Supervisor/Worker node, go to **ADMIN** > **Health** > **Cloud Health**. The top pane shows the overall health of various nodes – Supervisor and Workers. Click any one node and the bottom pane shows the health of the various processes in that node.

For details, see here.

Monitoring Collector Health

To see the system level health of every FortiSIEM Collector node, go to **ADMIN** > **Health** > **Collector Health**.

For details, see here.

Monitoring Elasticsearch Health

To see the Elasticsearch health information, go to **ADMIN** > **Health** > **Elasticsearch Health**.

For details, see here.

System Errors

To see the system errors, click the **Jobs/Errors** icon on the top-right corner of FortiSIEM GUI and select the **Error** tab. You can also run a report in **ANALYTICS** > click the **Folders** icon > **Shortcuts** > **Top FortiSIEM Operational Errors**.

Monitoring User and Query Activity

To see FortiSIEM User and Query Activity, click the **User Activity** icon (👤) on the top-right corner of FortiSIEM GUI.

The User Activity dialog box contains these tabs:

- Logged in Users
- Locked Users
- Query Status
- Query Workload

All of the tabs in the User Activity dialog box contain the time of the last refresh and the number of seconds until the next automatic refresh. By default, the automatic refresh interval is 60 seconds. To refresh the table on demand, click the **Refresh** button.

Logged in Users

This tab displays a table listing the users currently logged in to FortiSIEM. You can perform the following operations on this tab:

- **Log Out** - Select one or more users in the table and click **Log Out**. The selected users will be logged out of FortiSIEM.
- **Log Out and Lock Out** - Select one or more users in the table and click **Log Out and Lock Out**. The selected users will be logged out of FortiSIEM and prevented from logging back in.

The Logged in Users table contains the following information:

Column	Description
Organization	The Organization to which the user belongs.
User	The name of the user.
Full Name	The full name of the user.
Login IP	The IP address from which the user logged in.
Role	The name of the user's role.
Login Time	The date and time when the user logged in.
Session ID	The ID of the user's FortiSIEM session.

Locked Users

This tab displays a table listing the users currently locked out of FortiSIEM. Typically, user access to FortiSIEM can be locked due to multiple login failures. You can perform the following operations on this tab:

- **Unlock** - Select one or more users in the table and click **Unlock**.

Note: Users can also be unlocked by going to **CMDB > Users > Actions > Unlock**.

The Locked Users table contains the following information:

Column	Description
Organization	The Organization to which the user belongs.
User	The name of the user.
Full Name	The full name of the user.

Column	Description
Login IP	The IP address from which the user logged in.
Role	The name of the user's role.
Locked Time	The date and time when the user was locked out of FortiSIEM.

Query Status

This tab displays a table listing the status of current and recent queries. You can perform the following operations on this tab:

- **Stop Query** - Select a query from the table and click **Stop Query**. The selected query will be stopped remotely. If the query was sent from the **ANALYTICS** page, you should see a warning message saying this query was stopped manually. You should also be able to see the partial results you received before it was stopped.
- **Search** - Click the **Search** button to search for queries by Query name (plain text search), User name (multiple options selected via a checkbox), and/or query Type (multiple options selected via a checkbox).
- **Sort** - Click a column name. You can sort the column data in ascending or descending order.
- **Job Distribution for Query** - Click a query in the Query Status table to see the Job Distribution for Query <*query_name*> table. This table identifies the Worker nodes employed in processing the query and their status. For more information, see Obtaining Job Distribution for Query.

The Query Status table contains the following information:

Column	Description
Query ID	The ID of the query.
Query Name	The name of the query.
Organization	The organization where the query was issued.
User	The name of the user who issued the query.
Type	The value of Type can be: • **Interactive** - Queries executed directly from the **ANALYTICS** page. • **Scheduled** - Queries scheduled from **RESOURCES > Reports**.
Submit Time	The time the query was submitted.
Start Time	The date and time when the query was issued.
Status	The value of Status can be: • **Running** - The query is currently running. • **Waiting** - The query is waiting in the queue because the maximum number of running queries has been reached.
Progress	The percent of progress the query has made towards completion.

Column	Description
Elapsed	The time, in seconds, that the query has run.
Supervisor	The Supervisor involved with the query.

Obtaining Job Distribution for Query

To see how the query job is distributed between Worker nodes, click a query in the Query Status table. The Job Distribution for Query <*query_name*> table appears beneath the Query Status table.

- **Sort** - Click a column name. You can sort the column data in ascending or descending order.

The Job Distribution for Query <*query_name*> table contains the following information:

Column	Description
Node	The Worker IP address.
Role	The FortiSIEM role running the query.
Status	The value of Status can be: • **Unknown** - The query process is in an unknown state. • **Starting** - The query has started processing. • **Running** - The query is currently processing. • **Pausing** - The query is in the process of pausing processing. • **Resuming** - The query has resumed processing. • **Stopping** - the query is in the process of stopping processing. • **Paused** - The query has temporarily paused processing. • **Stopped** - The query has stopped processing. • **Completed** - The query has completed processing.
Progress	The percent of progress the query has made towards completion.
Elapsed	The time (in seconds) elapsed since the Start Time. *Note: This value is calculated from the last refresh time, not the Last Update minus the Start Time.*
Range Start Time	The start time period for scheduled queries.
Range End Time	The end time period for scheduled queries.
Start Time	The date and time when the query began processing.
Last Update	The date and time when the Worker last reported a progress update.

Query Workload

This tab displays a table listing the available Worker nodes for a query job. You can perform the following operations on this tab:

- **Sort** - Click a column name. You can sort the column data in ascending or descending order.
- **Status of Running Tasks** - Click a Worker node row in the Query Workload table to display the Tasks Running On <*Worker_IP_address*> table. For more information, see Obtaining Running Tasks.

The Query Workload table contains the following information:

Column	Description
Node	The Worker IP address.
Role	The FortiSIEM role running the query.
Status	The value of Status can be: • **Online** - The Worker node is currently online. • **Offline** - The Worker node is currently offline.
Interactive Tasks	The number of interactive tasks (that is, sent from the **ANALYTICS** page) assigned to the Worker node.
Scheduled Tasks	The number of scheduled tasks assigned to the Worker node.
Task Workload	The total number of tasks assigned to the Worker node.

Obtaining Running Tasks

To see the status of running tasks, click a Worker node in the Query Workload table. The Tasks Running On <*Worker_IP_address*> table appears beneath the Query Workload table. You can perform the following operations on this tab:

- **Sort** - Click a column name. You can sort the column data in ascending or descending order.

The Tasks Running On <*Worker_IP_address*> table contains the following information:

Column	Description
Query ID	The ID of the query.
Query Name	The name of the query.
Organization	The organization that the query originated from.
User	The name of the user who issued the query.
Type	The value of Type can be: • **Interactive** - Queries executed directly from the **ANALYTICS** page. • **Scheduled** - Queries scheduled from **RESOURCES > Reports**.
Start Time	The date and time when the query began processing.
Status	See Status in Obtaining Job Distribution for Query.

Column	Description
Progress	The percent of progress the query has made towards completion.
Range Start Time	The start time period for scheduled queries.
Range End Time	The end time period for scheduled queries.

Managing FortiSIEM Advanced Operations

FortiSIEM provides the following advanced operations to manage your FortiSIEM:

- Administrator Tools
- Backing Up and Restoring FortiSIEM Directories and Databases

Administrator Tools

For information on Administrator Tools, see here.

Backing Up and Restoring FortiSIEM Directories and Databases

For information on Backing Up and Restoring FortiSIEM Directories and Databases, see here.

Administration

The **ADMIN** tab provides the tools required to setup and monitor FortiSIEM.

The following tools are available:

Setup

Before initiating discovery and monitoring of your IT infrastructure, configure the following settings:

Configuring Storage

FortiSIEM provides 3 options for storing event data.

- Configuring ClickHouse Storage
- Configuring EventDB Storage
- Configuring Elasticsearch Storage

This document provides separate configuration steps for three event databases.

- Configuring ClickHouse Based Deployments
- Configuring EventDB Based Deployments
- Configuring Elasticsearch Based Deployments
- Changing Event Database
- Changing NFS Server IP

Configuring ClickHouse Based Deployments

This section covers the following topics.

- ClickHouse Configuration Overview
- Creating ClickHouse Online Storage
- Configuring ClickHouse Topology
- Creating ClickHouse Archive Storage

ClickHouse Configuration Overview

It may be helpful to review the concepts in ClickHouse Operational Overview and the ClickHouse Sizing Guide. First you need to design your ClickHouse Online Cluster and the role of supervisor and worker nodes. There are 3 cases:

1. **Small deployments**: All-in-one deployment using Supervisor Virtual Machine or a hardware appliance like FortiSIEM 2000G or 3500G.
2. **Medium sized deployments**: Supervisor is a member of Keeper Cluster but not the Data Cluster. Workers are members of both Keeper and Data Clusters.
3. **Large deployments**: Supervisor is not a part of Keeper or Data Clusters. Workers entirely form the Keeper and Data Clusters.

The configuration steps involve:

1. Creating storage on Supervisor and Worker nodes depending on their role.
2. Creating a ClickHouse topology to specify the Supervisor and Worker nodes belonging to Keeper cluster and Data cluster.

Next, you need to configure the Archive, where events will be stored after the Online data stores become full. There are two options:

- For on-premises deployments, you can use a large Warm disk tier as Archive; or real-time archive to NFS.
- For AWS Cloud deployments, you can use AWS S3 for Archive.

After configuring the online and archive storage, you need to specify the retention policies. See How ClickHouse Event Retention Works for details.

Information on Online event database usage can be seen at Viewing Online Event Data Usage.

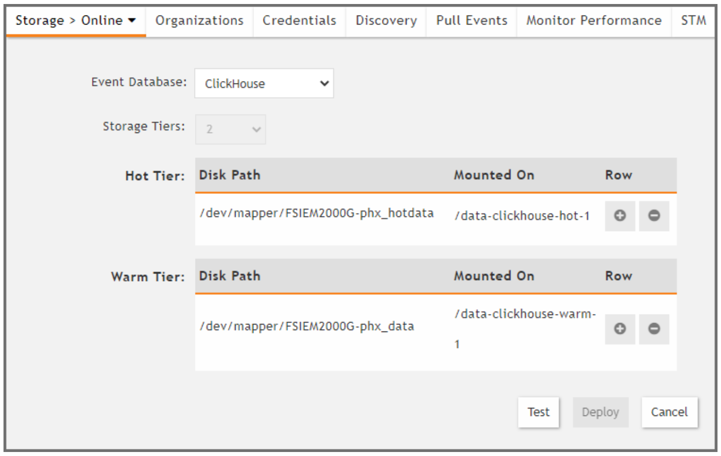
Information on Archive event database usage can be seen at Viewing Archive Data.

For Advanced Configuration Operations, see Advanced Operations in the Appendix.

Creating ClickHouse Online Storage

Case 1: If your FortiSIEM deployment is a **hardware appliance**, then the appliance acts both as a Keeper node and a ClickHouse Data Node. Follow these configuration steps:

1. Navigate to **ADMIN > License** and click **Upload** to load license. For more information, refer to FortiSIEM Licensing Guide.
2. Navigate to **ADMIN > Setup > Storage**, and click **Online** to choose storage.
   a. From the **Event Database** drop-down list, select **ClickHouse**.
   b. The Storage Tiers and the disks will be automatically set for you. If you are running a 2000G appliance, then there will be 2 Storage Tiers and **1 disk in Hot Tier (SSD disks) and 1 disk in Warm Tier (Magnetic Disks)**. If you are running a 3500G appliance, then there will be 1 Storage Tier and 1 disk in Hot Tier (Magnetic Disks).



Event Database: ClickHouse

Storage Tiers: 2

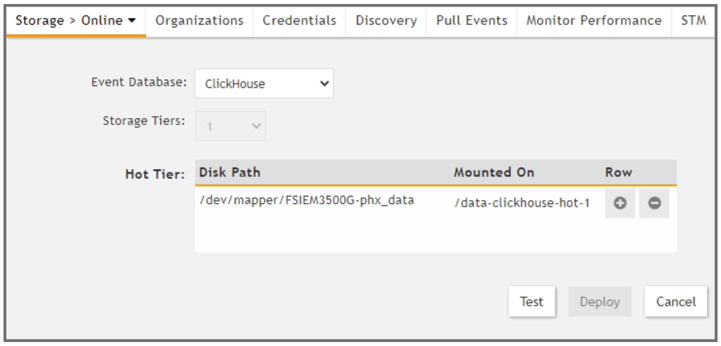
Hot Tier:

Disk Path	Mounted On	Row
/dev/mapper/FSIEM2000G-phx_hotdata	/data-clickhouse-hot-1	⊕ ⊖

Warm Tier:

Disk Path	Mounted On	Row
/dev/mapper/FSIEM2000G-phx_data	/data-clickhouse-warm-1	⊕ ⊖

2000G Storage Setup for ClickHouse



Event Database: ClickHouse

Storage Tiers: 1

Hot Tier:

Disk Path	Mounted On	Row
/dev/mapper/FSIEM3500G-phx_data	/data-clickhouse-hot-1	⊕ ⊖

3500G Storage Setup for ClickHouse

c. Click **Test**.

d. Once it succeeds, then click **Deploy**.

3. The system is now ready for use.

Case 2: If your FortiSIEM deployment is an **all-in-one Virtual Machine (VM)**, then the VM acts both as a Keeper node and a ClickHouse Data Node. Follow these configuration steps:

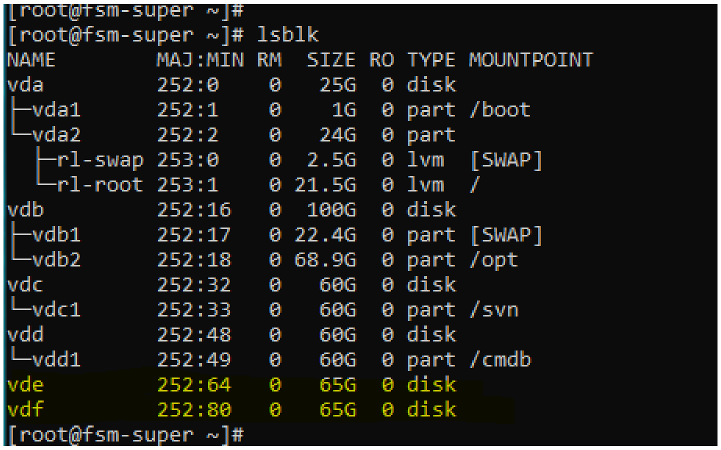
1. Navigate to **ADMIN > License** and click **Upload** to load license. For more information, refer to FortiSIEM Licensing Guide.
2. Navigate to **ADMIN > Setup > Storage**, and click **Online** to choose storage.
   a. From the **Event Database** drop-down list, select **ClickHouse**.
   b. **Storage Tiers**: [Required] Choose **1**.
   c. **Disk Path**: [Required] Click **+** and add a 200GB disk path. Use one of the following CLI commands to find the disk names.

      ```
      fdisk -l
      ```

      or

      ```
      lsblk
      ```

      When using `lsblk` to find the disk name, please note that the path will be '/dev/<disk>'. In the below example, running on KVM, the 5th disk (hot) will be '/dev/vde' and the 6th disk (warm) will be '/dev/vdf'.



```
[root@fsm-super ~]#
[root@fsm-super ~]# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
vda         252:0    0   25G  0 disk
├─vda1      252:1    0    1G  0 part /boot
└─vda2      252:2    0   24G  0 part
  ├─rl-swap 253:0    0  2.5G  0 lvm  [SWAP]
  └─rl-root 253:1    0 21.5G  0 lvm  /
vdb         252:16   0  100G  0 disk
├─vdb1      252:17   0 22.4G  0 part [SWAP]
└─vdb2      252:18   0 68.9G  0 part /opt
vdc         252:32   0   60G  0 disk
└─vdc1      252:33   0   60G  0 part /svn
vdd         252:48   0   60G  0 disk
└─vdd1      252:49   0   60G  0 part /cmdb
vde         252:64   0   65G  0 disk
vdf         252:80   0   65G  0 disk
[root@fsm-super ~]#
```

   d. Click **Test**.
   e. Once it succeeds, click **Deploy**.
3. The system is now ready for use.

Case 3: In this case, your ClickHouse deployment is a **cluster deployment**. This will involve creating storage for Supervisor and Worker nodes and forming Keeper and Data Clusters.

First, during the Supervisor node installation, take the following steps to choose ClickHouse as the Online Event Database and set up storage.

1. Navigate to **ADMIN > License** and click **Upload** to load license. For more information, refer to FortiSIEM Licensing Guide.
2. Navigate to **ADMIN > Setup > Storage**, and click **Online** to choose storage.
   a. From the **Event Database** drop-down list, select **ClickHouse**.
   b. If the Supervisor will be a Keeper node, then a 200GB disk is required. If Supervisor is neither a Keeper node nor a Data Node, then a small disk is still needed to store Query Results.

Next, create Worker nodes and add storage. See Adding a Worker Node for details.

Configuring ClickHouse Topology

After configuring storage, you need to set up the ClickHouse topology. This involves:

- Selecting the Supervisor or Worker nodes that belong to the ClickHouse Keeper Cluster.
- Choosing the number of shards for the ClickHouse Data cluster.
- Selecting the Worker nodes that belong to the ClickHouse Data cluster.

See ClickHouse Configuration for details.

Creating ClickHouse Archive Storage

There are two options:

- For on-premises deployments, you can use a large Cold disk tier as Archive, or you can use real-time archive to NFS.

- For AWS Cloud deployments, you can use AWS S3 for Archive.

Case 1: If you want ClickHouse Cold tier as archive, then configure Cold storage tier in each of the nodes in the ClickHouse Data Cluster. See Adding a Worker Node for details

Case 2: To configure real-time archive using NFS, follow these steps:

1. Go to **ADMIN > Setup > Storage**.
2. Click **Archive**, and select **NFS**.
3. Enter the following parameters:
   a. **IP/Host**: [Required] Select **IP** or **Host** and enter the IP address/Host name of the NFS server.
   b. **Exported Directory**: [Required] Enter the file path on the NFS Server which will be mounted.
4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Case 3: To configure AWS S3 for Archive, follow these steps:

1. Go to **ADMIN > Setup > Storage**.
2. Click **Archive**, and select **AWS S3**.
3. For **Credential Type**, select **Environmental Credentials** or **Explicit Credentials**.
   a. If **Environmental Credentials** is selected, you will need to have an Identity and Access Management. Follow the instructions in Creating IAM Policy for AWS S3 Explicit Credentials to create an IAM Policy
   b. If **Explicit Credentials** is selected, then enter the following information:
      i. **Access Key ID**: Access Key ID required to access the S3 bucket(s)
      ii. **Secret Access Key**: The Secret Access Key associated with the Access Key ID to access the S3 bucket(s)
4. For Buckets:
   a. In the **Bucket** field, enter the bucket URL.
   b. In the **Region** field, enter the region. For example, "us-east-1".
   Note: To minimize any latency, enter the closest region.
   c. If more Buckets are required, click **+** to add a new row.
5. Click **Test**.
6. If the test succeeds, click **Deploy**.
7. Configure each ClickHouse Worker to use the configured S3 bucket.
   a. Navigate to **Admin > License > Nodes**, edit each Worker, check **AWS S3** and choose the Bucket from the drop-down.
   b. Click **Test**, and if the test succeeds, click **Deploy**.
8. If the Supervisor is used as ClickHouse node, take the following steps:
   a. Navigate to **Admin > Setup > Storage**, click **Online**, check **AWS S3** and choose the Bucket from the drop-down.
   b. Click **Test**, and if the test succeeds, click **Deploy**.
9. Apply AWS S3 as the new storage policy to the ClickHouse cluster by taking the following steps.
   a. Navigate to **Admin > Settings > Database > ClickHouse Config**.
   b. Click **Test**, and if the test succeeds, click **Deploy**.

Implementation Notes:

1. AWS S3 buckets MUST be created prior to this configuration.
2. When storing ClickHouse data in AWS S3, Fortinet recommends turning Bucket Versioning off, or suspending it (if it was previously enabled). This is because data in ClickHouse files may change and versioning will keep both copies of data - new and old. With time, the number of stale objects may increase, resulting in higher AWS S3 costs. If versioning was previously enabled for the bucket, Fortinet recommends suspending it and configuring a policy to delete non-current versions.
3. Archive data will NOT be automatically purged by FortiSIEM or ClickHouse.

Creating IAM Policy for AWS S3 Explicit Credentials

Take the following steps from your AWS console.

1. From your **EC2 Dashboard**, select your instance.
2. Navigate to the **IAM dashboard**.
   Note: You can go there by clicking the **IAM** button, or by clicking on **Services** and selecting **IAM**.
3. Click **Policies** to navigate to the **Policies** page, and click **Create policy**.
4. From the **Create policy** page, click the **JSON** tab.
5. Paste the following JSON code into the editor to configure your policy.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "s3:ListStorageLensConfigurations",
            "s3:ListAccessPointsForObjectLambda",
            "s3:GetAccessPoint",
            "s3:PutAccountPublicAccessBlock",
            "s3:GetAccountPublicAccessBlock",
            "s3:ListAllMyBuckets",
            "s3:ListAccessPoints",
            "s3:PutAccessPointPublicAccessBlock",
            "s3:ListJobs",
            "s3:PutStorageLensConfiguration",
            "s3:ListMultiRegionAccessPoints",
            "s3:CreateJob"
         ],
         "Resource":"*"
      },
      {
         "Sid":"VisualEditor1",
         "Effect":"Allow",
         "Action":"s3:*",
         "Resource":[
            "arn:aws:s3:::demo-bucket",
            "arn:aws:s3:::demo-bucket/*"
         ]
```

```
                    }
                ]
            }
```

6. Click the **Next: Tags** button.
   Note: Tags does not need to be configured.
7. Click the **Next: Review** button.
8. On the **Create policy** page, in the **Name** field, enter a name for the policy.
9. Click the **Create policy** button. Your policy has been created.
10. Navigate back to the **IAM dashboard** and click **Roles**, and click **Create role**.
11. For **Select trusted entity**, select **AWS service**.
12. Under **Use case**, select **EC2**.
13. Click **Next**, and then click **Next** again.
14. On the **Name**, **review**, and **create** page, in the **Role name** field, enter a name for the role.
15. Under **Step 2: Add permissions**, click the **Edit** button, and select the policy you created earlier, and click **Next**.
16. Click **Create role**.
17. Navigate to the **Instances** page, select your instance and click the **Security** tab.
18. Click **Actions** (located upper left), and select **Security > Change security groups > Modify IAM role**.
19. Select the role you just created, and click **Update IAM role**.

Configuring EventDB Based Deployment

This section covers the following topics:

- EventDB Configuration Overview
- Creating EventDB Online Storage
- Creating EventDB Archive Storage

EventDB Configuration Overview

EventDB requires a file location for storing events.

- For all-in-one based deployments, you need to create a disk and enter that disk path in the GUI. (Case 1)
- For hardware-based deployments, the disk is already created, and you need to enter specific information in the GUI. (Case 1)
- For cluster-based installations using Workers, you must set up NFS and provide the mount point in the GUI. (Case 2)

You can set up separate Online and Archive EventDB, with separate file locations.

For managing Online and Archive event retention, see How EventDB Event Retention Works.

Information on Online event database usage can be seen at Viewing Online Event Data Usage.

Information on Archive event database usage can be seen at Viewing Archive Data.

Creating EventDB Online Storage

Case 1: If your deployment is on all-in-one node or a hardware appliance, then follow these steps:

1. Go to **ADMIN > Setup > Storage**.
2. Click **Online**, and from the **Event Database** drop-down list, select **EventDB Local Disk**.
3. Enter the following information for **Disk Name**.
   a. Hardware appliances: enter “hardware”
   b. Software installs: enter the 4th or 5th disk name that you configured (Refer to your specific Installation Guide in the FortiSIEM Document Library) during FortiSIEM installation. Use the command `fdisk -l` to find the disk name.
4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Case 2: If your deployment has Worker nodes, then you must configure event database on NFS. Make sure you have NFS server setup and then follow these steps:

1. Go to **ADMIN > Setup > Storage**.
2. Click **Online**, and from the **Event Database** drop-down list, select **EventDB on NFS**.
3. Enter the following parameters:
   a. **Server IP/Host**: [Required] Select **IP** or **Host** and enter the IP address/Host name of the NFS server.
   b. **Exported Directory**: [Required] Enter the file path on the NFS Server which will be mounted.
4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Creating EventDB Archive Storage

Follow these steps:

1. Go to **ADMIN > Setup > Storage**.
2. Click **Archive**, and select **NFS**.
3. Enter the following parameters:
   a. **IP/Host**: [Required] Select **IP** or **Host** and enter the IP address/Host name of the NFS server.
   b. **Exported Directory**: [Required] Enter the file path on the NFS Server which will be mounted.
4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Configuring Elasticsearch Based Deployment

This section covers the following topics:

- Elasticsearch Configuration Overview
- Creating Elasticsearch Online Storage
- Creating Archive for Elasticsearch Based Deployments

Elasticsearch Configuration Overview

FortiSIEM supports 3 Elasticsearch deployments

- Native Elasticsearch – You deploy your own Elasticsearch (Case 1)
- AWS Opensearch (previously known as AWS Elasticsearch) (Case 2)
- Elastic Cloud (Case 1)

Creating Elasticsearch Online Storage

This assumes that you have already deployed Elasticsearch or have an AWS Opensearch or Elastic Cloud account.

Case 1: To configure Native Elasticsearch or Elastic Cloud, follow these steps:

1. Go to **ADMIN > Setup > Storage**.
2. Click **Online**, and from the **Event Database** drop-down list, select **Elasticsearch**, and from the **ES Service Type** drop-down list, select **Native** or **Elastic Cloud** depending on your Elasticsearch set up.
3. Enter the following parameters.
    a. **Org Storage**: This is relevant for FortiSIEM Multi-tenant deployments. Select one of the following from the drop-down list.
        i. **All Orgs in One Index** – In this option, events from all Organizations are mixed in every Elasticsearch index. This is the most cost-effective option as Elasticsearch does not scale when there are many Organizations with high events per sec, and each Organization being in a separate index may lead to an excessive number of indices (note that Elasticsearch has been observed to have approximately 15K index limit per cluster).
        ii. **Each Org in its own Index** – In this option, events from each Organization is in its own Elasticsearch index. This is a flexible option that provides event isolation among Organizations, but Elasticsearch does not scale when there are many Organizations with high events per sec and each Organization being in a separate index may lead to an excessive number of indices.
        iii. **Custom Org Assignment** – In this option, Organizations can be grouped into Groups (maximum 15 allowed). Organizations belonging to the same group have their events in the same index. This is a balanced approach that provides some amount of event isolation, but does not let the number of indices grow excessively. To create and deploy a custom Organization to Group Mapping, follow these steps:
            I. Click **Edit**.
            II. In the follow up dialog, click **Add**.
            III. In the Mapping table, select an Organization in the left column and select the mapped Group in the right column. The 15 specific Groups are numbered 50,001-50,015. Any Organization that is not explicitly mapped, is mapped to the default Group numbered 50,000. A common use case, map 15 of your important customers to the specific groups and the rest to the default groups. Currently, the number of groups (15) is fixed and cannot be changed.
            IV. Click **Deploy**.
    b. **Endpoint**: Click **Edit** and enter the following information:
        i. **URL**: Enter Elasticsearch Coordinator node URL.
        ii. **Ingest/Query** checkbox: If this Coordinator node is to be used for Ingesting Events then check Ingest. If this Coordinator node is going to be used for Querying events, then check the Query flag. If you have multiple Coordinator nodes, then click **+** and select the URL and Ingest/Query flags. This flexibility enables FortiSIEM to separate a set of Coordinator nodes for Query and Ingest functionalities.
    c. **Port**: The TCP port for the URL above (set to HTTPS/443 by default)

   d. **User Name**: Enter the username for basic authentication to be used with the URL
   e. **Password**: Enter the password for basic authentication to be used with the URL
   f. **Shard Allocation**:
      i. If you set it to **Fixed**, then you enter the number of fixed **Shards**, FortiSIEM will not create new shards, even if a Shard reaches its size limit during event surge. You can set the Shard Allocation to Fixed only if you know your system well.
      ii. If you set it to **Dynamic**, then you enter the number of fixed Starting **Shards** (default 5) and FortiSIEM will dynamically adjust the number of shards based on event rate. **This is the recommended method.**
   g. **Replicas**: If you set it to N, then there will be N+1 copies of every index in Elasticsearch. The most common value is Replicas = 1. A higher number of replicas can increase query speed and resiliency against failures, but may slow down event ingest and will use more storage space.
   h. **Event Attribute Template**: This defines how FortiSIEM Event Attributes are mapped to Elasticsearch Event Attribute Types. This mapping is used to store events in Elasticsearch. If you set it to **Default**, then FortiSIEM will use the default mapping. The default mapping maps all (currently 2000+) FortiSIEM Event Attributes and can be a large file. Since this mapping is stored in every index, the global Elasticsearch state also becomes large. It is possible to use a smaller file by including only the FortiSIEM Event Attributes used in your environment. In that case, set this field to **Custom** and enter the custom mapping file.
4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Case 2: To configure AWS Opensearch, follow these steps:

1. Go to **ADMIN > Setup > Storage**.
2. Click **Online**, and from the **Event Database** drop-down list, select **Elasticsearch**, and from the **ES Service Type** drop-down list, select **Amazon**
3. Enter the following parameters.
   a. **Endpoint**: Click **Edit** and the enter the following information:
      i. **URL**: Enter the AWS Opensearch URL.
      ii. **Ingest/Query** checkbox: If this endpoint is to be used for Ingesting Events, then check Ingest. If this endpoint is going to be used for Querying events, then check the Query flag. If you have multiple endpoints, then click + and select the URL and Ingest/Query flags. This flexibility enables to separate a set of endpoints for Query and Ingest functionalities.
   b. **Port**: The TCP port for the URL above (set to HTTPS/443 by default).
   c. **Access Key ID**: Enter the Access Key ID for use with this endpoint.
   d. **Secret Key**: Enter the Secret Key to be used with this endpoint.
   e. **Shard Allocation**:
      i. If you set it to **Fixed**, then you enter the number of fixed **Shards**, FortiSIEM will not create new shards, even if a Shard reaches its size limit during event surge. You can set the Shard Allocation to Fixed only if you know your system well.
      ii. If you set it to **Dynamic**, then you enter the number of fixed Starting **Shards** (default 5) and FortiSIEM will dynamically adjust the number of shards based on event rate. **This is the recommended method.**

f. **Replicas**: If you set it to N, then there will be N+1 copies of every index in Elasticsearch. The most common value is Replicas = 1. A higher number of replicas can increase query speed and resiliency against failures, but may slow down event ingest and will use more storage space.

g. **Event Attribute Template**: This defines how FortiSIEM Event Attributes are mapped to Elasticsearch Event Attribute Types. This mapping is used to store events in Elasticsearch. If you set it to **Default**, then FortiSIEM will use the default mapping. The default mapping maps all (currently 2000+) FortiSIEM Event Attributes and can be a large file. Since this mapping is stored in every index, the global Elasticsearch state also becomes large. It is possible to use a smaller file by including only the FortiSIEM Event Attributes used in your environment. In that case, set this field to **Custom** and enter the custom mapping file.

4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Creating Archive for Elasticsearch Based Deployments

There are 3 archive options

- HDFS Archive from Elasticsearch
- Real-time HDFS Archive from FortiSIEM
- Real-time Archive to NFS

Configuring HDFS Archive from Elasticsearch

In this option, FortiSIEM HDFSMgr process creates Spark jobs to directly pull events from Elasticsearch and store in HDFS. Follow these steps.

1. Go to **ADMIN > Setup > Storage**.
2. Click **Archive**, and select **HDFS**.
3. Enter the following parameters:
   a. Uncheck **Real Time Archive**.
   b. For **Spark Master Node**:
      i. Select **IP** or **Host** and enter the IP address or Host name of the Spark Cluster Master node.
      ii. Set **Port** to the TCP port number for FortiSIEM to communicate to the Spark Master node.
   c. For **HDFS Name Node**:
      i. Select **IP** or **Host** and enter the IP address or Host name of the HDFS Name node. This is the machine which stores the HDFS metadata: the directory tree of all files in the file system, and tracks the files across the cluster.
      ii. Set **Port** to the TCP port number for FortiSIEM to communicate to the HDFS Name node.
4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Configuring Real-time HDFS Archive from FortiSIEM

In this option, FortiSIEM HDFSMgr process creates Spark jobs to pull events from FortiSIEM Supervisor and Worker nodes. Follow these steps.

1. Go to **ADMIN > Setup > Storage**.
2. Click **Archive**, and select **HDFS**.

3. Enter the following parameters:
    a. Check **Real Time Archive**. Set a Start time (in the future) when the real time archive should begin
    b. For **Spark Master Node**:
        i. Select **IP** or **Host** and enter the IP address or Host name of the Spark Cluster Master node.
        ii. Set **Port** to the TCP port number for FortiSIEM to communicate to Spark Master node.
    c. For **HDFS Name Node**:
        i. Select **IP** or **Host** and enter the IP address or Host name of the HDFS Name node. This is the machine which stores the HDFS metadata: the directory tree of all files in the file system, and tracks the files across the cluster.
        ii. Set **Port** to the TCP port number for FortiSIEM to communicate to HDFS Name node.
4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Configuring Real-time Archive to NFS

In this option, FortiSIEM Supervisor and Worker nodes store events in NFS managed by FortiSIEM EventDB. This happens while events are getting inserted into Elasticsearch. This approach has no impact in Elasticsearch performance, but events are stored in both Elasticsearch and EventDB and managed independently. Follow these steps.

1. Go to **ADMIN > Setup > Storage**.
2. Click **Archive**, and select **NFS**.
3. Enter the following parameters:
    a. **IP/Host**: [Required] Select **IP** or **Host** and enter the IP address/Host name of the NFS server.
    b. **Exported Directory**: [Required] Enter the file path on the NFS Server which will be mounted.
4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Changing Event Database

It is highly recommended to chose a specific event storage option and retain it. However, it is possible to switch to a different storage type.

Note: In all cases of changing storage type, the old event data is not migrated to the new storage. Contact FortiSIEM Support if this is needed - some special cases may be supported.

For the following cases, simply choose the new storage type from **ADMIN** > **Setup** > **Storage**.

- Local to Elasticsearch
- NFS to Elasticsearch
- Elasticsearch to Local

The following storage change cases need special considerations:

- Elasticsearch to NFS
- Local to NFS
- NFS to Local
- EventDB to ClickHouse
- Elasticsearch to ClickHouse
- ClickHouse to EventDB
- ClickHouse to Elasticsearch

Elasticsearch to NFS

1. Log in to FortiSIEM GUI.
2. Select and delete the existing Workers from **ADMIN** > **License** > **Nodes** > **Delete**.
3. Go to **ADMIN** > **Setup** > **Storage** and update the Storage type as **NFS** server
4. Go to **ADMIN** > **License** > **Nodes** and **Add** the recently deleted Workers in step #2.

Local to NFS

If you are running a single Supervisor, then follow these steps.

1. SSH to the Supervisor and stop FortiSIEM processes by running:
   `phtools --stop all`
2. Unmount `/data` by running:
   `umount /data`
3. Validate that /data is unmounted by running:
   `df -h`
4. Edit /etc/fstab and remove /data mount location.
5. Log in to FortiSIEM GUI, go to **ADMIN** > **Setup** > **Storage** and update the Storage type as **EventDB on NFS**.

If you are running multiple Supervisors in Active-Active cluster, then follow these steps.

1. Log on to Leader.
2. Run steps 1-4 in the single Supervisor case described above.
3. Log on to each Follower and repeat steps 1-4 in the single Supervisor case described above.
4. Log on to Leader, go to **ADMIN > Setup > Storage** and set the Storage type to **EventDB on NFS**.
5. Log on to any node and make sure that all processes are up on all Supervisors.

NFS to Local

1. SSH to the Supervisor and stop FortiSIEM processes by running:
   `phtools --stop all`
2. Unmount /data by running:
   `umount /data`
3. Validate that `/data` is unmounted by running:
   `df -h`
4. Edit /etc/fstab and remove /data mount location.
5. Connect the new disk to Supervisor VM.
6. Log in to FortiSIEM GUI, go to **ADMIN** > **Setup** > **Storage** and update the Storage type as **Local Disk**.

EventDB to ClickHouse

- Single Node Deployment
- Single Supervisor with Workers Deployment

- Multiple Supervisors and Workers Deployment

Assuming you are running FortiSIEM EventDB on a single node deployment (e.g. 2000F, 2000G, 3500G and VMs), the following steps shows how to migrate your event data to ClickHouse.

Follow these steps to migrate events from EventDB to ClickHouse.

1. Stop all the processes on Supervisor by running the following command.
   `phtools --stop all`
   Note: This will also stop all events from coming into Supervisor.
2. Edit `/etc/fstab` and remove all */data* entries for EventDB.
3. If the same disk is going to be used by ClickHouse (e.g. in hardware Appliances), then copy out events from FortiSIEM EventDB to a remote location. You can bring back the old data if needed (See Step 7).
   a. Mount a new remote disk for the appliance, assuming the remote server is ready, using the following command.`# mount -t nfs <remote server ip>:<remote share point> <local path>`
   b. Copy the data, using the following command.
      `# rsync -av --progress /data /<local path>`
      Example: `# rsync -av --progress /data /mnt/eventdb`
4. If the same disk is going to be used by ClickHouse (e.g. in hardware Appliances), then delete old data from FortiSIEM, by taking the following steps.
   a. Remove the data by running the following command.
      `# rm -rf /data/*`
   b. Unmount, by running the following commands.
      ```
      # note mount path for /data
      # umount /data
      ```
   c. For 2000G, run the following additional command.
      `# lvremove /dev/mapper/FSIEM2000G-phx_eventdbcache: y`
5. For VM based deployments, create new disks for use by ClickHouse by taking the following steps.
   a. Edit your Virtual Machine on your hypervisor.
   b. Add a new disk to the current disk controller.
   c. Run the following in your FortiSIEM Supervisor Shell if the disk is not automatically added.
      ```
      # echo "- - -" > /sys/class/scsi_host/host0/scan
      # echo "- - -" > /sys/class/scsi_host/host1/scan
      # echo "- - -" > /sys/class/scsi_host/host2/scan
      # lsblk
      ```
6. Log into the GUI as a full admin user and change the storage to ClickHouse by taking the following steps.
   a. Navigate to **ADMIN > Setup > Storage > Online**.
   b. From the **Event Database** drop-down list, select **ClickHouse**.
   c. From the **Storage Tiers** drop-down list, select **1**.
   d. In the Disk Path field, select the disk path.
      Example: `/dev/sde`
   e. Click **Test**.
   f. Click **Deploy**.
   g. Navigate to **Admin > Settings > Database > ClickHouse Config**, and click **Test** and then click **Deploy**.
7. (Optional) Import old events. For appliances they were copied out in Step 3 above. For VMs, they may be mounted remotely. To do this, run the following command from FortiSIEM.

```
# /opt/phoenix/bin/phClickHouseImport --src [Source Dir] --starttime [Start
Time] --endtime [End Time] --host [IP Address of ClickHouse - default 127.0.0.1]
--orgid [Organization ID (0 – 4294967295)
```

More information on `phClickHouseImport` can be found here.
Note the valid time format:
<*time*> : *"YYYY-MM-DD hh:mm:ss"* (notice the quotation marks, they need to be included.)
Example:

```
phClickHouseImport --src /test/sample --starttime "2022-01-27 10:10:00" --end-
time "2022-02-01 11:10:00"
```

Example with import all organizations:

```
[root@SP-191 mnt]# /opt/phoenix/bin/phClickHouseImport --src /mnt/eventdb/ --
starttime "2022-01-27 10:10:00" --endtime "2022-03-9 22:10:00"
Found 32 days' Data
[█ ] 3% 3/32 [283420]█
```

8. Log into FortiSIEM GUI and use the **ANALYTICS** tab to verify events are being ingested.
   Note: If your Single Node deployment also contains Workers, proceed to the next section for Worker configuration.

If you are running a single Supervisor with Workers, take the following steps for your Workers, after following the prior steps for your Supervisor in Single Node Deployment.

1. Navigate to **Admin > License**.
2. Click the **Nodes** tab.
3. From the **License > Nodes** page, take the following steps for each Worker.
   a. Select a Worker, and click **Edit**.
   b. Add disks.
   c. Click **Test**.
   d. Click **Save**.
   e. Repeat steps 3.a-3.d for each Worker. Proceed to step 4 after all Workers have been configured.
4. Navigate to **Admin > Settings > Database > ClickHouse Config**, and click **Test** and then click **Deploy**.

If you are running multiple Supervisors, Workers with EventDB on NFS and want to switch to ClickHouse, take the following steps:

1. Power off all Supervisors, Workers and add new disks for ClickHouse.
2. Power on all Supervisors, Workers.
3. Wait until all processes are up.
4. SSH to Primary Leader Supervisor node.
   a. Run the following command.
      ```
      phtools --stop all
      ```
   b. Unmount `/data` by running the following command.
      ```
      umount /data
      ```
   c. Validate that `/data` is unmounted by running the following command.
      ```
      df -h
      ```
   d. Edit `/etc/fstab` and remove `/data` mount location.
5. Repeat Step 4 for all Primary Follower Supervisor nodes.

6. SSH to Primary Leader Supervisor node.
   a. Configure ClickHouse following the steps in Configuring ClickHouse Based Deployments.
   b. Run the following command.
      ```
      phtools --start all
      ```
7. Log into FortiSIEM GUI and use the **ANALYTICS** tab to verify events are being ingested.

Elasticsearch to ClickHouse

To switch your Elasticsearch database to ClickHouse, take the following steps.

Note: Importing events from Elasticsearch to ClickHouse is currently not supported

1. Stop all the processes on Supervisor by running the following command.
   ```
   phtools --stop all
   ```
   Note: This command will also stop all events from coming into the Supervisor. Make sure `phMonitor` process is running.
2. Log into your hypervisor and add disks for ClickHouse by taking the following steps. You can have 3 Tiers of disks with multiple disks in each Tier. You must have at least 1 Tier one disk.
   a. Edit your Virtual Machine on your hypervisor.
   b. Add a new disk to the current disk controller.
   c. Run the following in your FortiSIEM Supervisor Shell if the disk is not automatically added.
      ```
      # echo "- - -" > /sys/class/scsi_host/host0/scan
      # echo "- - -" > /sys/class/scsi_host/host1/scan
      # echo "- - -" > /sys/class/scsi_host/host2/scan
      # lsblk
      ```
3. Set up ClickHouse as the online database by taking the following steps.
   a. Navigate to **ADMIN > Setup > Storage > Online**.
   b. From the **Event Database** drop-down list, select **ClickHouse**.
   c. From the **Storage Tiers** drop-down list, select **1**.
      Note: If you wish to have a warm tier or multiple hot tier disks, additional disks are required
   d. Provide the disk path.
   e. Click **Test**.
   f. Click **Deploy** when the test is successful.

   Events can now come in.
4. Log into FortiSIEM GUI and use the **ANALYTICS** tab to verify events are being ingested.

ClickHouse to EventDB

To switch your ClickHouse database to EventDB, take the following steps.

Note: Importing events from ClickHouse to EventDB is currently not supported.

1. Stop all the processes on the Supervisor by running the following command.
   ```
   phtools --stop all
   ```
   Note: This is will also stop all the events from coming into Supervisor.
2. Stop ClickHouse Service by running the following commands.
   ```
   systemctl stop clickhouse-server
   systemctl stop phClickHouseMonitor
   ```

3. Edit `phoenix_config.txt` in `/opt/phoenix/config` on Supervisor and set `enable = false` for ClickHouse.
4. Edit and remove any mount entries in `/etc/fstab` that relates to ClickHouse.
5. Unmount data by taking the following step depending on whether you are using a VM (hot and/or warm disk path) or hardware (2000F, 2000G, 3500G).
   a. For VM, run the following command.
      ```
      umount /data-clickhouse-hot-1
      ```
      If multiple tiers are used, the disks will be denoted by a number.
      Example:
      ```
      /data-clickhouse-hot-2
      /data-clickhouse-warm-1
      /data-clickhouse-warm-2
      ```
   b. For hardware, run the following command.
      ```
      umount /data-clickhouse-hot-1
      ```
   c. For 2000G, run the following additional commands.
      ```
      umount /data-clickhouse-warm-1
      lvremove /dev/mapper/FSIEM2000Gphx_hotdata : y
      ```
6. Delete old ClickHouse data by taking the following steps.
   a. Remove old ClickHouse configuration by running the following commands.
      ```
      # rm -f /etc/clickhouse-server/config.d/*
      # rm -f /etc/clickhouse-server/users.d/*
      ```
7. Clean up "incident" in psql, by running the following commands.
   ```
   psql -U phoenix -d phoenixdb
   truncate ph_incident;
   truncate ph_incident_detail;
   ```
8. Configure storage for EventDB by taking the following steps.
   - For VMs, proceed with Step 9, then continue.
   - For hardware appliances 2000F, 2000G, or 3500G, proceed to Step 10.
9. Set up EventDB as the online database by taking the following steps for Creating EventDB Online Storage (Local Disk) OR Creating EventDB Online Storage (NFS).
   a. For EventDB Local Disk configuration, take the following steps.
      i. Create a new disk for the VM by logging into the hypervisor and create a new disk.
      ii. Log into the FortiSIEM Supervisor GUI as a full admin user.
      iii. Navigate to **ADMIN > Setup > Storage > Online**.
      iv. From the **Event Database** drop-down list, select **EventDB Local Disk**.
      v. Target the new local disk.
      vi. Click **Test**.
      vii. Click **Deploy**.
      viii. Proceed to Step 11.
   b. For EventDB on NFS configuration, take the following steps.
      Note: Make sure remote NFS storage ready.
      i. Create a new disk for the VM by logging into the hypervisor and create a new disk.
      ii. Log into FortiSIEM Supervisor GUI as a full admin user.
      iii. Navigate to **ADMIN > Setup > Storage > Online**.
      iv. From the Event Database drop-down list, select **EventDB on NFS**.

   v. In the **IP/Host** field, select **IP** or **Host** and enter the remote NFS server IP Address or Host name.
   vi. In the **Exported Directory** field, enter the share point.
   vii. Click **Test**.
   viii. Click **Deploy**.
   ix. Proceed to Step 11.

10. Set up EventDB as the online database, by taking the following steps.
    a. Log into the FortiSIEM Supervisor GUI as a full admin user.
    b. Navigate to **ADMIN > Setup > Storage > Online**.
    c. From the **Event Database** drop-down list, select **EventDB**.
    d. Click **Test**.
    e. Click **Deploy**.
11. Make sure phMonitor process is running. Events can now come in.
12. Verify events are coming in by running Adhoc query in **ANALYTICS**.

ClickHouse to Elasticsearch

To switch your ClickHouse database to Elasticsearch, take the following steps.

Note: Importing events from ClickHouse to Elasticsearch is currently not supported.

1. Stop all the processes on Supervisor by running the following command.
   ```
   phtools --stop all
   ```
   Note: This is will also stop all the events from coming into Supervisor.
2. Stop ClickHouse Service by running the following commands.
   ```
   systemctl stop clickhouse-server
   systemctl stop phClickHouseMonitor
   ```
3. Edit `phoenix_config.txt` on the Supervisor and set `enable = false` for ClickHouse.
4. Edit and remove any mount entries in `/etc/fstab` that relates to ClickHouse
5. Unmount data by taking the following step depending on whether you are using a VM (hot and/or warm disk path) or hardware (2000F, 2000G, 3500G).
   a. For VM, run the following command.
      ```
      umount /data-clickhouse-hot-1
      ```
      If multiple tiers are used, the disks will be denoted by a number:
      Example:
      ```
      /data-clickhouse-hot-2
      /data-clickhouse-warm-1
      /data-clickhouse-warm-2
      ```
   b. For hardware, run the following command.
      ```
      umount /data-clickhouse-hot-1
      ```
   c. For 2000G, run the following additional commands.
      ```
      umount /data-clickhouse-warm-1
      lvremove /dev/mapper/FSIEM2000Gphx_hotdata : y
      ```
6. Delete old ClickHouse data by taking the following steps.
   a. Remove old ClickHouse configuration by running the following commands.
      ```
      # rm -f /etc/clickhouse-server/config.d/*
      # rm -f /etc/clickhouse-server/users.d/*
      ```

7. Clean up "incident" in psql, by running the following commands.
   ```
   psql -U phoenix -d phoenixdb
   truncate ph_incident;
   truncate ph_incident_detail;
   ```
8. Make sure `phMonitor` process is running.
9. Setup Elasticsearch as online database by taking the following steps.
   a. Log into the FortiSIEM Supervisor GUI as a full admin user.
   b. Navigate to **ADMIN > Setup > Storage > Online**.
   c. From the **Event Database** drop-down list, select **Elasticsearch**.
   d. From the **ES Service Type** drop-down list, select **Native**, **Amazon**, or **Elastic Cloud**.
   e. Configure the rest of the fields depending on the ES Service Type you selected.
   f. Click **Test**.
   g. Click **Deploy**.
10. Wait for `JavaQuerySever` process to start up.
11. Start new events.
12. Verify events are coming in by running Adhoc query in **ANALYTICS**.

Changing NFS Server IP

If you are running a FortiSIEM Cluster using NFS and want to change the IP address of the NFS Server, then take the following steps.

Step 1: Temporarily Change the Event Storage Type from EventDB on NFS to EventDB on Local

1. Go to **ADMIN > License > Nodes** and remove all the Worker nodes.
2. SSH to the Supervisor and stop FortiSIEM processes by running:
   ```
   phtools --stop all
   ```
3. Unmount `/data` by running:
   ```
   umount /data
   ```
4. Validate that `/data` is unmounted by running:
   ```
   df -h
   ```
5. Edit `/etc/fstab` and remove `/data` mount location.
6. Attach new local disk to the Supervisor. It is recommended that it is at least 50~80GB.
7. Go to **ADMIN > Setup > Storage > Online**.
8. Change the storage type to **Local Disk** and add the local disk's partition to the **Disk Name** field. (e.g. `/dev/sde`).
9. Click **Test** to confirm.
10. Click **Deploy**.

Step 2: Change the NFS Server IP Address

This is a standard system administrator operation. Change the NFS Server IP address.

Step 3: Change the Event Storage Type Back to EventDB on NFS

1. SSH to the Supervisor and stop FortiSIEM processes by running:
   ```
   phtools --stop all
   ```
2. Umount `/data` by running:
   ```
   umount /data
   ```

3. Validate that `/data` is unmounted by running:
   `df -h`
4. Edit `/etc/fstab` and remove `/data` mount location.
5. Go to **ADMIN > Setup > Storage > Online**.
6. Change the storage type to **NFS**.
7. In the **Server** field, with **IP** selected, enter the new IP address of the NFS server.
8. In the **Exported Directory** field, enter the correct NFS folder's path.
9. Click **Test** to confirm.
10. Click **Deploy**.
11. Go to **ADMIN > License > Nodes** and add back all the Worker nodes.

Setting Organizations and Collectors (Service Provider)

FortiSIEM supports multi-tenancy via Organizations in a Service Provider deployment. The devices and logs belonging to two Organizations are kept separate. Incidents trigger separately for Organizations.

A Collector enables FortiSIEM to collect logs and performance metrics from geographically disparate networks. Data collection protocols such as SNMP and WMI are often chatty and the devices may only be reachable from the Supervisor node via Internet and behind a firewall. Syslog protocol specially over UDP is unreliable and insecure. A Collector can be deployed behind the firewall to solve these issues. The Collector registers with FortiSIEM Supervisor node and then receives commands from the Supervisor regarding discovery and data collection. The Collector parses the logs and forwards the compressed logs to Supervisor/Worker nodes over an encrypted HTTPS channel. The Collector also buffers the logs locally for a period of time if the network connection to the Super/Worker is not available.

Organizations can be defined in one of two ways:

- Associating one or more Collectors to an Organization – the devices monitored by the Collector or the events sent to the Collector automatically belong to the associated Organization.
- Defining an IP range for an Organization – if the sending IP of a device belongs to the IP range, then the device and logs belong to that Organization.

This section provides the procedures to configure an Organization for a multi-tenant FortiSIEM deployment.

- Creating an Organization
- Installing a Collector
- Registering a Collector

Note: For information on Diode Collector, see the Diode Collector Installation Guide.

Make sure the Worker Upload has been configured prior to defining the Collectors.

Creating an Organization

Complete these steps to add an Organization:

1. Go to **ADMIN** > **Setup** > **Organizations** tab.
2. Click **New**.
3. In the **Organization Definition** dialog box, enter the information below.

Settings	Guidelines
Organization	[Required] Name of the Organization
Full Name	Full name of the Organization
Admin User	[Required] User name that will be used two purposes: (a) Users logging in to FortiSIEM Supervisor GUI for that Organization and (b) Collector registration to Supervisor. This user has 'Full Admin' role.
Admin Password/Confirm Admin Password	[Required] Password of the Admin user.
Admin Email	[Required] Email id of the Admin user for the Organization.
Phone	Contact number for the Organization
Include IP/IP Range	IP range for the Organization in case the Organization is defined by IP addresses. Allowed format is comma-separated individual IPs or IP range 10.10.10.1-10.10.10.8
Exclude IP/IP Range	IP range to be excluded for the Organization. Allowed format is comma-separated individual IPs or IP range 10.10.10.1-10.10.10.8
Agent User	User name used by FortiSIEM Windows and Linux Agents to register to FortiSIEM Supervisor. **Note**: An Agent User cannot be used to log into the UI.
Agent Password/Confirm Agent Password	Password of Agent User.
Max Devices	Maximum number of monitored CMDB devices for the Organization
Address	Contact address for the Organization

4. If your Organization uses Collectors, click **New** under **Collectors** and enter the information below.

Settings	Guidelines
Name	[Required] Name of the Collector

Settings	Guidelines
Guaranteed EPS	[Required] Events from this Collector are always accepted when its event rate is below this Guaranteed EPS. FortiSIEM will re-allocate excess EPS (license minus the sum of Guaranteed EPS over all the collectors) based on need but the allocation will never go below the Guaranteed EPS.
Upload Rate Limit (Kbps)	Maximum rate limit (in Kbps) at which a Collector can send events to all Workers.
Start Time	[Required] Select a specific start date or check 'Unlimited'. Collectors will not work outside of start and end dates if specific dates are chosen.
End Time	[Required] Select a specific end date or check 'Unlimited'. Collectors will not work outside of start and end dates if specific dates are chosen.

5. Enter the **Description** about the Organization.
6. Click **Save**.

Installing a Collector

For installing Collectors, see the "Install Collector" sections in the specific Installation Guides.See also the Upgrade Guide and the Sizing Guides available in the FortiSIEM Documents Library here.

Registering a Collector

Once a Collector has been created in the GUI, the Collector needs to be installed and registered.

For registering a Collector, follow these steps:

1. SSH to the Collector.
2. Run the following command:
   ```
           phProvisionCollector --add <user> '<password>' <super IP or host> <organization>
   <collectorName>
   ```
   The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped. In Enterprise mode, use `super` as the organization .

   Refer to the tables in steps 3 and 4 here for more information about these settings: `<user>`, `<password>`, `<organization>` and `<collectorName>`

Setting Collectors (Enterprise)

A Collector enables FortiSIEM to collect logs and performance metrics from geographically disparate networks. Data collection protocols such as SNMP and WMI are often chatty and the devices may only be reachable from the Supervisor node via Internet and behind a firewall. Syslog protocol, especially over UDP, is unreliable and insecure. A Collector can be deployed behind the firewall to solve these issues. The Collector registers with FortiSIEM Supervisor node and then receives commands from the Supervisor regarding discovery and data collection. The Collector parses the logs and forwards the compressed logs to Supervisor/Worker nodes over an encrypted HTTPS channel. The

Collector also buffers the logs locally for a period of time if the network connection to the Super/Worker is not available.

This section provides the procedures to configure a Collector in Enterprise deployment.

- Adding a Collector
- Installing a Collector
- Registering a Collector

Note: For information on Diode Collector, see the Diode Collector Installation Guide.

Make sure the Worker Upload has been configured prior to defining the Collectors.

Adding a Collector

Complete these steps to add an Collector:

1. Go to **ADMIN** > **Setup** > **Collector** tab.
2. Click **New**.
3. In the **Event Collector Definition** dialog box, enter the information below.

Settings	Guidelines
Name	[Required] Collector name
Guaranteed EPS	[Required] Events from this Collector are always accepted when its event rate is below this Guaranteed EPS. FortiSIEM will re-allocate excess EPS (license minus the sum of Guaranteed EPS over all the collectors) based on need but the allocation will never go below the Guaranteed EPS.
Upload Rate Limit (Kbps)	Maximum rate limit (in Kbps) at which a Collector can send events to all Workers. Rate limit is enforced at periodic 3 minute intervals. When either the upload rate limit or EPS limit are hit, events are buffered at the Collector and sent later.
Upload EPS Limit	Maximum events per second at which a Collector can send events to all Workers. EPS limit is enforced at periodic 3 minute intervals. When either the upload rate limit or EPS limit are hit, events are buffered at the Collector and sent later.
Start Time	[Required] Select a specific start date or check 'Unlimited'. Collectors will not work outside of start and end dates if specific dates are chosen.
End Time	[Required] Select a specific end date or check 'Unlimited'. Collectors will not work outside of start and end dates if specific dates are chosen.
Agent User	User name used by FortiSIEM Windows and Linux Agents to

Settings	Guidelines
	register to FortiSIEM Supervisor.
Agent Password/Confirm Agent Password	Password of Agent User

4. Click **Save**.

Installing a Collector

For installing Collectors, see the "Install Collector" sections in the specific Installation Guides. See also the Upgrade and Sizing Guides available in the FortiSIEM Documents Library here.

Registering a Collector

Once a Collector has been created in the GUI, the Collector needs to be installed and registered.

For registering a Collector, follow these steps:

1. SSH to the Collector.
2. Run the following command:
   ```
           phProvisionCollector --add <user> '<password>' <super IP or host> <organization>
   <collectorName>
   ```
   The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped. In Enterprise mode, use `super` as the organization .

   Refer to the tables in steps 3 and 4 here for more information about these settings: `<user>`, `<password>`, `<organization>` and `<collectorName>`

Setting Credentials

FortiSIEM communicates with various systems to collect operating system/hardware/software information, logs, and performance metrics. This section provides the procedures to set up a device credential and associate them to an IP or IP range. For information on generalized HTTPS based event collection, refer to "Generic Log API Poller (HTTPS Advanced) Integration" in the Appendix of the latest External Systems Configuration Guide.

- Creating a Credential
- Associating a Credential to IP Ranges or Hosts
- Testing Credentials and API Event Collection
- Modifying Device Credential
- Modifying a Credential Association
- Credentials Based on Access Protocol

Creating a Credential

Complete these steps to create a login credential:

1. Go to **ADMIN** > **Setup** > **Credentials** tab.
2. Under **Step 1: Enter Credentials** section, click **New**.

3. In the **Access Method Definition** dialog box, enter the information below.

Settings	Guidelines
Name	[Required] Name of the credential that will be used for reference purpose.
Device Type	Type of device from the drop-down.
Access Protocol	Type of access protocol from the drop-down. Note that this list depends on the selected device type.
Port	TCP/UDP Port number for communicating to the device for the access protocol.
Password config	Choose **Manual**, **CyberArk SDK** or **CyberArk REST API**. - **Manual**: The credentials will be defined and stored in FortiSIEM. See the External Systems Configuration Guide for the corresponding device type configuration settings. - **CyberArk SDK**: FortiSIEM will get credentials from CyberArk password Vault. See "CyberArk SDK Password Configuration" in the External Systems Configuration Guide for configuration settings. -**CyberArk REST API**: FortiSIEM will get credentials from CyberArk password Vault through REST API access. See "CyberArk REST API Password Configuration" in the External Systems Configuration Guide for configuration settings.

4. Enter the options in the remaining fields that appear based on the **Device Type** selection.
5. Click **Save**.

Associating a Credential to IP Ranges or Hosts

The association is on a per-Collector basis.

1. Under **Step 2: Enter IP Range to Credential Associations** section, click **New**.
2. In the **Device Credential Mapping Definition** dialog box, enter the information below.

Settings	Guidelines
IP/Host Name	[Required] Host name, IP address or IP range to associate with a credential. Allowed IP range syntax is single IP, single range, single CIDR or a list separated by comma – e.g. 10.1.1.1, 10.1.1.2,20.1.1.0/24, 30.1.1.1-30.1.1.10. Host names are only allowed for a specific set of credentials see below.
Credentials	Select one or more credentials by name. Use **+** to add more.

3. Click **Save**.

Testing Credentials and API Event Collection

Credentials can be tested to ensure that they are working correctly and do not perform a full discovery, and therefore provide results more quickly.

Test Connectivity also has a special function for certain Device API integrations. Instead of performing separate Discovery to integrate FortiSIEM with a Device API, clicking **Test Connectivity** will test the credential and start collecting event from the API. The External System Configuration Guide details Device integrations that require only this step to collect events.

1. If the user assigns a Test Connectivity or Discovery task to a Collector, then the Collector performs those tasks. The Supervisor also assigns the performance monitoring task to the same Collector that performed discovery.
2. For environments without Collector:
   a. Supervisor does discovery and Test Connectivity.
   b. Supervisor then assigns the performance monitoring tasks to the Active Workers in a weighted round robin fashion. Some jobs like vCenter monitoring has a higher weight than simple SNMP based CPU monitoring.
   c. Workers perform the performance monitoring tasks.
   d. If a Worker is removed, its performance monitoring jobs are redistributed to other Workers.
   e. If a Worker is added, new performance monitoring jobs are assigned to that Worker.
   f. If you disable and then enable performance monitoring jobs from the GUI, then a new global job distribution takes place.

1. Select an association.
2. Click **Test** after choosing:
   - **Test Connectivity** – the device will be pinged first and then the credential will be attempted. This shortens the test connectivity process in case the device with specified IP is not present or reachable.
   - **Test Connectivity without Ping** – the credential will be attempted without pinging first.
3. Check the test connectivity result in the pop up display.

Modifying Device Credentials

Complete these steps to modify device credentials:

1. Select an association from the list and click the required option.
   - **Edit** - to modify any credential settings.
   - **Delete** - to delete a credential.
   - **Clone** - to duplicate a credential.
2. Click **Save**.

Modifying a Credential Association

Complete these steps to modify a credential association:

1. Select the credential association from the list and click the required option under **Step 2: Enter IP Range to Credential Associations**:
   - **Edit** - to edit an associated IP/IP range
   - **Delete** - to delete any association
2. Click **Save**.

Credentials Based on Access Protocol

For information on the credential configuration settings for selected devices, see the External Systems Configuration Guide.

Discovering Devices

FortiSIEM automatically discovers devices, applications, and users in your IT infrastructure and start monitoring them. You can initiate device discovery by providing the credentials that are needed to access the infrastructure component, and from there FortiSIEM will discover information about your component such as the host name, operating system, hardware information such as CPU and memory, software information such as running processes and services, and configuration information. Once discovered, FortiSIEM will also begin monitoring your component on an ongoing basis.

1. If the user assigns a Test Connectivity or Discovery task to a Collector, then the Collector performs those tasks. The Supervisor also assigns the performance monitoring task to the same Collector that performed discovery.
2. For environments without Collector:
   a. Supervisor does discovery and Test Connectivity.
   b. Supervisor then assigns the performance monitoring tasks to the Active Workers in a weighted round robin fashion. Some jobs like vCenter monitoring has a higher weight than simple SNMP based CPU monitoring.
   c. Workers perform the performance monitoring tasks.
   d. If a Worker is removed, its performance monitoring jobs are redistributed to other Workers.
   e. If a Worker is added, new performance monitoring jobs are assigned to that Worker.
   f. If you disable and then enable performance monitoring jobs from the GUI, then a new global job distribution takes place.

This section provides the procedures for discovering devices.

- Creating a Discovery Entry
- Discovering on Demand
- Scheduling a Discovery
- Searching Previous Discovery Results

- Editing a Discovery
- Exporting Discovery Results

Creating a Discovery Entry

Complete these steps to create a discovery:

1. Go to **ADMIN** > **Setup** > **Discovery** tab.
2. Click **New**.
3. In the **Range Definition** dialog box, enter the information below.

Settings	Guidelines
Name	[Required] Name of the discovery entry that will be used for reference.
Discovery Type	Select the type of discovery: • **Range Scan** - FortiSIEM will sequentially discover each device in one or more IP ranges and CIDR subnets. • **Smart Scan** - FortiSIEM will first discover the Root IP, which will provide a list of devices that it knows about. Then FortiSIEM will discover each of the devices learnt from the Root IP device. Each of these devices will provide a list of devices they know about, which FortiSIEM will then discover. This process continues until the list of known devices is exhausted. • **AWS Scan** - FortiSIEM will discover the devices in Amazon Web Services (AWS) Cloud learnt via AWS SDK. For AWS Scan to succeed, there needs to be an AWS Credential mapped to aws.com or amazon.com in the IP to Credential mapping. • **L2 Scan** - FortiSIEM will discover only the Layer 2 connectivity of the devices. • **Azure Scan** - FortiSIEM will discover the devices in Azure Cloud learnt via Azure SDK. For Azure Scan to succeed, there needs to be a Credential mapped to azure.com in the IP to Credential mapping. • **Nozomi Scan** - FortiSIEM will discover the devices in Nozomi SCADAguardian and CMC learnt via Nozomi REST API. For Nozomi Scan to succeed, there needs to be a Credential mapped to Nozomi SCADAguardian/CMC in the IP to Credential mapping. See Setting Credentials and the FortiSIEM External Systems Configuration Guide for more information on Credential mapping.
Root IPs	IP address of the Starting device for Smart Scan. See Smart scan definition above.
Include	[Required] A list of IP addresses that will be included for discovery. Allowed IP range syntax is single IP, single range, single CIDR or a list separated by comma – e.g. 10.1.1.1, 10.1.1.2,20.1.1.0/24, 30.1.1.1-30.1.1.10.
Exclude	A list of IP addresses that will be excluded for discovery. Allowed IP range syntax is single IP, single range, single CIDR or a list separated by comma – e.g. 10.1.1.1,

Settings	Guidelines
	10.1.1.2,20.1.1.0/24, 30.1.1.1-30.1.1.10.
Include Types	A list of device Types that will be included for discovery. Click the edit icon to configure the **Range Definition** and **Save**.
Exclude Types	A list of device Types that will be excluded for discovery. Click the edit icon to configure the **Range Definition** and **Save**.
Name resolution	Host names can learn from DNS look up or SNMP/WMI. If these do not match, then choose which discovery method with higher priority. For example, if DNS is chosen then FortiSIEM will get host names from DNS. If DNS lookup fails for an IP, the host names will be obtained from SNMP/WMI.
Options	Select the options for this discovery: - **Do not ping before discovery**: Device will not be pinged before attempting the credentials. - **Ping before discovery**: Device will be pinged before attempting the credentials. A successful ping can shorten discovery times; since FortiSIEM may have to wait for a protocol timeout in case of failed credentials. - **Winexe based discovery -** for windows servers, we discover HyperV metrics and other AD replication metrics via Winexe. However, winexe installs a service and uninstalls the service after it finishes for certain old OS. This setting enables to control this behavior. - **Only discover devices not in CMDB** - **Discover Routes**: Routes help to discover neighboring devices for Smart Scan but “show route” can be expensive for BGP routers. This selection provides a way to control this behavior. - **Include powered off VMs**: This allows the administrator to control whether powered off VMs will be discovered during VCenter discovery - **Include VM templates**: This allows the administrator to control whether VM templates will be discovered during VCenter discovery. - **Set discovered devices as unmanaged**: This allows the administrator to set the discovered devices as unmanaged.

4. Click **Save**.

Discovering on Demand

1. Go to **ADMIN** > **Setup** > **Discovery**.
2. Select the required discovery from the table.
3. Click **Discover**.
4. Click **Results** to view the discovery result.
5. Click **Errors** to check for any errors found during discovery.
   Use the **Run in Background** to run discovery in background while performing other operations.
6. After successful discovery, **Discovery Completed.** message is displayed with the discovery results.

Scheduling a Discovery

Discovery can be a long-running process when performed on a large network, or over a large IP range, and so you may want to schedule it to occur when there is less load on your network or during off hours. You may also want to set up a schedule for the process to run and discover new devices on a regular basis.

1. Go to **ADMIN** > **Setup** > **Discovery**.
2. Click **Scheduled**.
3. Under **Discovery Schedule** dialog box, click **New**.
4. Select from the available ranges.
   You can select multiple ranges and set the order in which discovery will run on them using the up and down arrows.
5. Set the time at which you want discovery to run.
   - For a one-time scheduled discovery, select the **Start Time**.
   - For recurring discoveries, select how often (hourly, daily, weekly, monthly), you want discovery to run, and then enter other scheduling options.
6. Click **Save**.

Searching Previous Discovery Results

Complete these steps to search previously discovered results:

1. Go to **ADMIN** > **Setup** > **Discovery**.
2. Select a discovery result.
3. Click **History**.
4. In the **Discovery History** dialog box, click **View Results**, **View Errors** or **View Changes** to see the related information.

Editing a Discovery

Complete these steps to modify discovery settings:

1. Select the required option from the table below.
   - **Edit** - to edit any scheduled discovery settings.
   - **Delete** - to delete any scheduled discovery.
2. Click **OK**.

Exporting Discovery Results

Complete these steps to export discovery history:

1. Click **History**.
2. In the **Discovery History** dialog box, select the discovery type.
3. Based on the type of information required, select the required option:
   - **View Results** - to see the discovery results
   - **View Errors** - to see the errors during discovery
   - **View Changes** - to see the changes in discovery
4. Click **Export** based on your selection in step#3.
5. Optional - Enter the **User Notes**.

6. Select the **Output Format** as **PDF** or **CSV**.
7. Click **Generate**.
   'Export successful message' is displayed under **Export Report** dialog box.
8. Click **View** to see the discovery results.

Editing Event Pulling

After discovery is complete, FortiSIEM starts pulling events from devices with correct credentials. Examples include Windows Servers via WMI, VMWare VCenter via VMWare SDK, AWS CloudTrail via AWS SDK, etc.

The following section describes the procedures to see the status of these event pulling jobs and turn them on/off.

- Viewing Event Pulling Jobs
- Modifying Event Pulling Jobs
- Checking Status of Event Pulling Jobs
- Exporting Event Pulling Jobs into a Report
- Viewing Event Pulling Reports

Viewing Event Pulling Jobs

Complete these steps to enable event pulling:

1. Go to **ADMIN** > **Setup** > **Pull Events** tab.
2. See the listed jobs:
   - Enabled – the job is enabled at a device level.
   - Device name – name of the device in CMDB.
   - Access IP – IP address with which FortiSIEM accesses this device.
   - Device Type – the device type in CMDB.
   - Organization – the organization to which this device belongs (for a multi-tenant FortiSIEM install).
   - Method – the event pulling method – format - credential name (Access Protocol). An icon appears next to the method, showing the collection status. Hover your cursor over the icon/method to get more details.

Icon	Collection Status
✓	Data for the specific monitor is being collected normally.
☆	Method validated for the specific monitor, but data collection has not yet started.
⏸	Metric collection for the specific monitor not scheduled due to test failure during the beginning of the monitoring cycle, though discovery was successful. In most situations, this is caused by missing or invalid device credentials in FortiSIEM. Recommendation is to check the access protocol credentials and restart discovery.

Icon	Collection Status
⚠	Event pulling method for the specific monitor has failed.

- Maintenance – indicates if this device is in maintenance or not.

3. See **Enabled** option to view the enabled device.
4. Select **Errors** to view the list of errors, if any.

Modifying Event Pulling Jobs

Complete these steps to enable/disable event pulling at all device level (all jobs will be enabled/disabled).

1. Go to **ADMIN** > **Setup** > **Pull Events** tab.
2. Select the device from the list.
3. Select **All** check-box to enable all jobs or deselect to disable.
4. Click **Apply**.

Complete these steps to enable/disable a specific event pulling job for a device:

1. Go to **ADMIN** > **Setup** > **Pull Events** tab.
2. Select the device from the list.
3. Click **Edit**.
4. Check the specific job to enable/disable.
5. Click **Apply**.

Checking Status of Event Pulling Jobs

Complete these steps to the status of event pulling jobs:

1. Go to **ADMIN** > **Setup** > **Pull Events** tab.
2. Select the device from the list.
3. Hover over the method column – the tool tip shows the Execution Status.
4. To see the events generated from the event pulling job, click **Report**.
   A report is run for all the events generated by this event pulling job in the last 10 minutes.

Exporting Event Pulling Jobs into a Report

Complete these steps to export an event pulling job report:

1. Go to **ADMIN** > **Setup** > **Pull Events** tab.
2. Click **Export**.
3. Optional - Enter the **User Notes**.
4. Select the output format to **PDF** or **CSV** and click **Generate**.
5. Click **View** to download and view the report.

Viewing Event Pulling Reports

1. Go to **ADMIN** > **Setup** > **Pull Events** tab.
2. Select **Super/Local** or **Org with collector** or use the **Search** field to view any related jobs.

Editing Performance Monitors

After the discovery is complete, FortiSIEM starts monitoring successfully discovered devices for performance, availability and change. The following section describes the procedure to see the status of these performance monitoring jobs and edit them.

- Viewing Performance Monitoring Jobs
- Enabling/Disabling Performance Monitoring Jobs
- Modifying Performance Monitoring Jobs

Viewing Performance Monitoring Jobs

1. Go to **ADMIN** > **Setup** > **Monitor Performance** tab.
2. To check the **Device Health** details, select the device from the list and click the drop-down near the device name.
3. To check the errors during the monitoring job, select the device and click **More** > **Errors**.
4. To export a Performance Monitor, select the device and click **More** > **Export Monitors**.
5. To generate a Performance Monitoring report for any device(s), select the device and click **More** > **Report**.
6. The **Monitor** column displays the following icons for a quick assessment of monitor jobs. Hover your mouse cursor over the "Not Sheduled" or "Execution Failed" icon in the **Monitor** column to get more information.

Icon	Status
✓	Running.
⏸	Not Scheduled.
⚠	Execution Failed.

Enabling/Disabling Performance Monitoring Jobs

Complete these steps to enable/disable performance monitoring at a device level – all jobs will be enabled/disabled:

1. Go to **ADMIN** > **Setup** > **Monitor Performance** tab.
2. Select the device from the list.
3. Select **Enabled** check-box to enable and select again to disable.
4. Click **Apply**.

Modifying Performance Monitoring Jobs

Complete these steps to enable/disable a specific performance monitoring job for a device:

1. Change the Scope to Local and go to **ADMIN** > **Setup** > **Monitor Performance** tab.
2. Select the device from the list.
3. Click **More** and select the required option:
   - **Edit System Monitors** to select the Protocols and click **Save**.
   - **Edit App Monitors** to select the Protocols and click **Save**.
4. Click **Save**.
5. Click **Apply**.

Another way to enable/disable a specific job or tune monitoring intervals for specific jobs for all devices:

1. Go to **ADMIN** > **Setup** > **Monitor Performance** tab.
2. Click **More** > **Edit Intervals**.
3. In the **Set Intervals** pop-up:
   - Choose the Monitor on the left panel.
   - Choose the device on the middle panel.
   - Click **>>** to move the chosen jobs on the chosen devices to the right panel.
   - Choose the new polling interval or choose **Disabled**.
   - Click **Save**.
4. Click **Apply**.

Configuring Synthetic Transaction Monitoring

A Synthetic Transaction Monitoring (STM) test lets you test whether a service is up or down, and measure the response time. An STM test can range from something as simple as pinging a service, to complex as sending and receiving an email or a nested Web transaction.

This section provides the procedures to set up Synthetic Transaction Monitoring tests.

- Create Monitoring Definition
- Create STM Test
- Edit Monitoring Definition
- Protocol Settings for STM Tests

Creating Monitoring Definition

Complete these steps to create monitor definitions:

1. Go to **ADMIN** > **Setup** > **STM** tab.
2. Under **Step 1: Edit Monitoring Definitions**, click **New**.
3. In the **Add Monitor Definition** dialog box, enter the information below.
   a. Name – enter a name that will be used for reference.
   b. Description – enter a description.
   c. Frequency – how often the STM test will be performed.

   d. Protocol - See 'Protocol Settings for STM Tests' for more information about the settings and test results for specific protocols.
   e. Timeout – when the STM test will give up when it fails.
   f. Probe Settings - enter the timeout period in seconds.
4. Click **Save**.

Creating an STM Test

Complete these steps to create an STM test:

1. Go to **ADMIN** > **Setup** > **STM** tab.
2. Under **Step 2: Create synthetic transaction monitoring entry by associating host name to monitoring definitions**, select **New**.
3. Click **New** and enter the following information:
   a. **Monitoring Definition** – enter the name of the Monitor (previous step).
   b. **Host name or IP/IP Range** – enter a host name or IP or IP range on which the test will be performed.
   c. **Service Ports** – click the Port(s) on which the test will be performed. To add/delete Ports, click **+/-**.
   d. Check **SSL** option to enable SSL for encryption.
   e. Click **Test and Save** to test and save the changes.
   f. Click **Apply**.

Editing Monitoring Definition

Complete these steps to modify monitor definition settings:

1. In the **Step 1: Edit Monitoring Definitions** dialog box, click the tab based on the required action.

Tab	Description
Edit	To modify the Monitoring Definitions.
Delete	To delete the selected Monitoring Definition.
Clone	To duplicate the selected Monitoring Definition.

2. Click **Save**.

Protocol Settings for STM Tests

This table describes the settings associated with the various protocols used for Creating Monitoring Definition.

Protocol	Description	Settings	Notes
Ping	Checks packet loss and round trip time.	**Maximum Packet Loss PCT**: tolerable packet loss. **Maximum Average Round Trip Time**: tol-	Make sure the device is accessible from the FortiSIEM node from which this test is going to be performed.

Protocol	Description	Settings	Notes
		erable round trip time (seconds) from FortiSIEM to the destination and back. If either of these two thresholds are exceeded, then the test is considered as failed.	
LOOP Email	This test sends an email to an outbound SMTP server and then attempts to receive the same email from a mailbox via IMAP or POP. It also records the end-to-end time.	**Timeout**: the time limit by which the end to end LOOP EMAIL test must complete. **Outgoing Settings**: these specify the outgoing SMTP server account for sending the email. • **SMTP Server**: name of the SMTP server. • **User Name**: user account on the SMTP server. • **Email Subject**: content of the subject line in the test email. **Incoming Settings**: These specify the inbound IMAP or POP server account for fetching the email. • **Protocol Type**: choose IMAP or POP. • **Server**: name of the IMAP or POP server. • **User Name**: user account on the IMAP or POP server. • **Email Subject**: content of the subject line in the test email.	Before you set up the test you must have set up access credentials for an outbound SMTP account for sending email, and an inbound POP/IMAP account for receiving email.
HTTP(S) - Selenium Script	This test uses a Selenium script to play back a series of website actions in FortiSIEM.	**Upload**: select the java file you exported from Selenium. **Total Timeout**: the script must complete by this time or the test will be considered failed. **Step Timeout**: each step must complete by this time.	**How to export**: • Make sure Selenium IDE is installed within Firefox browser. • Open Firefox. • Launch Tools > Selenium IDE. From now on, Selenium is recording user actions. • Visit websites. • Once done, stop recording. • Click File > Export Test case as > Java / Junit 4

Protocol	Description	Settings	Notes
			/WebDriver. • Save the file as .java in your desktop. This file has to be inputted in FortiSIEM.
HTTP(S) - Simple	This test connects to a URI over HTTP(s) and checks the response time and expected results.	**URI**: the URI to connect to. **Authentication**: any authentication method to use when connecting to this URI. **Timeout**: this is the primary success criterion - if there is no response within the time specified here, then the test fails. **Contains**: an expected string in the test results. **Does Not Contain**: a string that should not be contained in the test results. The format should be a list of words, separated with a space, e.g. “fortinet firewall”. If **All** is selected, then every listed word is expected, e.g. “fortinet” AND “firewall” are expected to be found within the web page. If **Any** is selected, then any of the listed words are expected, e.g. “fortinet” OR “firewall” is expected to be found within the web page. **Response Code**: an expected HTTP(S) response code in the test results. The default is set to **200 - 204**.	
TCP	This test attempts to connect to the specified port using TCP.	**Timeout**: this is the single success criterion. If there is no response within the time specified here, then the test fails.	
DNS	Checks response time and expected IP address.	**Query**: the domain name that needs to be resolved. **Record Type**: the type of record to test against. **Result**: specify the expected IP address that should be associated with the DNS	

Protocol	Description	Settings	Notes
		entry. **Timeout**: this is the primary success criterion - if there is no response within the time specified here, then the test fails.	
SSH	This test issues a command to the remote server over SSH, and checks the response time and expected results.	**Remote Command**: the command to run after logging on to the system **Timeout**: this is the primary success criterion - if there is no response within the time specified here, then the test fails. **Contains**: an expected string in the test results.	You must set up an SSH credential on the target server before setting up this test. As an example test, you could set **Raw Command** to `ls`, and then set **Contains** to the name of a file that should be returned when that command executes on the target server and directory.
LDAP	This test connects to the LDAP server, and checks the response time and expected results.	**Base DN**: an LDAP base DN you want to run the test against. **Filter**: any filter criteria for the Base DN. **Scope**: any scope for the test. **Timeout**: this is the primary success criterion - if there is no response within the time specified here, then the test fails. **Number of Rows**: the expected number of rows in the test results. **Contains**: an expected string in the test results. **Does Not Contain**: a string that should not be contained in the test results.	You must set up an access credential for the LDAP server before you can set up this test
IMAP	This tests checks connectivity to the IMAP service.	**Timeout**: this is the single success criterion - if there is no response within the time specified here, then the test fails.	
POP	This test checks connectivity to the IMAP service.	**Timeout**: this is the single success criterion - if there is no response within the time specified here, then the test fails.	
SMTP	This test checks connectivity to the SMTP service.	**Timeout**: this is the single success criterion - if there is no response within the time specified here, then the test fails.	
JDBC	This test issues a SQL command over JDBC to a target database,	**JDBC Type**: the type of database to connect to.	

Protocol	Description	Settings	Notes
	and checks the response time and expected results.	**Database Name**: the name of the target database. **SQL**: the SQL command to run against the target database. **Timeout**: this is the primary success criterion - if there is no response within the time specified here, then the test fails. **Number of Rows**: the expected number of rows in the test results. **Contains**: an expected string in the test results. **Does Not Contain**: a string that should not be contained in the test results.	
FTP	This test issues a FTP command to the server and checks expected results.	**Anonymous Login**: choose whether to use anonymous login to connect to the FTP directory. **Remote Directory**: the remote directory to connect to. **Timeout**: this is the primary success criterion - if there is no response within the time specified here, then the test fails.	
TRACE ROUTE	This test issues a trace route command to the destination and parses the results to create PH_DEV_MON_TRACEROUTE events, one for each hop.	**Timeout**: If there is no response from the system within the time specified here, then the test fails. **Protocol Type**: Specifies the IP protocol over which trace route packets are send - current options are UDP, TCP and ICMP. **Max TTL**: Max time to live (hop) value used in outgoing trace route probe packets. **Wait Time**: Max time in seconds to wait for a trace route probe response.	For the trace route from AO to destination D via hops H1, H2, H3, FortiSIEM generates 3 hop by hop PH_DEV_MON_TRACEROUTE events. **First event:** Source AO, destination H1, Min/Max/Avg RTT, Packet Loss for this hop. **Second event:** Source H1, destination H2, Min/Max/Avg RTT, Packet Loss for this hop. **Third event:** Source H2, destination H3, Min/Max/Avg RTT, Packet Loss for this hop. **Fourth event:** Source H3, destination D, Min/Max/Avg RTT, Packet Loss for this hop **Fourth event:** Source H3,

Protocol	Description	Settings	Notes
			destination D, Min/Max/Avg RTT, Packet Loss for this hop.

When an STM test fails, three system rules are triggered, and you can receive an email notification of that failure by creating a notification policy for these rules:

- **Service Degraded - Slow Response to STM**: Detects that the response time of an end-user monitored service is greater than a defined threshold (average over 3 samples in 15 minutes is more than 5 seconds).
- **Service Down - No Response to STM:** Detects a service suddenly went down from the up state and is no longer responding to synthetic transaction monitoring probes.
- **Service Staying Down - No Response to STM**: Detects a service staying down, meaning that it went from up to down and did not come up, and is no longer responding to end user monitoring probes.

Configuring Maintenance Calendars

A Maintenance Calendar displays when a device is undergoing maintenance (likely due to hardware and software upgrades). When a device is in maintenance, it is not monitored for performance, availability and change and the corresponding rules do not trigger.

This section provides the procedures to set up maintenance calendars.

- Create a Maintenance Calendar
  - Specifying a Schedule
  - Specifying the Devices Under Maintenance
- Viewing Existing Maintenance Calendars
- Modifying Existing Maintenance Calendars

Create a Maintenance Calendar

Complete these steps to schedule maintenance:

1. Go to **ADMIN** > **Setup** > **Maintenance** tab.
2. Click **New** and specify the following:

Settings	Guidelines
Name	[Required] Name of the Calendar. This will be displayed on the Calendar.
Description	Description or details about this schedule.
Schedule	[Required] Specify the times during which devices will be in maintenance.
Groups/Devices	Specify the groups/devices and Synthetic Transaction Monitoring (STM) tasks that will be in maintenance.

3. Optional - To generate incidents during maintenance, enable **Generate Incidents for Devices under Maintenance**.
4. Click **Save**.

Specifying a Schedule

1. Click the **Schedule** drop-down list in the **Device Maintenance** window.
2. Enter values for the following options:
   - **Time Range** specifies start time (within the day) and the duration of the maintenance window.
   - **Recurrence Pattern** specifies if and how the maintenance window will repeat.
     - If the maintenance window is one time:
       a. Select **Once** for **Recurrence Pattern**.
       b. Select the specific date on the **Recurrence Range**.
     - If the maintenance window should repeat on certain days of the week:
       a. Select **Recurring Days** and select the Repeat Days and Repeat months.
       b. Select the start and end dates for Recurrence Range.
     - If the maintenance window should repeat on certain months of the year:
       a. Select **Recurring Months** and select the Repeat Months.
       b. Select the **Start From**/**End By** dates for Recurrence Range or select **No end date** to continue the recurrance forever.
3. Click **Save** to apply the changes.

Specifying the Devices Under Maintenance

1. Click the **Groups/Devices** drop-down list in the **Device Maintenance** dialog box.
2. From the **Folders** on the left pane, select either the Devices folder or the STM folder of all the STM jobs defined so far.
3. From the devices/STM jobs shown in the middle pane, select the appropriate ones and click **>** for them to appear in the right **Selections** pane.
4. To select all devices in a folder, select the folder on the left windows and click **>>** to move the folder into the right window.
5. Click **Save**.

Viewing Existing Maintenance Calendars

The existing maintenance calendars can be displayed in various time windows. These options are available on the top-right:

- Monthly view - click **Month**.
- Weekly view - click **Week** or **List (Week)**.
- Day view - click **Day**.

You can navigate to a specific month on the Calendar, click the **<** and **>** buttons on the top-left of the Calendar. To view the current Maintenance, click **Current**.

Modifying Existing Maintenance Calendars

Complete these steps to modify a maintenance schedule:

1. Select the schedule from the Calendar.
2. Click the tab based on the required action:
   - Edit - to edit the scheduled maintenance settings.
   - Delete - to delete the scheduled maintenance.
3. Click **Save**.

Configuring Windows Agent

Starting with version 3.0, Windows Agents can be configured and managed from the FortiSIEM Supervisor node. Windows Agent Manager is not required.

Before proceeding, follow the instructions in the Windows Agent Installation Guide to complete these steps:

1. Install the Windows Agent using the correct installation file.
2. Make sure the Agent appears in the CMDB page of the FortiSIEM GUI, using the host name defined in the installation file.
3. Configure the Windows Server to receive the types logs of interest (see Configuring Windows Servers for FortiSIEM Agents in the Windows Agent Installation Guide).

To receive logs from Windows Agent, you must complete the following steps:

1. Define Windows Agent Monitor Templates
2. Associate Windows Agents to Templates

Once these steps are completed, the Supervisor node will distribute monitoring policies to the Agents and you will be able to see events in FortiSIEM.

This section also covers these topics:

- Viewing Agent Status
- Enabling or Disabling an Agent
- Viewing Files in FortiSIEM
- Verifying Events in FortiSIEM
- Service Level Protection Properties
- Auto Restart Service Behavior
- Configuring Debug Trace Logging without Agent Service Restart
- Configuring the Agent Database Size
- Sample Windows Agent Logs
- Agent Troubleshooting Notes

Define the Windows Agent Monitor Templates

A Windows Monitoring Template consists of:

- Log Settings: Windows Event Logs and Log Files
- Change Settings: File Integrity Monitoring, Registry Changes, Installed Software Changes, Removable media
- Script Settings: WMI Classes and PowerShell Scripts

Complete these steps to add a Windows Agent Monitor Template:

1. Go to **ADMIN** > **Setup** > **Windows Agent** tab.
2. Click **New** under the section **Windows Agent Monitor Templates**.
3. In the **Windows Agent Monitor Template** dialog box, enter the information under each tab with reference to the tables below.

   a. Configure the **Generic** settings with reference to the table below:

Generic settings	Guidelines
Name	Enter the name of the Windows Agent Monitor Template. This name is used as a reference in Template associations.
Description	Enter a description of the Windows Agent Monitor Template.

   b. Configure the **Monitor** settings for Windows Agent using the table below. When done, click **Save**.

Monitor settings	Guidelines
Discover	To configure **Discover** settings: Click the **Discover** checkbox to enable Windows Agent discovery. In the **Hour(s)** field, enter the frequency (in number of hours) that discovery will be done.
Monitor	To configure **Monitor** settings: Click the appropriate **Monitor** checkboxes to enable specific monitoring performance of Windows Agents. • **Uptime** - Select to monitor uptime of Windows Agent. • **CPU** - Select to monitor CPU utilization. • **Memory** - Select to monitor memory utilization. • **Disk** - Select to monitor disk utilization. • **Network** - Select to monitor network utilization. • **Running Applications** - Select to monitoring running applications. In the time field, enter a numeric value for the monitoring frequency. The drop-down time field allows you to choose the frequency in Hour(s) or Minute(s).

   c. Configure the **Event** settings with reference to the table below. Make sure you have completed these steps from the Windows Agent Installation Guide:
   - To enable DNS logging, follow the steps in Configuring Windows DNS.
   - To enable DHCP logging, follow the steps in Configuring Windows DHCP.
   - To enable IIS logging, follow the steps in Configuring Windows IIS.
   - To get sysmon events, follow the steps in Configuring Windows Sysmon.
   - To get print log events, follow the steps in Configuring Print Log.

- To get Windows Terminal Services events, follow the steps in Configuring Windows Terminal Services (RDP - Remote Desktop Protocol)

Event settings	Guidelines
Event Log	To configure **Event log** settings: a. Select the **Type** of log from the drop-down: • **Application** — Events that are logged by Windows Application. Select All, Exchange Server or SQL Server as Source. • **Security** — Log that contains records of login/logout activity or other security-related events specified by the system's audit policy. • **System** — Events that are logged by the operating system components. • **DFS** — Logs to identify the users who accessed the Distributed File System. • **DNS** — DNS Debug logs and Name Resolution Activity logs. • **Hardware Events** — Events related to hardware. • **Key Management Service** — Events related to creation and control of keys used to encrypt your data. • **Setup** — Log files for all actions that occur during installation. • **Windows PowerShell** — Logs related to Windows PowerShell. • **Other** — Any other log type (specify the name under **Event Name** setting.) b. Enter the events to be included under **Include Event** and the ones to exclude under **Exclude Event** by entering each event ID followed by a semicolon as a separator.

d. Select UEBA to turn on UEBA functionality for all hosts running Windows 4.0 or later that are permitted by the UEBA license. For example, if you have 10 UEBA licenses and you applied the template to 100 hosts, system will apply the UEBA license to 10 random hosts. You can turn on/off UEBA on hosts via CMDB.

e. Configure the **User Log** settings with reference to the table below:

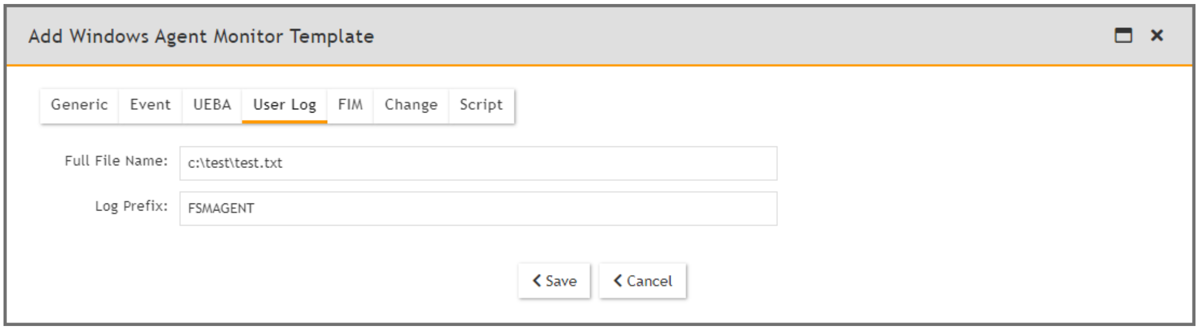
User Log settings	Guidelines
User Log	Click **New** to add the custom log files that must be monitored: • **File**—(Required) Enter the full file name. • **Log Prefix**—(Required) Any prefix to the identify events from this file for better accessibility.

Example:

The contents of the file `C:\test\test.txt` needs to be brought into FortiSIEM for analysis. The log prefix FSMAGENT was chosen. To configure the Windows Agent template in FortiSIEM, from the **User Log** tab, you would take the following steps.

In the **Full file Name** field, you would enter "C:\test\test.txt".

In the **Log Prefix** field, you would enter "FSMAGENT".

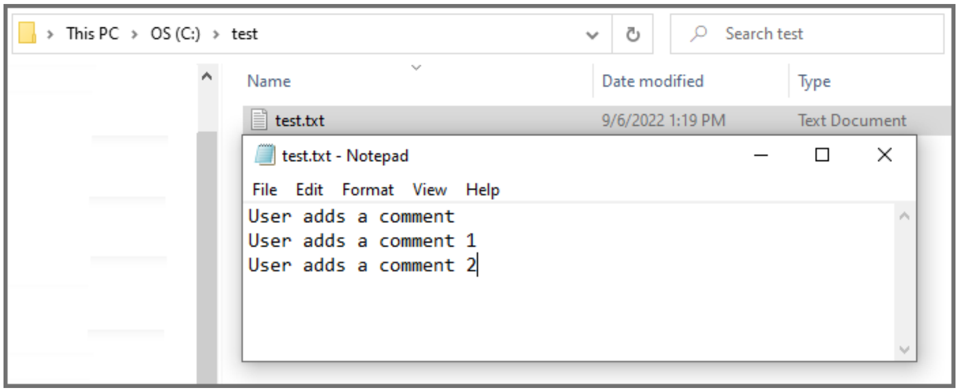


Full File Name: c:\test\test.txt

Log Prefix: FSMAGENT

Suppose the contents of the file C:\test\test.txt looks like this.

```
User adds a comment
User adds a comment 1
User adds a comment 2
```



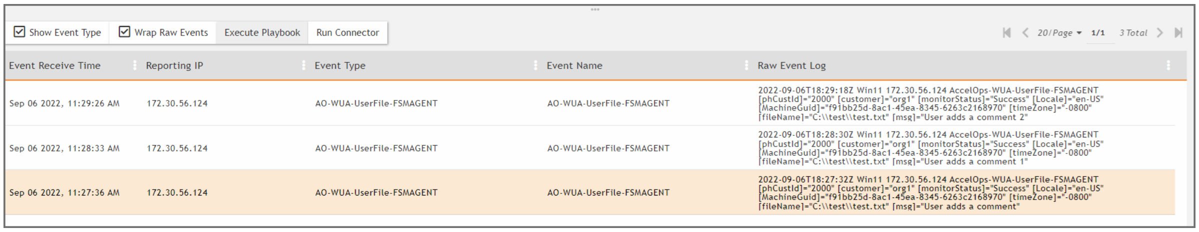
```
User adds a comment
User adds a comment 1
User adds a comment 2
```

FortiSIEM agent will send each line in a separate event.

```
2022-09-06T17:16:27Z Win11 172.30.56.124 AccelOps-WUA-UserFile-FSMAGENT
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]-
]="en-US" [MachineGuid]="f91bb25d-8ac1-45ea-8345-6263c2168970"
[timeZone]="-0800" [fileName]="C:\\test\\test.txt" [msg]="User adds a com-
ment"

2022-09-06T17:18:27Z Win11 172.30.56.124 AccelOps-WUA-UserFile-FSMAGENT
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]-
]="en-US" [MachineGuid]="f91bb25d-8ac1-45ea-8345-6263c2168970"
[timeZone]="-0800" [fileName]="C:\\test\\test.txt" [msg]="User adds a com-
ment 1"

2022-09-06T17:20:27Z Win11 172.30.56.124 AccelOps-WUA-UserFile-FSMAGENT
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]-
]="en-US" [MachineGuid]="f91bb25d-8ac1-45ea-8345-6263c2168970"
```

```
[timeZone]="-0800" [fileName]="C:\\test\\test.txt" [msg]="User adds a com-
ment 2"
```

The event type will be AO-WUA-UserFile-FSMAGENT.



Event Receive Time	Reporting IP	Event Type	Event Name	Raw Event Log
Sep 06 2022, 11:29:26 AM	172.30.56.124	AO-WUA-UserFile-FSMAGENT	AO-WUA-UserFile-FSMAGENT	2022-09-06T18:29:18Z Win11 172.30.56.124 AccelOps-WUA-UserFile-FSMAGENT [phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="f91bb25d-8ac1-45ea-8345-6263c2168970" [timeZone]="-0800" [fileName]="C:\\test\\test.txt" [msg]="User adds a comment 2"
Sep 06 2022, 11:28:33 AM	172.30.56.124	AO-WUA-UserFile-FSMAGENT	AO-WUA-UserFile-FSMAGENT	2022-09-06T18:28:30Z Win11 172.30.56.124 AccelOps-WUA-UserFile-FSMAGENT [phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="f91bb25d-8ac1-45ea-8345-6263c2168970" [timeZone]="-0800" [fileName]="C:\\test\\test.txt" [msg]="User adds a comment 1"
Sep 06 2022, 11:27:36 AM	172.30.56.124	AO-WUA-UserFile-FSMAGENT	AO-WUA-UserFile-FSMAGENT	2022-09-06T18:27:32Z Win11 172.30.56.124 AccelOps-WUA-UserFile-FSMAGENT [phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="f91bb25d-8ac1-45ea-8345-6263c2168970" [timeZone]="-0800" [fileName]="C:\\test\\test.txt" [msg]="User adds a comment"

f. Configure the **FIM** settings with reference to the table below. Make sure you have completed these steps from the Windows Agent Installation Guide:

- To enable logging appropriately, follow the steps in Configure Security Audit Logging Policy.
- To get user meta data in the file auditing logs, follow the steps in Configure File Auditing Policy.
- To enable change events for permission and/or ownership changes to files and/or directories, follow the steps in Configure Audit File System Policy.

FIM settings	Guidelines
FIM	To include the file directory details: a. Click **New** to add the file directory details: • **File/Directory**— Enter the full path of the file directory: • **Include Subfolder(s)** — Select if you must include the directory sub-folders. • **Exclude Subfolder(s)** — Enter any sub-folders to exclude, if any. • **Include File Type** — Enter the file types to include separated by a semi-colon. • **Exclude File Type** — Enter the file types to exclude, if any, separated by a semi-colon. • **On Modify:** • **Push Files**—Select this if you want Windows Agent to push files to FortiSIEM whenever there is a change. **File/Directory** must specify a specific file and not a directory. Also, the absolute file name, including the path, must be specified. For example `C:\temp\fileToBeMonitored.txt`. The files are stored in SVN and are accessible from the Supervisor. These files are displayed in **CMDB > Device > File**. Send only important files, as this can fill up disk space. • **Compare Baseline**—Select this if you want to be alerted when the file changes from a baseline. **File/Directory** must specify a specific file and not a directory. Also, the absolute file name, including the path, must be specified. For example `C:\temp\fileToBeMonitored.txt`. This is common for configuration files that rarely change. If you choose this option, you

FIM settings	Guidelines
	will be asked to provide a copy of the baseline file. Click **Choose File** and upload the file from your workstation. The Supervisor will compute the MD5 checksum and distribute the checksum to the agents for comparison. b. Click **Save**. Use the **Edit**/**Delete** buttons to modify/remove any file directory information.

g. Configure the **Change** settings with reference to the table below:

Change settings	Guidelines
Registry Change	Select the required key(s) to monitor: • **HKEY_CLASSES_ROOT**—key that contains file extension association information, as well as a programmatic identifier, Class ID, and Interface ID data. • **HKEY_CURRENT_USER**—key that contains configuration information for Windows and software specific to the currently logged in user. • **HKEY_LOCAL_MACHINE**—hive that contains the majority of the configuration information for the software you have installed, as well as for the Windows Operating System. • **HKEY_USERS**—key that contains user-specific configuration information of all currently active users on the computer. • **HKEY_CURRENT_CONFIG**—key that acts as a shortcut to a registry key which keeps information about the hardware profile currently used.
Check Every	Set the time period to check the Registry Change in Minute(s) or Hour(s).
Installed Software Change	Select to enable monitoring of any installed software change.
Removable Drive	Select the removable drive to track: • USB drive(s) • CD-DVD drive(s)

h. Configure the **Script** settings with reference to the table below:

Script settings	Guidelines
WMI Classes	To include a WMI Class: a. Click **New** to add a new WMI Class. Select the **Name**, **WMI Class**, and **Attributes** from the drop-down lists (Use ';' as the separator).

Script settings	Guidelines
	b. Set the time period to monitor in Minute(s) or Hour(s) under **Check Every** setting. Use the **Edit**/**Delete** buttons to modify/remove any WMI Classes.
PowerShell Script	To include a PowerShell Script: Click **New** to add a new PowerShell Script and enter the **Name** and **Script**. Use the **Edit**/**Delete** buttons to modify/remove any PowerShell Script.

4. Click **Save**.
   Use the **Edit** button to modify any template or **Delete** button to remove any Windows Agent Monitor template.

Associate Windows Agents to Templates

After defining the monitoring templates, you must associate hosts to templates. To scale to a large number of hosts, this is done via Policies. A Policy is a mapping from Organization and Host to Templates and Collectors. Policies are evaluated in order (lower order or rank is higher priority) and the policy that matches first is selected. Therefore, define the exceptions first followed by broad policies. Hosts are defined in terms of CMDB Device Groups or Business Services. Multiple templates can be used in one Policy and the system detects conflicts, if any.

Complete these steps to associate a Host to Template:

1. Click **New** under the section **Host To Template Associations**.
2. In the **Host To Template Associations** dialog box, enter the information below.

Settings	Guidelines
Name	Name of the Host to Template Association.
Organization	Select the organization.
Host	Use the drop-down list to browse the folders and select the **Devices** or/and **Business Services** to monitor and click **Save**.
Template	Select one or more monitoring templates from the list or select **All Templates** to include all. You can also use the search bar to find any specific template.
Collector	Select the Collector from the list or select **All Collectors** to include all. Agents forward events to Collectors via HTTP(S). A Collector is chosen at random and if that Collector is not available or non-responsive, then another Collector in the list is chosen.

3. Click **Save** and **Apply**.
   A **Rank** is automatically assigned to the association.

You can use the **Edit** button to modify or **Delete** button to remove any template association.

Viewing Agent Status

Complete these steps to view the Windows Agent status for any specific device:

1. Go to **CMDB** > **Devices** and select the device.
   The following fields display the information related to the Agent:
   - Agent Status: status of the Agent on the device
   - Agent Policy: agent policy name
   - Monitor Status: status of monitoring

   The **Agent Status** indicates the following:

Status	Description
Registered	Agent has completed registration but has not received the monitoring template.
Running Active	Agent has received a monitoring template and it is performing properly.
Running Inactive	Agent is running but does not have a monitoring template – the reasons can be (a) no license or (b) incomplete definition - no Collector or Template is defined for that host.
Stopped	Agent is stopped on the Linux Server.
Disconnected	Supervisor did not receive any status from the Agent for the last 10 minutes.

Enabling or Disabling an Agent

Complete these steps to enable or disable Agent for a specific device:

1. Go to **CMDB** > **Devices** and select the required device.
2. Select the **Action** drop-down menu and click **Enable Agent** to enable or **Disable Agent** to disable Agent monitoring for the selected device.

Viewing Files in FortiSIEM

If the FortiSIEM Agent is running on a Server and a FIM policy is enabled with **Push Files On Modify**, then the FortiSIEM Agent will send the files to FortiSIEM when a change is detected. FortiSIEM stores the files in SVN on the Supervisor.

1. Go to the **CMDB** page. Make sure that **AGENT** is one of the **Methods**.
2. Search for the device in CMDB by name.
   Use the host name that you used in the `InstallSettings.xml` file to install the Windows Agent.
3. Click **File** beneath the device table.
   You will see all of the files that were changed since the monitoring template was applied.
4. Select a file.
   If you need to search for a file, set the **From** and **To** dates. The files which changed between those dates will be displayed.

5. Click the file name on the left and its contents will be displayed in the right hand window.
   Each file has a header containing file meta data followed by the actual file content.
   - **FILEPATH:** The full file name, including the path.
   - **ARCHIVE:** Set to true if **ArchiveBit** is set; set to false if it is not.
   - **HASHCODE:** The file hash.
   - **HASHALGO:** The algorithm used to compute file hash.
   - **OWNER:** The file owner.
   - **USER, PERMIT, DENY:** Permissions are specified as a (User, Permit, Deny) triple. This describes the actions that the user is allowed to perform.
   - **MODIFIED_TIME:** The time when the file was last modified.
6. To see the differences between two files, select two files on left and click **Diff**.

Verifying Events in FortiSIEM

Follow the steps below to verify the events in FortiSIEM:

1. Go to **ANALYTICS** tab.
2. Click the **Filters** field.
3. Create the following condition: **Attribute**= Raw Event Log, **Operator** = CONTAIN, **Value** = AccelOps-WUA and click **Save & Run.**
   Note: All event types for all Windows Server generated logs are prefixed by **AccelOps-WUA**.
4. Select the following **Group By**:
   a. Reporting Device Name
   b. Reporting IP
5. Select the following **Display Fields:**
   a. Reporting Device Name
   b. Reporting IP
   c. COUNT(Matched Events)
6. Run the query for the last 15 minutes.
   The query will return all hosts that reported events in the last 15 minutes.

Service Level Protection Properties

When Windows Agent is running, the FSMLogAgent is shown as part of your services on your Windows machine. The ability to Start, Stop, Pause, or Resume this service is disabled. This is intentional, to provide service level protection.

Auto Restart Service Behavior

In the event of a Windows Agent crash, Windows Agent will automatically restart itself after 60 seconds has passed.

Configuring Debug Trace Logging without Agent Service Restart

To enable/disable debug trace logging, you will need to modify the `LogLevel` entry in your Registry Editor. Take the following steps:

1. Using the Registry Editor (Regedit), navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\AccelOps\Agent`.
2. Select `LogLevel` to edit.

- Select Decimal for **Base** and change **Value data** to 2 to enable trace logging. Both "DBGTRACE" and "TRACE" information will be logged.
- Select Decimal for **Base** and change **Value data** to 1 to enable debug logging. Only "DBGTRACE" information will be logged.

  Note: It will take about 2-3 minutes for your change to take effect.

Go to your log folder, typically `C:\ProgramData\AccelOps\Agent\Logs`, and examine your `FSMLogAgent.log` file with any text editor.

Configuring the Agent Database Size

The default size for your Agent Database is 1GB. If you wish to change this, you will need to modify the `MaxDBSizeInMB` entry in your Registry Editor. Take the following steps:

1. Using the Registry Editor (Regedit), navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\AccelOps\Agent`.
2. Select `MaxDBSizeInMB` to edit.
3. Select Decimal for **Base** and change **Value data** to the number of MB you wish to apply as the maximum capacity.

Sample Windows Agent Logs

FortiSIEM Windows Agent Manager generates Windows logs in an easy way to analyze "attribute=value" style without losing any information.

- System Logs
- Application Logs
- Security Logs
- DNS Logs
- DHCP Logs
- IIS Logs
- DFS Logs
- File Content Monitoring Logs
- File Integrity Monitoring Logs
- Installed Software Logs
- Registry change Logs
- Removeable Media Logs
- WMI Logs
- Agent Troubleshooting Notes

System Logs

```
#Win-System-Service-Control-Manager-7036
Thu May 07 02:13:42 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog [monitorStatus]="Success" [eventName]="System"
[eventSource]="Service Control Manager" [eventId]="7036" [eventType]="Information"
[domain]="" [computer]="WIN-2008-LAW-agent"
[user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="May 07 2015 10:13:41"
```

```
[deviceTime]="May 07 2015 10:13:41"
[msg]="The Skype Updater service entered the running state."
```

```
Thu May 07 02:13:48 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog [mon-
itorStatus]="Success" [eventName]="System"
[eventSource]="Service Control Manager" [eventId]="7036" [eventType]="Information"
[domain]="" [computer]="WIN-2008-LAW-agent"
[user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="May 07 2015 10:13:47" [deviceTime]-
]="May 07 2015 10:13:47"
[msg]="The Skype Updater service entered the stopped state."
```

Application Logs

```
#Win-App-MSExchangeServiceHost-2001
Thu May 07 03:05:42 2015 WIN-2008-249.ersijiu.com 10.1.2.249 AccelOps-WUA-WinLog [mon-
itorStatus]="Success" [eventName]="Application" [eventSource]="MSExchangeServiceHost"
[eventId]="2001" [eventType]="Information" [domain]="" [computer]="WIN-2008-249.er-
sijiu.com"
[user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="May 07 2015 11:05:42" [deviceTime]-
]="May 07 2015 11:05:42"
[msg]="Loading servicelet module Microsoft.Exchange.OABMaintenanceServicelet.dll"



#MSSQL
#Win-App-MSSQLSERVER-17137
Thu May 07 03:10:16 2015 WIN-2008-249.ersijiu.com 10.1.2.249 AccelOps-WUA-WinLog [mon-
itorStatus]="Success" [eventName]="Application"
[eventSource]="MSSQLSERVER" [eventId]="17137" [eventType]="Information" [domain]="" [com-
puter]="WIN-2008-249.ersijiu.com" [user]=""
[userSID]="" [userSIDAcctType]="" [eventTime]="May 07 2015 11:10:16" [deviceTime]="May 07
2015 11:10:16"
[msg]="Starting up database 'model'."
```

Security Logs

```
#Win-Security-4624(Windows logon success)
Thu May 07 02:23:58 2015 WIN-2008-249.ersijiu.com 10.1.2.249 AccelOps-WUA-WinLog [mon-
itorStatus]="Success" [eventName]="Security"
[eventSource]="Microsoft-Windows-Security-Auditing" [eventId]="4624" [eventType]-
]="Audit Success" [domain]=""
[computer]="WIN-2008-249.ersijiu.com" [user]="" [userSID]="" [userSIDAcctType]=""
[eventTime]="May 07 2015 10:23:56"
[deviceTime]="May 07 2015 10:23:56" [msg]="An account was successfully logged on."
[[Subject]][Security ID]="S-1-0-0" [Account Name]=""
```

```
[Account Domain]="" [Logon ID]="0x0" [Logon Type]="3" [[New Logon]][Security ID]="S-1-
5-21-3459063063-1203930890-2363081030-500"
[Account Name]="Administrator" [Account Domain]="ERSIJIU" [Logon ID]="0xb9bd3" [Logon
GUID]="{00000000-0000-0000-0000-000000000000}"
[[Process Information]][Process ID]="0x0" [Process Name]="" [[Network Information]]
[Workstation Name]="SP171" [Source Network Address]="10.1.2.171"
[Source Port]="52409" [[Detailed Authentication Information]][Logon Process]="NtLmSsp"
[Authentication Package]="NTLM" [Transited Services]=""
[Package Name (NTLM only)]="NTLM V2" [Key Length]="128" [details]=""
```

DNS Logs

```
#DNS Debug Logs
#AccelOps-WUA-DNS-Started
Thu May 07 02:35:43 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DNS [mon-
itorStatus]="Success"
[msg]="5/7/2015 10:34:05 AM 20BC EVENT   The DNS server has started."


#AccelOps-WUA-DNS-ZoneDownloadComplete
Thu May 07 02:35:43 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DNS [mon-
itorStatus]="Success" [msg]="5/7/2015 10:34:05 AM 20BC EVENT
The DNS server has finished the background loading of zones. All zones are now available
for DNS updates and zone
transfers, as allowed by their individual zone configuration."


#AccelOps-WUA-DNS-A-Query-Success
Thu May 07 02:48:25 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DNS [mon-
itorStatus]="Success" [msg]="5/7/2015
 10:47:13 AM 5D58 PACKET  0000000002B74600 UDP Rcv 10.1.20.232  0002   Q [0001   D
NOERROR] A      (8)testyjyj(4)yjyj(3)com(0)"Thu May 07 02:48:25 2015 WIN-2008-LAW-agent
10.1.2.242 AccelOps-WUA-DNS [monitorStatus]="Success" [msg]="5/7/2015
 10:47:13 AM 5D58 PACKET  0000000002B74600 UDP Snd 10.1.20.232     0002 R Q [8085 A DR
NOERROR] A      (8)testyjyj(4)yjyj(3)com(0)"


#AccelOps-WUA-DNS-PTR-Query-Success
Thu May 07 02:48:25 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DNS [mon-
itorStatus]="Success" [msg]="5/7/2015
10:47:22 AM 5D58 PACKET  00000000028AB4B0 UDP Rcv 10.1.20.232 0002   Q [0001   D   NOERROR]
PTR
(3)223(3)102(3)102(3)102(7)in-addr(4)arpa(0)"
```

```
Thu May 07 02:48:25 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DNS [mon-
itorStatus]="Success" [msg]="5/7/2015
10:47:22 AM 5D58 PACKET  00000000028AB4B0 UDP Snd 10.1.20.232     0002 R Q [8085 A DR
NOERROR] PTR
(3)223(3)102(3)102(3)102(7)in-addr(4)arpa(0)"


#DNS System Logs
#Win-App-DNS-2(DNS Server started)
Thu May 07 02:39:17 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog [mon-
itorStatus]="Success"
[eventName]="DNS Server" [eventSource]="DNS" [eventId]="2" [eventType]="Information"
[domain]="" [computer]="WIN-2008-LAW-agent"
[user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="May 07 2015 10:39:17" [deviceTime]-
]="May 07 2015 10:39:17"
[msg]="The DNS server has started."


#Win-App-DNS-3(DNS Server shutdown)
Thu May 07 02:39:16 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog [mon-
itorStatus]="Success" [eventName]="DNS Server"
[eventSource]="DNS" [eventId]="3" [eventType]="Information" [domain]="" [computer]="WIN-
2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 10:39:16" [deviceTime]="May 07 2015 10:39:16"
[msg]="The DNS server has shut down.
```

DHCP Logs

```
AccelOps-WUA-DHCP-Generic
Thu May 07 05:44:44 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DHCP [mon-
itorStatus]="Success" [ID]="00" [Date]="05/07/15"
[Time]="13:44:08" [Description]="Started" [IP Address]="" [Host Name]="" [MAC Address]=""
[User Name]="" [ TransactionID]="0"
[ QResult]="6" [Probationtime]="" [ CorrelationID]="" [Dhcid.]=""


#AccelOps-WUA-DHCP-IP-ASSIGN
Thu May 07 05:56:41 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DHCP [mon-
itorStatus]="Success" [ID]="10" [Date]="05/07/15"
[Time]="13:56:37" [Description]="Assign" [IP Address]="10.1.2.124" [Host Name]="Agent-
247.yj" [MAC Address]="000C2922118E"
[User Name]="" [ TransactionID]="2987030242" [ QResult]="0" [Probationtime]="" [ Cor-
relationID]="" [Dhcid.]=""
```

```
#AccelOps-WUA-DHCP-Generic(Release)
Thu May 07 05:56:41 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DHCP [mon-
itorStatus]="Success" [ID]="12" [Date]="05/07/15"
[Time]="13:56:33" [Description]="Release" [IP Address]="10.1.2.124" [Host Name]="Agent-
247.yj" [MAC Address]="000C2922118E"
[User Name]="" [ TransactionID]="2179405838" [ QResult]="0" [Probationtime]="" [ Cor-
relationID]="" [Dhcid.]=""
```

```
#AccelOps-WUA-DHCP-IP-LEASE-RENEW
Wed Feb 25 02:53:28 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DHCP [mon-
itorStatus]="Success" [ID]="11" [Date]="02/25/15"
[Time]="10:53:19" [Description]="Renew" [IP Address]="10.1.2.123" [Host Name]="WIN-2008-
249.yj" [MAC Address]="0050568F1B5D"
[User Name]="" [ TransactionID]="1136957584" [ QResult]="0" [Probationtime]="" [ Cor-
relationID]="" [Dhcid.]=""
```

IIS Logs

```
#AccelOps-WUA-IIS-Web-Request-Success
Thu May 07 03:49:23 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-IIS [mon-
itorStatus]="Success" [date]="2015-05-07"
[time]="03:44:28" [s-sitename]="W3SVC1" [s-computername]="WIN-2008-LAW-AG" [s-ip]-
]="10.1.2.242" [cs-method]="GET"
[cs-uri-stem]="/welcome.png" [cs-uri-query]="-" [s-port]="80" [cs-username]="-" [c-ip]-
]="10.1.20.232" [cs-version]="HTTP/1.1"
[cs(User-Agent)]="Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.36+(KHTML,+-
like+Gecko)+Chrome/42.0.2311.135+Safari/537.36"
[cs(Cookie)]="-" [cs(Referer)]="http://10.1.2.242/" [cs-host]="10.1.2.242" [sc-status]-
]="200" [sc-substatus]="0" [sc-win32-status]="0"
[sc-bytes]="185173" [cs-bytes]="324" [time-taken]="78" [site]="Default Web Site" [form-
at]="W3C"
```

```
#AccelOps-WUA-IIS-Web-Client-Error
Thu May 07 03:49:23 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-IIS [mon-
itorStatus]="Success" [date]="2015-05-07" [time]="03:44:37"
[s-sitename]="W3SVC1" [s-computername]="WIN-2008-LAW-AG" [s-ip]="10.1.2.242" [cs-meth-
od]="GET" [cs-uri-stem]="/wrongpage" [cs-uri-query]="-"
[s-port]="80" [cs-username]="-" [c-ip]="10.1.20.232" [cs-version]="HTTP/1.1" [cs(User-
Agent)]="Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.36+(KHTML,+-
like+Gecko)+Chrome/42.0.2311.135+Safari/537.36" [cs(Cookie)]="-" [cs(Referer)]="-" [cs-
host]="10.1.2.242" [sc-status]="404"
[sc-substatus]="0" [sc-win32-status]="2" [sc-bytes]="1382" [cs-bytes]="347" [time-taken]]="0" [site]="Default Web Site" [format]="W3C"
```

```
#AccelOps-WUA-IIS-Web-Forbidden-Access-Denied
Thu May 07 03:30:39 2015 WIN-2008-249.ersijiu.com 10.1.2.249 AccelOps-WUA-IIS [monitorStatus]="Success" [date]="2015-05-07" [time]="03:30:15" [s-ip]="10.1.2.249" [cs-method]="POST" [cs-uri-stem]="/AOCACWS/AOCACWS.svc" [cs-uri-query]="-" [s-port]="80" [cs-username]="-"
[c-ip]="10.1.2.42" [cs(User-Agent)]="-" [sc-status]="403" [sc-substatus]="4" [sc-win32-status]="5" [time-taken]="1" [site]="Default Web Site"
[format]="W3C"
```

DFS Logs

```
#Win-App-DFSR-1002
Thu May 07 03:01:12 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog [monitorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1002" [eventType]="Information" [domain]="" [computer]="WIN-2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:12" [deviceTime]="May 07 2015 11:01:12"
[msg]="The DFS Replication service is starting."
```

```
#Win-App-DFSR-1004
Thu May 07 03:01:12 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog [monitorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1004" [eventType]="Information" [domain]="" [computer]="WIN-2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:12" [deviceTime]="May 07 2015 11:01:12"
[msg]="The DFS Replication service has started."
```

```
#Win-App-DFSR-1006
Thu May 07 03:01:10 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog [monitorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1006" [eventType]="Information" [domain]="" [computer]="WIN-2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:10" [deviceTime]="May 07 2015 11:01:10"
[msg]="The DFS Replication service is stopping."
```

```
#Win-App-DFSR-1008
Thu May 07 03:01:11 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog [mon-
itorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1008" [eventType]="Information" [domain]="" [com-
puter]="WIN-2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:11" [deviceTime]="May 07 2015 11:01:11"
[msg]="The DFS Replication service has stopped."
```

File Content Monitoring Logs

```
#AccelOps-WUA-UserFile
Thu May 07 05:40:08 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-UserFile [mon-
itorStatus]="Success" [fileName]="C:\test\i.txt"
[msg]="another newline adddeddddd"
```

File Integrity Monitoring Logs

The following sections describe various use cases that can be detected by File Integrity Monitoring Logs.

- Use Case 1: File or Directory Created
- Use Case 2: File or Directory Deleted
- Use Case 3: File Content Modified
- Use Case 4: File Content Modified and Upload is Selected
- Use Case 5: File Renamed
- Use Case 6: File Permission Changed
- Use Case 7: File Ownership Changed
- Use Case 8: File Archive Bit Changed
- Use Case 9: File Baseline Changed

Use Case 1: File or Directory Created

Event Type

`AO-WUA-FileMon-Added`

Important Event Attributes

- `userId`: The ID of the user who added the file.
- `domain`: The user's domain for a Domain computer.
- `osObjType`- Can be either File or Directory.
- `fileName`: The name of the file or directory that was added.
- `hashCode, hashAlgo`: The file hash obtained by using the specified algorithm.
- `procName`: The name of the Windows process that was used to create the file.
- `fileOwner`: The owner of the file.
- `targetUserType, targetUser`: The user or group to whom the permission applies.
- `targetFilePermit`: The permitted file operations.

- `targetFileDeny`: The denied file operations.
- `archiveSet`: Is `true` if the Archive bit is set for this file; `false` otherwise.

Reports

`Agent FIM: Windows File/Directory Created/Deleted/Renamed`

Rules

`Agent FIM - Windows File or Directory Created`

Sample Log

```
2020-03-25T07:30:50Z Win-167 10.30.2.167 AccelOps-WUA-FileMon [phCustId]="2000" [cus-
tomer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="e892a6e4-bbfa-4ba6-
bc8c-00d2c31812b4" [timeZone]="+0800" [userId]="jdoe" [domain]="ACME" [eventTime]="Mar 25
2020 07:30:48" [fileName]="C:\\test\\New Text Document.txt" [osObjAction]="Added"
[objectType]="File" [hashCode]-
]="e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855" [hashAlgo]="SHA256"
[procName]="C:\\Windows\\explorer.exe" [msg]="" [archiveSet]="true" [fileOwner]=""
```

Use Case 2: File or Directory Deleted

Event Type

`AO-WUA-FileMon-Removed`

Important Event Attributes

- `userId`: The ID of the user who removed the file.
- `domain`: The user’s domain for a Domain computer.
- `fileName`: The name of the file that was removed.
- `procName`: The Windows process that was used to remove the file.

Report

`Agent FIM: Windows File/Directory Creation/Deletion/Rename`

Rule

`Agent FIM - Windows File or Directory Deleted`

Sample Log

```
2020-03-25T07:43:24Z Win-167 10.30.2.167 AccelOps-WUA-FileMon [phCustId]="2000" [cus-
tomer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="e892a6e4-bbfa-
4ba6-bc8c-00d2c31812b4" [timeZone]="+0800" [userId]="jdoe" [domain]="ACME" [eventTime]-
]="Mar 25 2020 07:43:21" [fileName]="C:\\test\\test1.txt" [osObjAction]="Removed"
[objectType]="Unknown" [hashCode]="" [hashAlgo]="SHA256" [procName]-
]="C:\\Windows\\explorer.exe" [msg]="" [archiveSet]="false" [fileOwner]=""
```

Use Case 3: File Content Modified

Event Type

`AO-WUA-FileMon-Modified`

Important Event Attributes

- `userId`: The user who modified the file.
- `domain`: The user's domain for a Domain computer.
- `fileName`: The name of the file that was modified.
- `procName`: The Windows process that was used to modify the file.
- `hashCode, hashAlgo`: The file hash after modification and the algorithm used to calculate the hash.

Report

`Agent FIM: Windows File Content Modified`

Rule

`Agent FIM - Windows File Content Modified`

Sample Log

```
2020-03-25T10:50:40Z WIN-167.fortinet.wulei.com 10.30.2.167 AccelOps-WUA-FileMon
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="e892a6e4-bbfa-4ba6-bc8c-00d2c31812b4" [timeZone]="+0800" [user-
Id]="jdoe" [domain]="ACME" [eventTime]="Mar 25 2020 10:50:37" [fileName]-
]="C:\\test\\test.txt" [osObjAction]="Modified" [objectType]="File"
[hashCode]="6396e3c19b155770f3ae25afa5f29832d6f35b315407ed88820339b705fd2bcc" [hashAl-
go]="SHA256" [procName]="C:\\Windows\\System32\<br/>otepad.exe" [msg]="" [archiveSet]-
]="true" [fileOwner]=""
```

Use Case 4: File Content Modified and Upload is Selected

Event Type

`PH_DEV_MON_FILE_CONTENT_CHANGE`

Important Event Attributes

- `userId`: The ID of the user who modified the file.
- `domain`: The user's domain for a Domain computer.
- `fileName`: The name of the file that was modified.
- `procName`: The Windows process that was used to modify the file.
- `hashCode, hashAlgo`: The file hash after modification and the algorithm used to calculate the hash.
- `oldSVNVersion`: The SVN revision number of file before the change.
- `newSVNVersion`: The SVN revision number of file after the change.
- `addedItem`: The lines that were added to the file.
- `deletedItem`: The lines that were removed from the file.

Report

`Agent FIM: Windows File Content Modified in SVN`

Rule

`Audited file or directory content modified in SVN`

Sample Log

```
<14>Mar 25 20:30:44 sp3 phPerfMonitor[17521]: [PH_DEV_MON_FILE_CONTENT_CHANGE]:[eventSeverity]=PHL_INFO,[procName]=phPerfMonitor,[fileName]=phSvnUpdate.cpp,[lineNumber]=306,[phCustId]=2000,[hostName]=Win-169,[hostIpAddr]=10.30.3.169,[fileName]]=/C:/test/test.txt,[hashCode]=08998b2cce90ee6695bd8dae82d43137,[oldSVNVersion]=50,[newSVNVersion]=51,[deletedItem]=(none),[addedItem]=333;,[user]=Administrator,[hashAlgo]=SHA256,[phLogDetail]=
```

Use Case 5: File Renamed

Event Type

`AO-WUA-FileMon-Renamed-New-Name`

Important Event Attributes

- `userId`: The ID of the user who renamed the file.
- `domain`: The user's domain for a Domain computer.
- `fileName`: The new name of the file.
- `procName`: The Windows process that was used to rename the file.
- `hashCode, hashAlgo`: The new file hash using the specified algorithm.

Report

`Agent FIM: Windows File/Directory Creation/Deletion/Rename`

Rule

None

Sample Log

```
2020-03-25T09:59:34Z WIN-167.fortinet.wulei.com 10.30.2.167 AccelOps-WUA-FileMon [phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="e892a6e4-bbfa-4ba6-bc8c-00d2c31812b4" [timeZone]="+0800" [userId]="jdoe" [domain]="ACME" [eventTime]="Mar 25 2020 09:59:32" [fileName]]="C:\\test\\test5.txt" [osObjAction]="Renamed [New Name]" [objectType]="File" [hashCode]="2b64c6d9afd8a34ed0dbf35f7de171a8825a50d9f42f05e98fe2b1addf00ab44" [hashAlgo]="SHA256" [procName]="C:\\Windows\\explorer.exe" [msg]="" [archiveSet]="true" [fileOwner]=""
```

Event Type

AO-WUA-FileMon-Renamed-Old-Name

Important Event Attributes

userId: The ID of the user who modified the file.

domain: The user’s domain for a Domain computer.

fileName: The old name of the file before renaming.

procName: The Windows process that was used to remove the file.

Report

Agent FIM: Windows File/Directory Creation/Deletion/Rename

Rule

None

Sample Log

None

Use Case 6: File Permission Changed

Event Type

AO-WUA-FileMon-PermissionChange

Important Event Attributes

- userId: The ID of the user who modified the file permission.
- domain: The user’s domain for a Domain computer.
- objectType: The type of object. Can be File or Directory.
- fileName: The name of the file or directory whose permission was changed.
- procName: The Windows process that was used to change the permission.
- hashCode, hashAlgo: The file hash using the specified algorithm.
- fileOwner: The name of the owner of the file.
- targetUserType, targetUser: The name of the user or group to whom the permission below applies.
- targetFilePermit: The permitted file operations after change.
- targetFileDeny: The denied file operations after change.
- archiveSet: Is true if the Archive bit is set for this file; false otherwise.

Report

Agent FIM: Windows File/Directory Permission Changes

Rule

Agent FIM - Windows File Permission Changed

Sample Log

```
2020-03-25T10:21:00Z WIN-167.fortinet.wulei.com 10.30.2.167 AccelOps-WUA-FileMon
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US"
```

```
[MachineGuid]="e892a6e4-bbfa-4ba6-bc8c-00d2c31812b4" [timeZone]="+0800" [user-
Id]="jdoe" [domain]="ACME" [eventTime]="Mar 25 2020 10:20:58" [fileName]-
]="C:\\test\\test.txt" [osObjAction]="PermissionChange" [objectType]="File"
[hashCode]="7936d255ef43706a93fdd15f4bbfde45e3b2d2b9a0d4cc7c39184cf745ab78c5" [hashAl-
go]="SHA256" [procName]="C:\\Windows\\System32\\dllhost.exe" [msg]="" [archiveSet]-
]="true" [fileOwner]=“Joe” [targetUserType]="USER"
[targetUser]="BUILTIN\Administrators" [targetFilePermit]="ALL" [tar-
getFileDeny]="WRITE"
```

Use Case 7: File Ownership Changed

Event Type

`AO-WUA-FileMon-OwnershipChange`

Important Event Attributes

- `userId`: The ID of the user who modified the file ownership.
- `domain`: The user’s domain for a Domain computer.
- `objectType`: The type of object whose ownership was changed: `File` or `Directory`.
- `fileName`: The name of the file or directory whose ownership was changed.
- `procName`: The Windows process that was used to change ownership.
- `hashCode, hashAlgo`: The file hash using the specified algorithm.
- `fileOwner`: The name of the new file owner.
- `archiveSet`: Is `true` if the `Archive` bit is set for this file; `false` otherwise.

Report

`Agent FIM: Windows File/Directory Ownership Changes`

Rule

`Agent FIM - Windows File Ownership Changed`

Sample Log

```
2020-03-06T07:08:56Z Win-167 10.30.2.167 AccelOps-WUA-FileMon [phCustId]="1" [cus-
tomer]="super" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="e892a6e4-
bbfa-4ba6-bc8c-00d2c31812b4" [timeZone]="+0800" [userId]="Administrator" [domain]-
]="WIN-167" [eventTime]="Mar 06 2020 07:08:53" [fileName]="C:\\test\\test1.txt" [osOb-
jAction]="OwnershipChange" [objectType]="File"
[hashCode]="d17f25ecfbcc7857f7bebea469308be0b2580943e96d13a3ad98a13675c4bfc2" [hashAl-
go]="SHA256" [procName]="C:\\Windows\\System32\\dllhost.exe" [msg]="" [archiveSet]-
]="true" [fileOwner]=“Joe”
```

Use Case 8: File Archive Bit Changed

Event Type

AO-WUA-FileMon-ArchivedBitChange

Important Event Attributes

- userId: The ID of the user who modified the file.
- domain: The user’s domain for a Domain computer.
- objectType: The type of object whose Archive bit was changed: File or Directory.
- fileName: The name of the file whose archive bit was changed.
- procName: The Windows process that was used to change archive bit.
- hashCode, hashAlgo: The file hash using the specified algorithm.
- archiveSet: Is true if the Archive bit is set for this file; false otherwise.

Report

Agent FIM: Windows File/Directory Archive Bit Changes

Rule

Agent FIM - Windows File/Directory Archive Bit Changed

Sample Log

```
2020-03-25T10:02:38Z WIN-167.fortinet.wulei.com 10.30.2.167 AccelOps-WUA-FileMon
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="e892a6e4-bbfa-4ba6-bc8c-00d2c31812b4" [timeZone]="+0800" [user-
Id]="jdoe" [domain]="ACME" [eventTime]="Mar 25 2020 10:02:35" [fileName]-
]="C:\\test\\test.txt" [osObjAction]="ArchivedBitChange" [objectType]="File"
[hashCode]="7936d255ef43706a93fdd15f4bbfde45e3b2d2b9a0d4cc7c39184cf745ab78c5" [hashAl-
go]="SHA256" [procName]="C:\\Windows\\System32\\attrib.exe" [msg]="" [archiveSet]-
]="false" [fileOwner]=""
```

Use Case 9: File Baseline Changed

Event Type

AO-WUA-FileMon-BaselineChange

Important Event Attributes

- userId: The ID of the user who modified the file.
- domain: The user’s domain for a Domain computer.
- fileName: The name of the file that was changed.
- procName: The Windows process that was used to remove the file.
- hashCode, hashAlgo: The file hash using the specified algorithm.
- targetHashCode: The hash of the target file (defined in the GUI).

Report

Agent FIM: Windows File Change from Baseline

Rule

```
Agent FIM - Windows File Changed From Baseline
```

Sample Log

```
2020-03-25T12:52:42Z Win-169 10.30.3.169 AccelOps-WUA-FileMon [phCustId]="2000" [cus-
tomer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="5c83ec12-73fd-4e06-
a396-1f128564f09e" [timeZone]="+0800" [userId]="Administrator" [domain]="WINSRV2012-169"
[fileName]="C:\\test\\test.txt" [osObjAction]="BaselineChange" [hashCode]-
]="c1f79ea2bbfb77bf30446a4c9be762eb" [hashAlgo]="MD5" [tar-
getHashCode]="74DE7651DFC55294CC59240AE514A676" [msg]="
```

Installed Software Logs

```
#AccelOps-WUA-InstSw-Added
Thu May 07 05:28:17 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-InstSw [mon-
itorStatus]="Success" [osObjAction]="Added"
[appName]="7-Zip 9.20 (x64 edition)" [vendor]="Igor Pavlov" [appVersion]="9.20.00.0"


#AccelOps-WUA-InstSw-Removed
Thu May 07 05:28:30 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-InstSw [mon-
itorStatus]="Success" [osObjAction]="Removed"
[appName]="7-Zip 9.20 (x64 edition)" [vendor]="Igor Pavlov" [appVersion]="9.20.00.0"
```

Registry Change Logs

```
#AccelOps-WUA-Registry-Modified
Thu May 07 04:01:58 2015 WIN-2008-249.ersijiu.com 10.1.2.249 AccelOps-WUA-Registry [mon-
itorStatus]="Success" [regKeyPath]-
]="HKLM\\SOFTWARE\\Microsoft\\ExchangeServer\\v14\\ContentIndex\\CatalogHealth\\{0d2a342a-
0b15-4995-93db-d18c3df5860d}" [regValueName]="TimeStamp" [regValueType]="1" [osOb-
jAction]="Modified" [oldRegValue]-
]="MgAwADEANQAtADAANQAtADAANwAgADAAMwA6ADQAOQA6ADQANwBaAAAA"
[newRegValue]="MgAwADEANQAtADAANQAtADAANwAgADAANAA6ADAAMQA6ADQAOABaAAAA"


#AccelOps-WUA-Registry-Removed
Thu May 07 05:25:09 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-Registry [mon-
itorStatus]="Success"
[regKeyPath]="HKLM\\SOFTWARE\\RegisteredApplications" [regValueName]="Skype" [regValueType]-
]="1" [osObjAction]="Removed" [oldRegValue]-
="UwBPAEYAVABXAEEAUgBFAFwAQwBsAGkAZQBuAHQAcwBcAEkAbgB0AGUAcgBuAGUAdAAgAEMAYQBsAGwAXABTAGs-
AeQBwAGUAXABDAGEAcABhAGIAaQBsAGkAdABpAGUAcwBkAGgAZABoAGQAaABkAGgAZABoAGQAAAA="
[newRegValue]=""
```

Removeable Media Monitoring Logs

AO-WUA-RemovableMedia-Insert

```
2022-06-24T19:06:55Z CD-DESK-S 0.0.0.0 AccelOps-WUA-RemovableMedia-Insert [phCustId]-
]="1" [customer]="super" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]-
]="38ba7825-34a2-41b8-8e3d-0548878bef5b" [timeZone]="-0500" [user]="" [domain]=""
[eventTime]="Jun 24 2022 19:06:55" [fileName]="" [diskName]="D:" [isMe-
diaEncrypted]="false" [osObjAction]="" [diskType]="USB" [diskDisplayName]="Samsung
USB" [diskVendor]="samsung" [hwDiskModel]="flash_drive_fit 1100" [msg]="Storage media
inserted."
```

AO-WUA-RemovableMedia-Write-ModifyFile

```
2022-06-24T19:25:06Z CD-DESK-S 192.168.1.147 AccelOps-WUA-RemovableMedia-Write
[phCustId]="1" [customer]="super" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="38ba7825-34a2-41b8-8e3d-0548878bef5b" [timeZone]="-0500" [user]=""
[domain]="" [eventTime]="Jun 24 2022 19:25:02" [fileName]="D:\\agenttest\\Wireshark-
win64-3.6.6.exe" [diskName]="D:" [isMediaEncrypted]="false" [osObjAction]="Modified"
[diskType]="USB" [diskDisplayName]="Samsung USB" [diskVendor]="samsung" [hwDiskModel]-
]="flash_drive_fit 1100" [msg]=""
```

AO-WUA-RemovableMedia-Write-AddFile

```
2022-06-24T19:25:01Z CD-DESK-S 192.168.1.147 AccelOps-WUA-RemovableMedia-Write
[phCustId]="1" [customer]="super" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="38ba7825-34a2-41b8-8e3d-0548878bef5b" [timeZone]="-0500" [user]=""
[domain]="" [eventTime]="Jun 24 2022 19:25:00" [fileName]="D:\\agenttest\\Wireshark-
win64-3.6.6.exe" [diskName]="D:" [isMediaEncrypted]="false" [osObjAction]="Added"
[diskType]="USB" [diskDisplayName]="Samsung USB" [diskVendor]="samsung" [hwDiskModel]-
]="flash_drive_fit 1100" [msg]=""
```

AO-WUA-RemovableMedia-Write-RemoveFile

```
2022-06-24T19:24:01Z CD-DESK-S 192.168.1.147 AccelOps-WUA-RemovableMedia-Write
[phCustId]="1" [customer]="super" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="38ba7825-34a2-41b8-8e3d-0548878bef5b" [timeZone]="-0500" [user]=""
[domain]="" [eventTime]="Jun 24 2022 19:23:56" [fileName]="D:\\agenttest\\WinSCP-
5.17.8-Setup.zip" [diskName]="D:" [isMediaEncrypted]="false" [osObjAction]="Removed"
[diskType]="USB" [diskDisplayName]="Samsung USB" [diskVendor]="samsung" [hwDiskModel]-
]="flash_drive_fit 1100" [msg]=""
```

WMI logs

```
#AccelOps-WUA-WMI-Win32_Processor
Thu May 07 03:53:33 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WMI
```

```
[monitorStatus]="Success"  [__CLASS]="Win32_Processor"
[AddressWidth]="64" [Architecture]="9" [Availability]="3" [Caption]="Intel64 Family 6
Model 26 Stepping 5" [ConfigManagerErrorCode]="" [ConfigManagerUserConfig]=""
[CpuStatus]="1" [CreationClassName]="Win32_Processor" [CurrentClockSpeed]="2266" [Cur-
rentVoltage]="33"
[DataWidth]="64" [Description]="Intel64 Family 6 Model 26 Stepping 5" [DeviceID]-
]="CPU0" [ErrorCleared]="" [ErrorDescription]=""
[ExtClock]="" [Family]="12" [InstallDate]="" [L2CacheSize]="0" [L2CacheSpeed]=""
[L3CacheSize]="0" [L3CacheSpeed]="0"
[LastErrorCode]="" [Level]="6" [LoadPercentage]="8" [Manufacturer]="GenuineIntel"
[MaxClockSpeed]="2266"
[Name]="Intel(R) Xeon(R) CPU           E5520  @ 2.27GHz" [NumberOfCores]="1" [Num-
berOfLogicalProcessors]="1"
[OtherFamilyDescription]="" [PNPDeviceID]="" [PowerManagementCapabilities]="" [Power-
ManagementSupported]="0"
[ProcessorId]="0FEBFBFF000106A5" [ProcessorType]="3" [Revision]="6661" [Role]="CPU"
[SocketDesignation]="CPU socket #0"
[Status]="OK" [StatusInfo]="3" [Stepping]="" [SystemCreationClassName]="Win32_Com-
puterSystem" [SystemName]="WIN-2008-LAW-AG"
UniqueId]="" [UpgradeMethod]="4" [Version]="" [VoltageCaps]="2"
```

Agent Troubleshooting Notes

A Windows Agent can be in following states (shown in CMDB):

- Registered
- Running Inactive
- Running Active
- Disabled
- Disconnected

When an Agent is installed and registered, then it is in Registered state. The following audit event is generated: `PH_AUDIT_AGENT_INSTALLED`.

When a monitoring template is assigned to the device, then the state moves to Running Inactive. When the agent receives the template and starts monitoring, then the state moves to Running Active. In both cases, the following audit event is generated: `PH_AUDIT_AGENT_RUNNING`.

Agent periodically sends heartbeat messages. When a heartbeat not received for 10 minutes, the state moves to Disconnected and the audit event `PH_AUDIT_AGENT_NOTRESPONDING` is generated. Status is checked every 1 hour. At that time, if we heard from the Agent in the last 15 minutes, the state moves back to Running Inactive and a `PH_AUDIT_AGENT_RUNNING` audit event is generated.

If the Agent is disabled from the GUI, the state moves to Disabled and `PH_AUDIT_AGENT_DISABLED` audit event is generated.

If the Agent is uninstalled or the service is stopped, then the state moves to Disconnected and the audit event `PH_AUDIT_AGENT_NOTRESPONDING` is generated.

Audit events are generated at state transitions, however, the event `PH_AUDIT_AGENT_NOTRESPONDING` is generated every hour to identify all agents that are currently disconnected. A nested query can be run to detect Agents that did not report in the last N hours. Note that `PH_AUDIT` events must be queried with `System Event Category = 2`. Rules do not need this condition.

Configuring Linux Agent

Linux Agents can be configured and managed from the FortiSIEM Supervisor node.

Before proceeding, install the Linux Agent following the instructions in the *Linux Agent Installation Guide.*

To receive logs from the Linux Agent, you must complete the following steps

1. Define the Linux Agent Monitoring Templates.
2. Associate Linux Agents to Templates.

Once these steps are completed, the Supervisor node will distribute monitoring policies to the Linux Agents and you will be able to see events in FortiSIEM.

Note: FortiSIEM Linux Agent will not perform file integrity monitoring on the `/root` directory.

This section also covers these topics.

- Viewing Agent Status
- Enabling or Disabling an Agent
- Viewing Files in FortiSIEM
- File Integrity Monitoring Logs
- Agent Troubleshooting Notes

Define the Linux Agent Monitor Templates

Complete these steps to add a Linux Agent Monitor Template:

1. Go to **ADMIN** > **Setup** > **Linux Agent** tab.
2. Click **New** under the section **Linux Agent Monitor Templates**.
3. In the **Linux Agent Monitor Template** dialog box, enter the information below.

Generic tab:

Configure the **Generic** settings with reference to the table below:

Generic Settings	Guidelines
Name	[Required] Enter the name of the FortiSIEM Linux Agent. This name is used as a reference in Template associations.

Generic Settings	Guidelines
Description	[Required] Enter the description about the FortiSIEM Linux Agent.

Monitor tab

Configure the **Monitor** settings with reference to the table below:

Monitor settings	Guidelines
Discover	To configure **Discover** settings: Click the **Discover** checkbox to enable Linux Agent discovery. In the **Hour(s)** field, enter the frequency (in number of hours) that discovery will be done.
Monitor	To configure **Monitor** settings: Click the appropriate **Monitor** checkboxes to enable specific monitoring performance of Linux Agents. • **Uptime** - Select to monitor uptime of Linux Agent. • **CPU** - Select to monitor CPU utilization. • **Memory** - Select to monitor memory utilization. • **Disk** - Select to monitor disk utilization. • **Network** - Select to monitor network utilization. • **Running Applications** - Select to monitoring running applications. In the time field, enter a numeric value for the monitoring frequency. The drop-down time field allows you to choose the frequency in Hour(s) or Minute(s).

Syslog tab:

Configure the **Syslog** settings with reference to the table below:

Syslog Settings	Guidelines
Syslog	Select the **Facility** with the corresponding Syslog levels: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Info** • **Debug**

Log File tab:

Configure the **Log File** settings with reference to the table below:

Log File Settings	Guidelines
Log Files	Click **New** to add the custom log files to monitor: • **File**—(Required) Enter the full file name. • **Log Prefix**—(Required) Any prefix to the identify events from this file for better accessibility.

If you cannot collect logs from the specified log file, please check if SELinux is enabled and that the SELinux context configuration for the file is correct. The `var_log_t` type is needed for the log file.

To check for SELinux context, assuming `/testLinuxAgent/testLog.log` is the log file, run the following command:

```
ls -Z /testLinuxAgent/testLog.log
```

The expected result should have `var_log_t` in the output, as shown here:

```
system_u:object_r:var_log_t:s0 /testLinuxAgent/testLog.log
```

If you need to set `var_log_t` type to the log file, run the following commands:

```
chcon -t var_log_t /testLinuxAgent
chcon -t var_log_t /testLinuxAgent/testLog.log
```

FIM tab:

Configure the **FIM** settings with reference to the table below:

FIM Settings	Guidelines
FIM	Click **New** to add the files to monitor: • **Include File/Directory**—Enter the file or directory to monitor. • **Exclude File/Directory**—Enter the file or directory to exclude from monitoring using a semi-colon (`;`) as a separator. • **Action**—Select the actions to monitor when there is an event in the included file or directory: ◦ **All**—All of the following actions will be monitored. ◦ **Open**—One or more of the monitored files or directories has been opened. ◦ **Close**—One or more of the monitored files or directories has been closed. ◦ **Create**—A file or directory has been created in one or more of the monitored files or directories. ◦ **Modify**—One or more of the monitored files or directories has been edited. ◦ **Delete**—One or more of the monitored files or directories has been deleted.

FIM Settings	Guidelines
	- **Attribute Change**—An attribute belonging to one or more of the monitored files or directories has been changed. • **On Modify** (appears only if All or Modify is selected): - **Push Files**—Select this if you want Linux Agent to push files to FortiSIEM whenever there is a change. The files are stored in SVN and are accessible from the Supervisor. These files are displayed in **CMDB > Device > File**. Send only important files, as this can fill up disk space. - **Compare Baseline**—Select this if you want to be alerted when the file changes from a baseline. This is common for configuration files that rarely change. If you choose this option, you will be asked to provide a copy of the baseline file. Click **Choose File** and upload the file from your workstation. The Supervisor will compute the MD5 checksum and distribute the checksum to the agents for comparison.

Process Monitoring tab:

Configure the **Process Monitoring** settings with reference to the table below:

Process Monitoring Settings	Guidelines
Process Monitoring	Check the **Process Monitoring** checkbox to collect Linux Server related performance metrics.

4. Click **Save**

Associate Linux Agents to Templates

After defining the monitoring templates, associate the hosts to templates. To scale to large number of Hosts, this is done via Policies. A Policy is a mapping from Organization and Host to Templates and Collectors. Policies are evaluated in order (lower order or rank is higher priority) and the policy that matches first is selected. Therefore, define the exceptions first followed by broad policies. Hosts can be defined in terms of CMDB Device Groups or Business Services. Multiple templates can be used in one Policy and the system detects conflicts, if any.

Complete these steps to associate a Host to Template:

1. Click **New** under the section **Host To Template Associations**.
2. In the **Host To Template Associations** dialog box, enter the information below.

Settings	Guidelines
Name	Name of the Host to Template Association.

Settings	Guidelines
Organization	Select the organization.
Host	Use the drop-down list to browse the folders and select the items.
Template	Select one or more monitoring templates from the list or select **All Templates** to select all. You can also use the search bar to find a specific template.
Collector	Select the Collector from the list or select **All Collectors** to select all. Agents forward events to Collectors via HTTP(S). A Collector is chosen at random and if that Collector is not available or non-responsive, then another Collector in the list is chosen.

3. Click **Save** and **Apply**.
   A **Rank** number is automatically assigned to the association.

You can use the **Edit** button to modify or **Delete** button to remove any template association.

Viewing Agent Status

Complete these steps to view the Agent status for any specific device:

1. Go to **CMDB** > **Devices** and select the device.
   The following fields displays the information related to the Agent:
   - Agent Status: status of the Agent running on the device.
   - Agent Policy: agent policy.
   - Monitor Status: status of monitoring.

   The **Agent Status** indicates the following:

Status	Description
Registered	Agent has completed registration but has not received the monitoring template.
Running Active	Agent has received a monitoring template and it is performing properly.
Running Inactive	Agent is running but does not have a monitoring template – the reasons can be (a) no license or (b) incomplete definition - no Collector or Template is defined for that host.
Stopped	Agent is stopped on the Linux Server.
Disconnected	Supervisor did not receive any status from the Agent for the last 10 minutes.

Enabling or Disabling an Agent

Complete these steps to enable or disable Linux Agent for a specific device:

1. Go to **CMDB** > **Devices** and select the required device.
2. Select the **Action** drop-down menu and click **Enable Agent** to enable or **Disable Agent** to disable Agent monitoring for the selected device.

Viewing Files in FortiSIEM

If the FortiSIEM Agent is running on a Server and a FIM policy is enabled with **Push Files On Modify**, then the FortiSIEM Agent will send the files to FortiSIEM when a change is detected. FortiSIEM stores the files in SVN on the Supervisor.

1. Go to the **CMDB** page. Make sure that **AGENT** is one of the **Methods**.
2. Search for the device in CMDB by name.
   Use the host name that you used to install the Linux Agent.
3. Click **File** beneath the device table.
   You will see all of the files that were changed since the monitoring template was applied.
4. Select a file.
   If you need to search for a file, set the **From** and **To** dates. The files which changed between those dates will be displayed.
5. Click the file name on the left and its contents will be displayed in the right hand window.
   Each file has a header containing file meta data followed by the actual file content.
   - **OWNER**: The name of the file owner
   - **GROUP**: User group for specifying file permissions.
   - **PERMISSION=USER: “OWNER”, PERMIT: "..."**: The file owner’s permissions.
   - **PERMISSION=GROUP: “MEMBER”, PERMIT: "..."**:: The group member’s file permissions.
   - **PERMISSION=GROUP: “OTHER”, PERMIT: "..."**:: Other group file permissions.
   - **FILEPATH:** The full file name, including the path.
   - **HASHCODE:** The file hash.
   - **HASHALGO:** The algorithm used to compute file hash.
   - **MODIFIED_TIME:** The time when the file was last modified.
6. To see the differences between two files, select two files on left and click **Diff**.

File Integrity Monitoring Logs

The following sections describe various use cases that can be detected by File Integrity Monitoring Logs.

- Use Case 1: File Created
- Use Case 2: File Deleted
- Use Case 3: File Attributes Changed
- Use Case 4: File Modified
- Use Case 5: File Modified and Upload is Selected
- Use Case 6: File Baseline Changed
- Use Case 7: File Renamed
- Use Case 8: File Accessed
- Use Case 9: File Opened
- Use Case 10: File Closed
- Agent Troubleshooting Notes

Use Case 1: File Created

Event Type

FSM_LINUX_FILE_CREATE

Important Event Attributes

- targetOsObjType: The type of object that was created: File or Directory.
- targetOsObjName: The name of the file or directory.
- user: The name of the user who made the change.
- hashCode: The hash code of the file.
- hashAlgo: The algorithm used to create the file.

Reports

Agent FIM: Linux File/Directory Creation/Deletion/Movement/Unmount Activity

Rules

Agent FIM - Linux File or Directory Created

Sample Log

```
Fri Mar 27 09:39:25 2020 centos7: [FSM_LINUX_FILE_CREATE]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=CREATE,[targetObjType]=File,[targetObjName]="/mlm/a.log",[hashCode]="d41d8cd98f00b204e9800998ecf8427e",[hashAlgo]="MD5",[user]=root
```

Use Case 2: File Deleted

Event Type

FSM_LINUX_FILE_DELETE

Important Event Attributes

- targetOsObjType: The type of object that was created: File or Directory.
- targetOsObjName: The name of the file or directory.
- user: The name of the user who made the change.

Reports

Agent FIM: Linux File/Directory Creation/Deletion/Movement/Unmount Activity

Rules

Agent FIM - Linux File or Directory Deleted

Sample Log

```
Fri Mar 27 09:43:11 2020 centos7: [FSM_LINUX_FILE_DELETE]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=DELETE,[targetObjType]=File,[targetObjName]="/mlm/k.log",[user]=root
```

Use Case 3: File Attributes Changed

Event Type

FSM_LINUX_FILE_ATTRIB_CHANGE

Important Event Attributes

- `targetOsObjType`: The type of object: `File` or `Directory`.
- `targetOsObjName`: The name of the file or directory.
- `user`: The name of the user who made the change.
- `fileOwner`: The name of the owner of the file or directory.
- `userGrp`: The name of the user group for the file or directory.
- `userPerm`: The permission granted to the owner.
- `groupPerm`: The permission granted to the user group.
- `otherPerm`: Other permissions.

Reports

`Agent FIM: Linux File/Directory Ownership or Permission Changes`

Rules

- `Agent FIM - Linux Directory Ownership or Permission changed`
- `Agent FIM - Linux File Ownership or Permission Changed`

Sample Log

```
Fri Mar 27 09:45:27 2020 centos7: [FSM_LINUX_FILE_ATTRIB_CHANGE]: [objectType]-
]=Directory,[objectName]=/mlm,[objectAction]=ATTRIBUTE_CHANGE,[targetObjType]=File,
[targetObjName]="/mlm/mlm.txt",[fileOwner]="root",[groupName]="mlm",[user-
Perm]="READ,WRITE,EXEC",[groupPerm]="READ,EXEC",[otherPerm]="READ,EXEC",[user]=root
```

Use Case 4: File Modified

Event Type

`FSM_LINUX_FILE_MODIFY`

Important Event Attributes

- `targetOsObjName`: The name of the file.
- `user`: The name of the user who made the change.
- `hashCode`: The hash code of the file.
- `hashAlgo`: The algorithm used to create the file.

Reports

`Agent FIM: Linux File Content Modified`

Rules

`Agent FIM - Linux File Content Modified`

Sample Log

```
Fri Mar 27 09:47:06 2020 centos7: [FSM_LINUX_FILE_MODIFY]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=MODIFY,[targetObjType]=File,[tar-
getObjName]="/mlm/mlm.txt",[hashCode]=5d71f074cf9a75e0324f210160d4b9cb,[hashAlgo]=md5,
[user]=root
```

Use Case 5: File Modified and Upload is Selected

Event Type

`PH_DEV_MON_FILE_CONTENT_CHANGE`

Important Event Attributes

- `userId`: The ID of the user who modified the file.
- `domain`: The user's domain for a Domain computer.
- `fileName`: The name of the file that was modified.
- `procName`: The Windows process that was used to modify the file.
- `hashCode, hashAlgo`: The file hash after modification and the algorithm used to calculate the hash.
- `oldSVNVersion`: The SVN revision number of the file before change.
- `newSVNVersion`: The SVN revision number of the file after change.
- `addedItem`: The lines that were added to the file.
- `deletedItem`: The lines that were removed from the file.

Reports

`Agent FIM: Linux File Content Modified in SVN`

Rules

`Audited file or directory content modified in SVN`

Sample Log

```
<14>Mar 27 09:51:30 sp3 phPerfMonitor[6340]: [PH_DEV_MON_FILE_CONTENT_CHANGE]:
[eventSeverity]=PHL_INFO,[procName]=phPerfMonitor,[fileName]=phSvnUpdate.cpp,[lineNum-
ber]=306,[phCustId]=2000,[hostName]=centos7,[hostIpAddr]=10.30.3.39,[fileName]-
]=/mlm/mlm.txt,[hashCode]=ac399331afa9d1f13618c9eff36ed51c,[oldSVNVersion]=53,
[newSVNVersion]=54,[deletedItem]=(none),[addedItem]=retest;,[user]=root,[hashAl-
go]=MD5,[phLogDetail]=
```

Use Case 6: File Baseline Changed

Event Type

`FSM_LINUX_FILE_CHANGE_BASELINE`

Important Event Attributes

- `targetOsObjName`: The name of the baseline file.
- `user`: The name of the user who made the change.
- `hashCode`: The hash code of the file after modification.
- `hashAlgo`: The algorithm used to create the file hash.
- `targetHashCode`: The hash code of the baseline file.

Reports

`Agent FIM: Linux File Change from Baseline`

Rules

`Agent FIM - Linux File Changed From Baseline`

Sample Log

```
Fri Mar 27 09:51:23 2020 centos7: [FSM_LINUX_FILE_CHANGE_BASELINE]: [fileName]-
]=/mlm/mlm.txt,[targetHashCode]="aa63e826654915e0e2e1da385e6d14f8",[hashCode]-
]="ac399331afa9d1f13618c9eff36ed51c",[hashAlgo]="MD5",[user]=root
```

Use Case 7: File Renamed

Event Types

- `FSM_LINUX_FILE_MOVED_TO`
- `FSM_LINUX_FILE_MOVED_FROM`

Important Event Attributes

- `targetOsObjType`: The file type: `File` or `Directory`.
- `targetOsObjName`: The file or directory name.
- `user`: The name of the user who renamed the file.

Reports

`Agent FIM: Linux File/Directory Creation/Deletion/Movement/Unmount Activity`

Rules

None

Sample Logs

```
Fri Mar 27 09:57:42 2020 centos7: [FSM_LINUX_FILE_MOVED_FROM]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=MOVED_FROM,[targetObjType]=File,[tar-
getObjName]="/mlm/bb.log",[user]=root


Fri Mar 27 09:57:42 2020 centos7: [FSM_LINUX_FILE_MOVED_TO]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=MOVED_TO,[targetObjType]=File,[tar-
getObjName]="/mlm/cc.log",[user]=root
```

Use Case 8: File Accessed

Event Type

`FSM_LINUX_FILE_ACCESS`

Important Event Attributes

- `targetOsObjType`: The file type: `File` or `Directory`.
- `targetOsObjName`: The file or directory name.
- `user`: The name of the user who accessed the file.

Reports

None

Rules

None

Sample Log

```
Fri Mar 27 10:05:28 2020 centos7: [FSM_LINUX_FILE_ACCESS]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=ACCESS,[targetObjType]=File,[targetObjName]="/mlm/mlm.txt",[user]=root
```

Use Case 9: File Opened

Event Type

`FSM_LINUX_FILE_OPEN`

Important Event Attributes

- `targetOsObjType`: The file type: `File` or `Directory`.
- `targetOsObjName`: The file or directory name.
- `user`: The name of the user who opened the file.

Reports

None

Rules

None

Sample Log

```
Fri Mar 27 09:57:40 2020 centos7: [FSM_LINUX_FILE_OPEN]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=OPEN,[targetObjType]=Directory,[targetObjName]="/mlm",[user]=root
```

Use Case 10: File Closed

Event Types

- FSM_LINUX_FILE_CLOSE_WRITE
- FSM_LINUX_FILE_CLOSE_NOWRITE

Important Event Attributes

- targetOsObjType: The file type: File or Directory.
- targetOsObjName: The file or directory name.
- user: The name of the user who closed the file.

Reports

None

Rules

None

Sample Logs

```
Fri Mar 27 09:57:36 2020 centos7: [FSM_LINUX_FILE_CLOSE_WRITE]: [objectType]-
]=Directory,[objectName]=/mlm,[objectAction]=CLOSE_WRITE,[targetObjType]=File,[tar-
getObjName]="/mlm/bb.log",[user]=root


Fri Mar 27 10:05:28 2020 centos7: [FSM_LINUX_FILE_CLOSE_NOWRITE]: [objectType]-
]=Directory,[objectName]=/mlm,[objectAction]=CLOSE_NOWRITE,[targetObjType]=File,[tar-
getObjName]="/mlm/mlm.txt",[user]=root
```

Agent Troubleshooting Notes

A Linux Agent can be in following states (shown in CMDB):

- Registered
- Running Inactive
- Running Active
- Disabled
- Disconnected

When an Agent is installed and registered, then it is in Registered state. The following audit event is generated: PH_AUDIT_AGENT_INSTALLED.

When a monitoring template is assigned to the device, then the state moves to Running Inactive. When the agent receives the template and starts monitoring, then the state moves to Running Active. In both cases, the following audit event is generated: PH_AUDIT_AGENT_RUNNING.

Agent periodically sends heartbeat messages. When a heartbeat not received for 10 minutes, the state moves to Disconnected and the audit event PH_AUDIT_AGENT_NOTRESPONDING is generated. Status is checked every 1 hour. At that time, if we heard from the Agent in the last 15 minutes, the state moves back to Running Inactive and a PH_AUDIT_AGENT_RUNNING audit event is generated.

If the Agent is disabled from the GUI, the state moves to Disabled and PH_AUDIT_AGENT_DISABLED audit event is generated.

If the Agent is uninstalled or the service is stopped, then the state moves to Disconnected and the audit event `PH_AUDIT_AGENT_NOTRESPONDING` is generated.

Audit events are generated at state transitions, however, the event `PH_AUDIT_AGENT_NOTRESPONDING` is generated every hour to identify all agents that are currently disconnected. A nested query can be run to detect Agents that did not report in the last N hours. Note that `PH_AUDIT` events must be queried with `System Event Category = 2`. Rules do not need this condition.

Configuring FortiSIEM Instance for FortiSIEM Manager

To configure a FortiSIEM instance to connect with FortiSIEM Manager, take the following steps from Supervisor.

Note: Make sure the FortiSIEM instance has been added to Manager before registering. For more information on adding a FortiSIEM instance to Manager, see Add a FortiSIEM Instance.

1. In the **FortiSIEM Manager FQDN/IP** field, enter the FortiSIEM Manager Fully Qualified Domain Name (FQDN) or IP address.
2. In the **FortiSIEM Instance Name** field, enter the name for this instance.
3. In the **Account** field, enter your account user name for FortiSIEM Manager that you created while adding the instance.
4. In the **Password** field, enter the password associated with the account.
5. In the **Confirm Password** field, re-enter your password.
6. Click **Test** to validate the configuration.
7. Click **Register**.

Unregister FortiSIEM Manager Instance

To unregister the FortiSIEM instance from FortiSIEM Manager, click **Unregister**.

Deleting FortiSIEM Manager Instance

To delete the FortiSIEM Manager instance, click **Delete**.

Testing FortiSIEM Instance

To test the FortiSIEM instance connection, click **Test**.

Device Support

The following sections provide procedures to configure device support:

Working with Devices or Applications

You can create a device/application if it is not available in the list for creating a parser or monitoring under **ADMIN** > **Device Support** > **Devices/Apps**.

This section provides the procedure to configure devices or applications.

- Adding a Device or Application
- Modifying a Device or Application

Adding a Device or Application

Complete these steps to add a new device or application:

1. Go to **ADMIN** > **Device Support** > **Devices/Apps** tab.
2. Click **New**.
3. In the **Device/Application Type Definition** dialog box, enter the information below.

Settings	Guidelines
Category	[Required] Select the **Device** or **Application** from the drop-down list.
Vendor	[Required] Vendor of the device or application.
Model	[Required] Device or application model.
Version	[Required] Version number of the device or application.
Device/App Group	[Required] Select the group where you want to add this new device/application
Biz Service Group	Select the Biz Service group.
Access Protocol	Select the Access Protocol from the drop-down.
App Package Group	This setting is applicable only for 'Application' category. Enter the app package group here.
Description	Description about the device or application.

4. Click **Save**.
   The new device(s)/application(s) appears in the list.
5. Select the device(s)/application(s) from the list and click **Apply**.

You can clone an existing device/application by clicking **Clone** and modify as necessary.

Modifying a Device or Application

Complete these steps to modify a device or application:

1. Select one or more device(s)/application(s) to edit from the list.
2. Click the required option:
   - **Edit** to modify any device/application setting.
   - **Delete** to remove any device /application.
3. Click **Save**.

Working with Event Attributes

Event attributes are used to capture parsed information from events. Create a new attribute if the one you want to use for your custom parser or monitor is not listed in **ADMIN** > **Device Support** > **Event Attributes**.

This section provides the procedure to create event attributes.

- Adding an Event Attribute
- Modifying an Event Attribute

Adding an Event Attribute

Complete these steps to add a new event attribute:

1. Go to **ADMIN** > **Device Support** > **Event Attributes** tab.
2. Click **New**.
3. In the **Add Event Attribute Type Definition** dialog box, enter the information below.

Settings	Guidelines
Name	[Required] Event attribute name
Display Name	[Required] Display name of the event attribute
Value Type	[Required] Select the value type from the drop-down to associate with the event attribute type.
Display Format	Units in which the event attribute has to be displayed
Description	Description of the event attribute

4. Click **Save**.
   The new event attribute appears in the list.
5. Select the event attribute(s) from the list and click **Apply**.

You can clone an existing event attribute type to use as the basis for a new one. Select the event attribute type you want to use, click **Clone** and modify as necessary.

Modifying an Event Attribute

Complete these steps to modify an event attribute setting:

1. Select one or more event attribute(s) to edit from the list.
2. Click the required option:
   - **Edit** to modify the settings of an event attribute(s).
   - **Delete** to remove an event attribute(s).
3. Click **Save**.

Working with Event Types

After parsing an event or log, FortiSIEM assigns a unique event type to that event/log. When you create a new custom parser for device logs, you have to add a new event type to FortiSIEM so the log events can be identified.

This section provides the procedure to create event types.

- Adding an Event Type
- Modifying an Event Type

Adding an Event Type

Complete these steps to add an event:

1. Go to **ADMIN** > **Device Support**> **Event Types** tab.
2. Click **New**.
3. In the **Event Definition** dialog box, enter the information below.

Settings	Guidelines
Name	[Required] If the event will be used for Custom Monitoring, the Event Type name must begin with `PH_DEV_MON_CUST_`. See here for more details on Custom Monitoring.
Device Type	[Required] Select a device from the drop-down list.
Event Type Group	[Required] Select the type of group for the event.
Severity	[Required] Severity (0 - lowest) to 10 (highest).
Description	Description of the event type.

4. Click **Save**.
   The new event appears in the table.
5. Select the event(s) from the list and click **Apply**.

You can also use the **Clone** option to duplicate and modify an existing event type.

Modifying an Event Type

Complete these steps to modify an event type:

1. Select one or more event attribute(s) to edit from the list.
2. Click the required option from the following table.
   - **Edit** - To modify the settings of a selected event(s).
   - **Delete** - To delete an event type.
3. Click **Save**.

Working with Parsers

Creating a custom parser for device logs involves writing an XML specification for the parser and using a test event to make sure the logs are parsed correctly.

Prerequisites

You should have:

- examples of the logs that you want to parse.
- created any new device/application types, event attribute types, or event types that you want to use in your XML specification.
- already written the XML specification for your parser.
- prepared a test event that you can use to validate the parser.

Parsers are applied in the order they are listed in **ADMIN** > **Device Support** > **Parsers**, so it is important to add your custom parser to the list in relation to any other parsers that may be applied to your device logs. If you click **Fix Order**, this will arrange the parsers with system-defined parsers at the top of the list in their original order, and user-defined parsers at the bottom. Be sure to click **Apply** to ensure the change in order is picked up by the back-end module.

After making a parser change, you must click **Apply** for the parser modules on all nodes to pick up the change. This is by design. If this does not occur, then SSH to the node where you expect the event to arrive first, and restart the phParser module.

The following sections provide information about working with parsers:

- Event Parser XML Specification
- Creating a Custom Parser
- Deleting or Disabling a Parser
- Ingesting JSON Formatted Events Received via HTTP(S) POST
- Parser Inbuilt Functions
- Parser Examples

Event Parser Specification

- Custom Parser XML Specification Template
- Parser File
- Device or Application Type Specification
- Event Format Recognizer Specification

- Pattern Definition Specification
- Parsing Instructions Specification

Custom Parser XML Specification Template

The basic template for a custom parser XML specification includes five sections. Click the name of any section for more information.

Section	Description
Parser File	Adding, editing, or cloning a parser file.
Device or Application Type Specification	The type of device or application associated with the parser.
Event Format Recognizer Specification	Patterns that determine whether an event will be parsed by this parser.
Pattern Definition Specification	Defines the parsing patterns that are iterated over by the parsing instructions.
Parsing Instructions Specification	Instructions on how to parse events that match the format recognizer patterns.

Custom Parser XML Specification Template

```
<patternDefinitions> </patternDefinitions>
<eventFormatRecognizer> </eventFormatRecognizer>
<parsingInstructions> </parsingInstructions>
```

Parser File

This section provides steps to create, edit, or clone a parser file.

- Create a Parser File
- Edit a Parser File
- Clone a Parser File

Create a Parser File

To create a parser, take the following steps:

1. Navigate to **ADMIN > Device Support > Parsers**.
2. Click **New**.
3. From the **Add Event Parser Definition** window, take the following steps:
   a. In the **Name** field, enter the name of the parser.
   b. In the **Device Type** drop-down list, select the appropriate device.

c. In the main field, provide your parser XML.

d. The following options are also available:

Parser XML Button	Description
Validate	Click to check your XML code syntax.
Test	Click to test your XML code.
Reformat	Click to format your XML code.
Enable	Click the Enable checkbox to enable the parser/XML code.
Clear XML	Click to remove the existing XML code.
Previous	Click to go to the prior XML code page.
Next	Click to go to the next XML code page.

e. When done, click **Save**.

Edit a Parser File

You are only allowed to edit a custom parser file. To edit an existing custom parser, take the following steps:

1. From **ADMIN > Device Support > Parsers**, select a custom parser.
2. Click **Edit**.
3. From the **Edit Event Parser Definition** window, you can make changes to the following fields:
   a. In the **Name** field, make any changes to the name of the parser.
   b. In the **Device Type** drop-down list, make any changes to the device type.
   c. In the main field, make any changes to your parser XML.
   See the table in Create a Parser for available options.
4. When done, click **Save**.

Clone a Parser File

To clone an existing parser, take the following steps:

1. From **ADMIN > Device Support > Parsers**, select a parser.
2. Click **Clone**.
3. From the **Add Event Parser Definition** window, you can make changes to the following fields:
   a. In the **Name** field, make any changes to the name of the parser.
   b. In the **Device Type** drop-down list, make any changes to the device type.
   c. In the main field, make any changes to your parser XML.
   See the table in Create a Parser for available options.
4. When done, click **Save**.

Device or Application Type Specification

This section specifies the device or the application to which this parser applies. The device and application definitions enable FortiSIEM to detect the device and application type for a host from the received events. This is called **log-**

based discovery in FortiSIEM. Once a received event is successfully parsed by this file, a CMDB entry is created with the device and application set from this file. FortiSIEM discovery may further refine the device.

There are two separate subsections for device and application. In each section, vendor, model and version can be specified, but version is not typically needed.

Set Version to Any

In the examples in this topic, `<Version>` is set to `ANY` because events are generally not tied to a particular version of a device or software. You could of course set this to a specific version number if you only wanted this parser to apply to a specific version of an application or device.

Vendor and Model Must Match the FortiSIEM Version

`<Vendor>` and `<Model>` entries must match the spelling and capitalization in the CMDB.

Examples of Specifications for Types of Device and Applications

Hardware Appliances

In this case, the type of event being parsed specifies the device type, for example Cisco IOS, Cisco ASA, etc.

To add a device type, see Adding a Device or Application.

Software Operating Systems that Specify the Device Type

In this case, the type of events being parsed specifies the device type, for example Microsoft Windows etc. In this case the device type section looks like:

```
<deviceType>
  <Vendor>Microsoft</Vendor>
  <Model>Windows</Model>
  <Version>ANY</Version>
</deviceType>
```

Applications that Specify Both Device Type and Application

In this case, the events being parsed specify the device and application types because Microsoft SQL Server can only run on Microsoft Windows OS.

```
<deviceType>
  <Vendor>Microsoft</Vendor>
  <Model>Windows</Model>
  <Version>ANY</Version>
</deviceType>
<appType>
  <Vendor>Microsoft</Vendor>
  <Model>SQL Server</Model>
  <Version>ANY</Version>
  <Name> Microsoft SQL Server</Name>
</appType>
```

Applications that Specify the Application Type but Not the Device Type

Consider the example of an Oracle database server, which can run on both Windows and Linux operating systems. In this case, the device type is set to **Generic** but the application is specific. FortiSIEM depends on discovery to identify the device type.

```
<deviceType>
  <Vendor>Generic</Vendor>
  <Model>Generic</Model>
  <Version>ANY</Version>
</deviceType>
<appType>
  <Vendor>Oracle</Vendor>
  <Model>Database Server</Model>
  <Version>ANY</Version>
  <Name>Oracle Database Server</Name>
</appType>
```

Format Recognizer Specification

In many cases, events associated with a device or application will contain a unique pattern. You can enter a regular expression in the Format Recognizer section of the parser XML file to search for this pattern, which if found, will then parse the events according to the parser instructions. After the first match, the event source IP to parser file map is cached, and only that parser file is used for all events from that source IP. A notable exception is when events from disparate sources are received via a syslog server, but that case is handled differently.

While not a required part of the parser specification, a format recognizer can speed up event parsing, especially when one parsing pattern file among many pattern files must be chosen. Only one pattern check can determine whether the parsing file must be used or not. The other less efficient option would be to examine patterns in every file. At the same time, the format recognizer must be carefully chosen so that it is not so broad to misclassify events into wrong files, and at the same time, not so narrow that it fails at classifying the right file.

Order in Which Parsers are Used

FortiSIEM parser processes the files in the specific order listed in the file `parserOrder.csv`.

Format Recognizer Syntax

The specification for the format recognizer section is:

```
<eventFormatRecognizer><!\[CDATA\[regexpattern\]\]></eventFormatRecognizer>
```

In the `regexpattern` block, a pattern can be directly specified using regex or a previously defined pattern (in the pattern definition section in this file or in the `GeneralPatternDefinitions.xml` file) can be referenced.

Example Format Recognizers

Cisco IOS

All Cisco IOS events have a `%module name` pattern.

```
<patternDefinitions>
  <pattern name="patCiscoIOSMod" list="begin"><!\[CDATA\[FW|SEC|SEC_
LOGIN|SYS|SNMP|\]\]></pattern>
  <pattern name="patCiscoIOSMod" list="continue"><!\[CDATA\
[LINK|SPANTREE|LINEPROTO|DTP|PARSER|\]\]></pattern>
  <pattern name="patCiscoIOSMod" list="end"><!\[CDATA\[CDP|DHCPD|CONTROLLER|PORT_
SECURITY-SP\]\]></pattern>
</patternDefinitions>
<eventFormatRecognizer><!\[CDATA\[:%<:patCiscoIOSMod>-<:gPatInt>-<:patStrEndCo-
lon>:\]\]></eventFormatRecogniz
er>
```

Cisco ASA

All Cisco ASA events have the pattern `ASA-severity-id` pattern, for example `ASA-5-12345`.

```
<eventFormatRecognizer><!\[CDATA\[ASA-\\d-\\d+\]\]></eventFormatRecognizer>
```

Palo Alto Networks Log Parser

In this case, there is no unique keyword, so the entire message structure from the beginning to a specific point in the log must be considered.

Event

```
<14>May 6 15:51:04 1,2010/05/06 15:51:04,0006C101167,TRAFFIC,start,1,2010/05/06
15:50:58,192.168.28.21,172.16.255.78,::172.16.255.78,172.16.255.78,rule3,,,icm-
p,vsys1,untrust,untrust,ethernet1/1,ethernet1/1,syslog-172.16.20.152,2010/05/06
15:51:04,600,2,0,0,0,0,0x40,icmp,allow,196,196,196,2,2010/05/06 15:50:58,0,any,0
```

```
<eventFormatRecognizer><!\[CDATA\[<:gPatTime>,\\w+,
(?:TRAFFIC|THREAT|CONFIG|SYSTEM)\]\]></eventFormatRecognizer>
```

Pattern Definition Specification

In this section of the parser XML specification, you set the regular expression patterns that that FortiSIEM will iterate through to parse the device logs.

Reusing Pattern Definitions in Multiple Parser Specifications

If you want to use a pattern definition in multiple parser specifications, you must define it in the `GeneralPatternDefinitions.xml` file. The patterns in the file must have a `g` prefix, and can be referenced as shown in this example:

```
<generalPatternDefinitions>
<pattern name="gPatSyslogPRI"><!\[CDATA\[<\\d+>\]\]></pattern>
  <pattern name="gPatMesgBody"><!\[CDATA\[.*\]\]></pattern>
  <pattern name="gPatMonNum"><!\[CDATA\[\\d{1,2}\]\]></pattern>
```

```
    <pattern name="gPatDay"><!\[CDATA\[\\d{1,2}\]\]></pattern>
    <pattern name="gPatTime"><!\[CDATA\[\\d{1,2}:\\d{1,2}:\\d{1,2}\]\]></pattern>
    <pattern name="gPatYear"><!\[CDATA\[\\d{2,4}\]\]></pattern>
  </generalPatternDefinitions>
```

Each pattern has a name and the regular expression pattern within the CDATA section. This the basic syntax:

```
<pattern name="patternName"><!\[CDATA\[pattern\]\]></pattern>
```

This is an example of a pattern definition:

```
<patternDefinitions>
  <pattern name="patIpV4Dot"><!\[CDATA\[\\d{1,3}.\\d{1,3}.\\d{1,3}.\\d{1,3}\]\]></pat-
tern>
  <pattern name="patComm"><!\[CDATA\[\[^,\]+\]\]></pattern>
  <pattern name="patUpDown"><!\[CDATA\[up|down\]\]></pattern>
  <pattern name="patStrEndColon"><!\[CDATA\[\[^:\]*\]\]></pattern>
</patternDefinitions>
```

You can also write a long pattern definition in multiple lines and indicate their order as shown in this example. The value of the `list` attribute should be `begin` in first line and `end` in last line. If there are more than two lines, the attribute should be set to `continue` for the other lines.

```
<pattern name="patSolarisMod" list="begin"><!\[CDATA\[sshd|login|\]\]></pattern>
<pattern name="patSolarisMod" list="continue"><!\[CDATA\[inetd|lpstat|\]\]></pattern>
<pattern name="patSolarisMod" list="end"><!\[CDATA\[su|sudo\]\]></pattern>
```

Parsing Instructions Specification

This section is the heart of the parser, which attempts to recognize patterns in a log message and populate parsed event attributes.

In most cases, parsing involves applying a regular expression to the log, picking up values, and setting them to event attributes. Sometimes the processing is more involved, for example when attributes must be stored as local variables and compared before populating the event attributes. There are three key components that are used in parsing instructions: Event attributes and variables, inbuilt functions that perform operations on event attributes and variables, and `switch` and `choose` branching constructs for logical operations. Values can be collected from both unstructured and structured strings in log messages.

- Event Attributes and Variables
- Inbuilt Functions
- Branching Constructs
- Collecting Fields from Structured Strings
- Collecting Values from Unstructured Strings

Event Attributes and Variables

The dictionary of event attributes are defined in FortiSIEM database and any member not belonging to that list is considered a local variable. For readability, local variables should begin with an underscore (_), although this is not enforced.

Setting an Event Attribute to a Constant

```
<setEventAttribute attr="eventSeverity">1</setEventAttribute>
```

Setting an Event Attribute from Another Variable

The `$` symbol is used to specify the content of a variable. In the example below, attribute `hostMACAddr` gets the value stored in the local variable `_mac`.

```
<setEventAttribute attr="hostMACAddr">$_mac</setEventAttribute>
```

Inbuilt Functions

Combining Two or More Strings to Produce a Final String

Use the `combineMsgId` function to do this. Here `_evIdPrefix` is the prefix, `_evIdSuffix` is the suffix, and the output will be `string1-_evIdPrefix-_evIdSuffix`.

```
<setEventAttribute attr="eventType">combineMsgId("string1", $_evIdPrefix, "-", $_
evIdSuffix)</setEventAttribute>
```

Strings can only be wrapped by double quotes `"` but not single quotes `'`.

Normalize MAC Address

Use the `normalizeMAC` function to do this. The output will be six groups of two nibbles separated by a colon, for example `AA:BB:CC:DD:EE:FF`.

```
<setEventAttribute attr="hostMACAddr">normalizeMAC($_mac)</setEventAttribute>
```

Compare Interface Security Level

Use the `compIntfSecVal` function to do this. This primarily applies to Cisco ASA and PIX firewalls. The results returned are:

- `LESS` if `srcIntf` has strictly lower security level than `destIntf`
- `GREATER` if `srcIntf` has strictly higher security level than `destIntf`
- `EQUAL` if `srcIntf` and `destIntf` have identical security levels

```
<setEventAttribute attr="_result">compIntfSecVal($srcIntf, $destInt-
f)</setEventAttribute>
```

Convert Hex Number to Decimal Number

Use the `convertHexStrToInt` function to do this.

```
<setEventAttribute attr="ipConnId">convertHexStrToInt($_ipConnId)</setEventAttribute>
```

Convert TCP/UDP Protocol String to Port Number

Use the `convertStrToIntIpPort` function to do this.

```
<setEventAttribute attr="destIpPort">convertStrToIntIpPort($_dport)</-
setEventAttribute>
```

Convert Protocol String to Number

Use the `convertStrToIntIpProto` function to do this.

```
<setEventAttribute attr="ipProto">convertStrToIntIpProto($_proStr)</setEventAttribute>
```

Convert Decimal IP to String

Use the `converIpDecimalToStr` function to do this.

```
<setEventAttribute attr="srcIpAddr">convertIpDecimalToStr($_srcIpAd-
dr)</setEventAttribute>
```

Convert Host Name to IP

Use the `convertHostNameToIp` function to do this.

```
<setEventAttribute attr="srcIpAddr">convertHostNameToIp($_saddr)</setEventAttribute>
```

Add Two Numbers

Use the `add` function to do this.

```
<setEventAttribute attr="totBytes">add($sentBytes, $recvBytes)</setEventAttribute>
```

Divide Two Numbers

Use the `divide` function to do this.

```
<setEventAttribute attr="memUtil">divide($\_usedMem, $\_totalMem)</setEventAttribute>
```

Scale Function

Use the `scale` function to do this.

```
<setEventAttribute attr="durationMSec">scale($_durationSec, 1000)</setEventAttribute>
```

Calculate Micro Seconds

Use the `calculateMSec` function to do this.

```
<setEventAttribute attr="durationMSec">calculateMSec($_duration)</setEventAttribute>

_duration: 00:00:15
durationMSec: 15000
```

Extract Host from Fully Qualified Domain Name

Use the **extractHostFromFQDN** function to do this. If `_fqdn` contains a period `(.)`, get the string before the first period. If it does not contain a period, get the entire string.

```
<setEventAttribute attr="hostName">extractHostFromFQDN($_fqdn)</setEventAttribute>
```

Replace a String Using a Regular Expression

Use the `replaceStringByRegex` function to do this.

```
<setEventAttribute attr="computer">replaceStrInStr($_computer, "\\\", "")</-
setEventAttribute>
```

Replace String in String

Use the `replaceStrInStr` function to do this.

```
<setEventAttribute attr="computer">replaceStrInStr($_computer, "\\\", "")</-
setEventAttribute>
```

Resolve DNS Name

Use the `resolveDNSName` function to do this. This function converts the DNS name to an IP address.

```
<setEventAttribute attr="destIpAddr">resolveDNSName($destName)</setEventAttribute>
```

Shift Time Seconds

Use the `shiftTimeSec` function to do this.

```
<setEventAttribute attr="logonTime">shiftTimeSec($_mon, $_day, $_year, $_time, $_dur-
ationSec)</setEventAttribute>

_mon: 1
_day: 1
_year: 2000
_time: 01:00:10
_durationSec: 10
logonTime: 01:00:00 01/01/2000
```

Convert to UNIX Time

Use the `toDateTime` function to do this.

```
<setEventAttribute attr="deviceTime">toDateTime($_mon, $_day, $_year, $_time)</-
setEventAttribute><setEventAttribute attr="deviceTime">toDateTime($_mon, $_day, $_
time)</setEventAttribute>
```

Trim Attribute

Use the `trimAttribute` function to do this. In this example, it is used to trim the leading and trailing dots in `destName`.

```
<setEventAttribute attr="destName">trimAttribute($destName, ".")</setEventAttribute>
```

Get Severity from Syslog Priority

Use the `getEventSeverityFromSyslogPriority` function to do this.

Set severity by syslog priority. The bottom 3 bits of the priority indicates the severity. Refer to

https://en.wikipedia.org/wiki/Syslog#Severity_level

```
<setEventAttribute attr="eventSeverity">getEventSeverityFromSyslogPriority($_pri)</-
setEventAttribute>
_pri: 52
eventSeverity: 5
```

Convert to UNIX Time (with Timezone)

Use the `toUnixTime` function to do this.

```
<setEventAttribute attr="deviceTime">toUnixTime($_deviceTime)</setEventAttribute>
_deviceTime: 20130509073221.932817-000
```

Decode Base64

Use the `decodeBase64` function to do this.

```
<setEventAttribute attr="httpFullRequest">decodeBase64($_msg)</setEventAttribute>
```

Calculate Latency

Use the `calculateLatency` function to do this.

Calculate the latency. If `_evtRecvTime` is later than `deviceTime`, return the latency in seconds. Otherwise, return 0.

```
<setEventAttribute attr="_latency">calculateLatency($_evtRecvTime, $deviceTime)</-
setEventAttribute>
```

Decode URL

Use the `URLDecode` function to do this.

```
<setEventAttribute attr="infoURL">URLDecode($_url)</setEventAttribute>
```

Branching Constructs

- **Choose**
  The format is:

```
<choose>
  <when test="$AttributeOrVariable1 operator Value1">
    ...
  </when>
  <when test="$AttributeOrVariable2 operator Value2">
    ...
  </when>
  <otherwise>
    ...
  </otherwise>
</choose>
```

- **Switch**
  The format is:

```
<switch>
  <case>
    ...
  </case>
  <case>
    ...
  </case>
</switch>
```

Collecting Values from using prebuilt functions for Structured and Unstructured Logs

Summary: Functions used to simplify data extraction from certain sections of a log event. The usual first step is to separate the log header from the log message body. Identify the event type (usually by message ID if possible), and parse specific attributes based on event type.

Collecting Fields from Structured Strings

Summary: Logs that contain a structured mapping / format such as the below.

There are usually two types of structured strings in device logs:

- Key=value structured
- Value list structured

Common parse methods:

collectAndSetAttrByByJSON

collectAndSetAttrByByKeyValuePair

Collecting Fields from Unstructured Strings

Summary: Logs that contain variable / non consistent formatting of data structure depending on log type. Use a combination of regex parsing, <switch><case></case></switch> or <choose><when></when></choose> statements to break down and parse logs based on a particular format.

Example vendors with unstructured logs: Cisco ASA / Firepower

Common parse methods:

collectAndSetAttrByRegex - Evaluates and maps match groups to variables based on regex inserted given an argument containing a string log message.

Function List:

- collectAndSetAttrByJSON
- collectAndSetAttrByJsonArray
- collectAndSetAttrByJsonSymbol
- collectAndSetAttrByKeyValuePair
- collectAndSetAttrByKeyValuePairMultiValue
- collectAndSetAttrByPos
- collectAndSetAttrByPosWithNestedSep
- collectAndSetAttrByPosWithQuotes
- collectAndSetAttrByRegex
- collectAndSetAttrBySymbol
- collectAndSetAttrByXPath
- collectAndSetAttrFromAnotherEvent
- collectFieldsByCsvFile
- collectFieldsByKeyValuePair
- collectFieldsByRegex
- collectFieldsBySNMPTrap

collectAndSetAttrByJSON

Summary: Used to extract key value pairs from a json variable, in our example $_body is the variable containing a json object.

Note one example to access sub elements where a json key value contains a json array of objects.

```
<collectAndSetAttrByJSON src="$_body">
  <attrKeyMap attr="domain" key="domain"/>
  <attrKeyMap attr="_eventTime" key="ts"/>
  <attrKeyMap attr="ipConnId" key="uid"/>
  <attrKeyMap attr="hostIpAddr" key="assigned_ip"/>
  <attrKeyMap attr="durationMSec" key="lease_time"/>
  <attrKeyMap attr="seqNum" key="trans_id"/>
  <!-- access json key network_addresses that contains a json array, access first element's ip key, return value -->
  <attrKeyMap attr="hostIpAddr" key="network_addresses[0].ip"/>
</collectAndSetAttrByJSON>
```

collectAndSetAttrByJsonArray

Summary: Another method to gather data from JSON Arrays, iterate through an array of objects. If an object key matches one type, gather the value of another key.

Example: You have a json array where the key Type can be one of 3 values. Only map attribute x if Type=`someValue`

Sample event parsable by this function:

```
"Resources":[{"Type":"AwsAc-
count","Id":"AWS::::Account:600000000000","Partition":"aws","Region":"us-west-
2"}],"Compliance":{"Status":"WARNING"},"WorkflowState":"NEW","RecordState":"ACTIVE"}]]

<collectAndSetAttrByJsonArray src="$_resource" sep=" ">
  <attrKeyMap attr="ec2InstanceId" key="entries.find(Type='AwsEc2Instance', Id)"/>
  <attrKeyMap attr="_ec2IP" key="entries.find(Type='AwsEc2Instance', Details.AwsEc2In-
stance.IpV4Addresses[0])"/>
  <attrKeyMap attr="user" key="entries.find(Type='AwsIamAccessKey', Details.AwsIamAc-
cessKey.UserName)"/>
</collectAndSetAttrByJsonArray>
```

collectAndSetAttrByJsonSymbol

Summary: Seen only in GenericJSONParser so far, I believe the purpose of this was to auto map the keys of a json object into temp variables.

```
<collectAndSetAttrByJsonSymbol src="$_rawmsg">
  <!-- Auto maps to key into a tmp var? -->
</collectAndSetAttrByJsonSymbol>
```

collectAndSetAttrByKeyValuePair

Certain logs, such as SNMP traps, are structured as `Key1 = value1 <separator> Key2 = value2`,.... These can be parsed using the `collectAndSetAttrByKeyValuePair` XML attribute tag with this syntax.

```
<collectAndSetAttrByKeyValuePair sep="separatorString"src="$inputString">
  <attrKeyMap attr="variableOrEventAttribute1" key="key1"/>
  <attrKeyMap attr="variableOrEventAttribute2" key="key2"/>
</collectAndSetAttrByKeyValuePair>
```

When a `key1` match is found, the entire string following `key1` up to the `separatorString` is parsed out and stored in the attribute `variableOrEventAttribute1`.

For example, consider this log fragment:

```
\_body =
SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.60 = Hex-STRING: 07 D8 06 0B 13 15 00 00 2D
07 00   SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.11.0 = Hex-STRING: 00 16 B6 DB 12 22
SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.12.0 = Hex-STRING: 00 21 55 4D 66 B0
SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.13.0 = INTEGER: 36   SNMPv2-SMI::en-
terprises.14823.2.3.1.11.1.1.1.0 = Hex-STRING: 00 1A 1E C0 60 7A        SNMPv2-SMI::en-
terprises.14823.2.3.1.11.1.1.56.0 = INTEGER: 2  SNMPv2-SMI::en-
terprises.14823.2.3.1.11.1.1.17.0 = STRING: "00:1a:1e:c0:60:7a"
```

The corresponding parser fragment is:

```
<collectAndSetAttrByKeyValuePair sep="\\t\\\| SNMP" src="$_body">
  <attrKeyMap attr="srcMACAddr" key="SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.11.0 =
Hex-STRING: "/>
  <attrKeyMap attr="_destMACAddr" key="SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.12.0
= Hex-STRING: "/>
  <attrKeyMap attr="wlanSSID" key="SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.6.0 =
STRING: "/>
  <attrKeyMap attr="wlanRadioId" key="SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.56.0
= INTEGER: "/>
  <attrKeyMap attr="apMac" key="SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.17.0 =
STRING: "/>
</collectAndSetAttrByKeyValuePair>
```

After parsing, the attribute values are set:

Value	Attribute
00 16 B6 DB 12 22	`srcMACAddr`
00 21 55 4D 66 B0	`destMacAddr`
2	`wlanRadioId`
00:1a:1e:c0:60:7a	`apMac`

collectAndSetAttrByKeyValuePairMultiValue

Summary: Seen only in CiscoACSParserPlus.xml so far, designed when a key is repeated multiple times, each with distinct values. Notice Step= is repeated many times.

Each value should be concatenated into a parsable var. --untested

```
 <181>May 16 08:18:13 dotacs12 CSCOacs_Passed_Authentications 0001575987 3 0 2012-05-
16 08:18:13.572 -05:00 0025628800 5201 NOTICE Passed-Authentication: Authentication
succeeded, ACSVersion=acs-5.3.0.40-B.839, ConfigVersionId=21, Device IP Address-
s=10.15.1.248, UserName=abc, Protocol=Tacacs, RequestLatency=13, Net-
workDeviceName=Default Network Device, Type=Authentication, Action=Login, Privilege-
Level=1, Authen-Type=ASCII, Service=Login, User=joeUser, Port=tty1, Remote-Address-
s=10.16.13.251, UserName=joeUser, AcsSessionID=dotacs12/126121712/1427032, Authentic-
ationIdentityStore=Internal Users, AuthenticationMethod=PAP_ASCII,
SelectedAccessService=TACACS Administration, SelectedShellProfile=NetworkAdmins, Iden-
tityGroup=IdentityGroup:All Groups:Network Administrators, Step=13020 , Step=13013 ,
Step=15008 , Step=15004 , Step=15012 , Step=15041 , Step=15004 , Step=15013 , Step-
p=24210 , Step=24212 , Step=13045 , Step=13015 , Step=13020 , Step=13014 , Step=15037
, Step=15041 , Step=15004 , Step=15013 ,
```

Example:

```
<collectAndSetAttrByKeyValuePairMultiValue src="$_body" sep=",">
  <attrKeyMap attr="_step" key="Step="/>
  <attrKeyMap attr="_deviceadmin" key="Device-Administration: "/>
</collectAndSetAttrByKeyValuePairMultiValue>
```

collectAndSetAttrByPos

<a id="Value"></a>Value List Structured Data

Certain application logs, such as those from Microsoft IIS, are structured as a list of values with a separator. These can be parsed using the `collectAndSetAttrByPos` XML attribute tag following this syntax.

```
<collectAndSetAttrByPos sep="separatorString" src="$inputString">
  <attrPosMap attr="variableOrEventAttribute1" pos="offset1"/>
  <attrPosMap attr="variableOrEventAttribute2" pos="offset2"/>
</collectAndSetAttrByPos>
```

When the position `offset1` is encountered, the subsequent values up to the `separatorString` is stored in `variableOrEventAttribute1`.

For example, consider this log fragment:

```
\_body =
W3SVC1 ADS-PRI 192.168.0.10 GET /Document/ACE/index.htm - 80 -
192.168.20.55 HTTP/1.1
Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-US;+rv:1.8.1.11)+Gecko/20071
127+Firefox/2.0.0.11 \[http://wwwin/Document/\] wwwin 200 0 0 5750 445 15
```

The parser fragment is:

```
<collectAndSetAttrByPos src="$_body" sep="  ">
  <attrPosMap attr="srvInstName" pos="1"/>
  <attrPosMap attr="destName" pos="2"/>
  <attrPosMap attr="relayDevIpAddr" pos="2">
  <attrPosMap attr="destIpAddr" pos="3"/>
  <attrPosMap attr="httpMethod" pos="4"/>
  <attrPosMap attr="uriStem" pos="5"/>
  <attrPosMap attr="uriQuery" pos="6"/>
  <attrPosMap attr="destIpPort" pos="7"/>
  <attrPosMap attr="user" pos="8"/>
  <attrPosMap attr="srcIpAddr" pos="9"/>
  <attrPosMap attr="httpVersion" pos="10"/>
```

```
    <attrPosMap attr="httpUserAgent" pos="11"/>
    <attrPosMap attr="httpReferrer" pos="13"/>
    <attrPosMap attr="httpStatusCode" pos="15"/>
    <attrPosMap attr="httpSubStatusCode" pos="16"/>
    <attrPosMap attr="httpWin32Status" pos="17"/>
    <attrPosMap attr="recvBytes" pos="18"/>
    <attrPosMap attr="sentBytes" pos="19"/>
    <attrPosMap attr="durationMSec" pos="20"/>
   </collectAndSetAttrByPos>
```

For structured strings, techniques in this section are more efficient than in the previous section because the expression is simpler and ONE tag can be used to parse regardless of the order in which the keys or values appear in the string.

collectAndSetAttrByPosWithNestedSep

Summary: Some events will be position separated, and have position separators, or nested separators. In logs that have space separators, but the values themselves contain spaces, they use nested delimiters to treat the value of each position as a literal.

Example Log:

```
<166>Sep 25 17:39:43 hog (squid-1): 192.168.0.171 33763 example.net 192.168.0.86 3128
204 - - - - [25/Sep/2015:17:39:43 +0100] GET "http://example.net/ping?" HTTP/1.1 200
356 921 "http://example.com/news/england" "Mozilla/5.0 (X11; Linux x86_64) AppleWe-
bKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.157 Safari/537.36" TCP_MISS:HIER_
DIRECT
```

In the above log, values are space separated, but use quotes to signify the start and end of the value of that position. User Agent is position 9, contains several spaces, which is okay since they are in the nested separator values "user agent data". L2Sep also takes a comma separated list of multiple separator types.

Position 1 (Device Time), uses the option for [] for inner separator

Position 9 (User Agent), uses the option for "" for inner separator

```
<collectAndSetAttrByPosWithNestedSep src="$_body" L1Sep=" " L2Sep="&quot;&quot;, []">
  <attrPosMap attr="_devTime" pos="1"/>
  <attrPosMap attr="httpMethod" pos="2"/>
  <attrPosMap attr="uriStem" pos="3"/>
  <attrPosMap attr="httpVersion" pos="4"/>
  <attrPosMap attr="httpStatusCode" pos="5"/>
  <attrPosMap attr="recvBytes64" pos="6"/>
  <attrPosMap attr="sentBytes64" pos="7"/>
  <attrPosMap attr="httpReferrer" pos="8"/>
  <attrPosMap attr="httpUserAgent" pos="9"/>
</collectAndSetAttrByPosWithNestedSep>
```

collectAndSetAttrByPosWithQuotes

Summary: Used to specify an inner separator in addition to outer separator by position. The difference between this and collectAndSetAttrByPosWithNestedSep is that Nested Separator can supply a list of inner separators.

`collectAndSetAttrByPosWithNestedSep src="$_body" L1Sep=" " L2Sep="&quot;&quot;,[]"` - This allows key="value" or key=[value].

`collectAndSetAttrByPosWithQuotes` - This can only provide a single argument for the inner separator.

Seen in JuniperSteelBeltAAAParser.xml and a few others.

Example log: CSV separated, with quotes for nested separator

```
<45>Jul  9 03:20:30 example.com SteelBeltedLog      0       "2008-07-09","03:20:26","SJ-QA-A-CAT-COR","AbcHacker","NT Domain User","User name or credential incorrect","","172.16.10.1"
```

```
<collectAndSetAttrByPosWithQuotes src="$_body" sep="," quo="&quot;">
  <attrPosMap attr="_nasNameOrIp" pos="3"/>
  <attrPosMap attr="_user1OrPort" pos="4"/>
  <attrPosMap attr="_user2" pos="5"/>
  <attrPosMap attr="_reasonOrNasIp" pos="6"/>
  <attrPosMap attr="_reasonOrOwnIp" pos="7"/>
  <attrPosMap attr="_someIp" pos="8"/>
</collectAndSetAttrByPosWithQuotes>
```

collectAndSetAttrByRegex

From a string input source, a regex match is applied and variables are set. The variables can be event attributes or local variables. The input will be a local variable or the default raw message variable. The syntax is:

```
<collectAndSetAttrByRegex src="$inputString">
  <regex><!\[CDATA\[regexpattern\]\]></regex>
</collectAndSetAttrByRegex>
```

The `regexpattern` is specified by a list of variables and sub-patterns embedded within a larger pattern. Each variable and sub-pattern pair are enclosed within angle brackets (<>).

Consider an example in which the local variable `_body` is set to `list 130 permitted eigrp 172.16.34.4 (Serial1 ) > 172.16.34.3, 1 packet`. From this string we must set the values to local variables and event attributes.

Value	Set To	Type
130	`_aclName`	Local Variable
permitted	`_action`	Local Variable
eigrp	`_proto`	Local Variable

Value	Set To	Type
172.16.34.4	`srcIpAddr`	Event Attribute
Serial1	`srcIntfName`	Event Attribute
172.16.34.3	`destIpAddr`	Event Attribute
1	`totPkts`	Event Attribute

This is achieved by using this XML. Note that you can use both the `collectAndSetAttrByRegex` and `collectFieldsByRegex` functions to collect values from fields.

```
<collectAndSetAttrByRegex src="$_body">
  <regex><!\[CDATA\[list <\_aclName:gPatStr> <\_action:gPatWord> <_proto:gPatWord>
<srcIpAddr:gPatIpV4Dot>(<:srcIntfName:gPatWord>) -> <destIpAddr:gPatIpV4Dot>, <totPkt-
s:gPatInt> <:gPatMesgBody>\]\]></regex>
</collectAndSetAttrByRegex>
```

collectAndSetAttrBySymbol

Summary: Automatically maps The key between symStart and symEnd as a variable that contains the value. Primarily used with log formats built by phAgentManager pollers, which have key values

that match valid programmatic names of event attributes in FortiSIEM, e.g. sentBytes64 which is the correct FortiSIEM event attribute for Sent Bytes uint64.

Sample Event:

```
Tue Sep 19 18:00:06 2017 AWS_VPC_FLOW_ACCEPT [accountName]=abc@cda.com,[awsRegion]=us-
east-2,[groupName]=logGroupName,[streamName]=eni-1780864b-all,[version]=2,[accoun-
tId]=658308615768,[srcIntfName]=eni-1780864b,[srcIpPort]=22,[destIpPort]=16931,[ipPro-
to]=6,[sentPkts64]=13,[sentBytes64]=3171,[sentPktsReverse]=14,[sentBytesReverse]=1268,
[startTime]=1505808418,[endTime]=1505808460,[status]=OK,[srcAction]=ACCEPT,[destAc-
tion]=ACCEPT,[srcIpAddr]=10.0.0.244,[destIpAddr]=10.112.150.78
```

Example: Map [attribName]=Value to variable attribName for each, separated by ',['

```
<collectAndSetAttrBySymbol src="$_body" sep=",[" symStart="[" symEnd="]=">
  <excludeAttr>phLogDetail</excludeAttr>
</collectAndSetAttrBySymbol>
```

Resulting variables:

ipProto == 6

awsRegion == us-east-2

collectAndSetAttrByXPath

Summary: Uses XML XPath notation to place the value of a given XML tag into a variable.

Sample Event:

```
<13>Nov 09 00:55:09 172.30.58.88 <!-- PHBOX RULE ENGINE --><event name-
="phRuleI-
ncid-
ent"><deviceTime>1409271060</deviceTime><firstSeenTime>1409271060</firstSeenTime><-
coun-
t>1</count><durationMSec>900000</durationMSec><ruleId>1491921</ruleId><ruleName>Server
Hardware Critical</ruleName><ruleDescription>Detects a critical server hardware aler-
t.</ruleDescription><eventType>PH_RULE_SERVER_HW_CRITICAL</eventType><eventSever-
ity>9</eventSever-
ity><eventSever-
ityCat>HIGH</eventSever-
ityCat><phEventCat-
egory>1</phEventCat-
egory><phCustId>1</phCustId><incidentSrc></incidentSrc><incidentTarget>hostName:Host-
172.16.22.120, hostIpAddr:172.16.22.120,
</incidentTarget><hostIpAddr>172.16.22.120</hostIpAddr><hostName>Host-
172.16.22.120</hostName><hwComponentName>RAID 0 vol2 Logical Volume 1 on controller 0-
Drives(1e32-?)  - OFFLINE</h-
wCom-
ponentName><hwComponentStatus></hwComponentStatus><incidentDetail>hwComponentName:RAID
0 vol2 Logical Volume 1 on controller 0- Drives(1e32-?)  - OFFLINE, hwCom-
ponentStatus:, </in-
cidentDe-
tail><incidentRptIp>172.16.22.120</incidentRptIp><triggerEventLists><triggerEvents
sub-
patName-
="HwI-
ssueCrit">8264949741156592346</trig-
gerEvents></triggerEventLists><incidentId>14</incidentId></event>
```

Example: place nested xml value of the event tag into the $_body variable.

```
<collectAndSetAttrByXPath src="$_body" xpath="/event/*"/>
```

Documentation: XML path expressions

https://www.w3schools.com/xml/xml_xpath.asp

collectAndSetAttrFromAnotherEvent

Summary: Allows for mapping of correlated events given some variable in each event matches. Example, if two authentication events occur in a chain, and contain a logonID, you can have the SIEM search for the prior event, and retrieve a given attribute from that event to copy into the one you are parsing. This is used for advanced intelligence where a later log event does not contain a needed attribute. Assuming the events have an attribute linking them, e.g. the same user causing the generated audit events.

Sample Log:

```
<13>Dec 12 10:09:00 ADS-Pri.example.com MSWinEventLog    1       Security        1756
  Wed Dec 12 10:08:53 2007        517     Security        SYSTEM  User    Success
Audit   ADS-PRI The audit log was cleared              Client User Name: joeUser
Client Domain: ABC          Client Logon ID: (0x0, 0x158E87)
```

Example: Seen in Windows Event 517 - Audit log cleared. Copy the source IP from Windows event 540 or 528 if the logonIDs match, as event 517 itself does not contain a source IP attribute.

```
<collectAndSetAttrFromAnotherEvent AnotherEventType="Win-Security-540 OR Win-Security-
528">
  <when test="$winLogonId = $AnotherEventType.winLogonId">
    <setEventAttribute attr-
r="srcIpAddr">$AnotherEventType.srcIpAddr</setEventAttribute>
  </when>
</collectAndSetAttrFromAnotherEvent>
```

collectFieldsByCsvFile

Summary: Allows for a search of a key,value CSV file that replaces the target variable with the value of the key in the CSV file. You can specify which column you want to map.

Example CSV for Windows Logon Failure Codes: /opt/phoenix/data-definition/eventAttrDesc/winLogonFailCode2.csv

0XC000005E,Login failed - There are currently no logon servers available to service the logon request.

0XC0000064,Login failed - User logon with misspelled or bad user account

0XC000006A,Login failed - User logon with misspelled or bad password

0XC000006D,Login failed - This is either due to a bad username or authentication information

0XC000006E,Login failed - Unknown user name or bad password.

Structure of CSV File:

col0,col1

Logon Code,Logon Code Description

Example: Take the upper case arg variable $subStatus, if it matches one of the CSV lines, map column 1 to variable description.

```
<when test="exist subStatus">
  <setEventAttribute attr="_subStatus">toUpper($subStatus)</setEventAttribute>
  <collectFieldsByCsvFile file="/opt/phoenix/data-defin-
ition/eventAttrDesc/winLogonFailCode2.csv" key="$_subStatus" reloadInterval="3600">
    <attrKeyMap attr="description" column="1"/>
  </collectFieldsByCsvFile>
</when>
```

collectFieldsByKeyValuePair

Summary: Near duplicate of collectAndSetAttrByKeyValuePair, allows for kvsep so you don't have to include the key value separator in the key mapping.

Sample Event:

```
<134>Jul 24 2008 03:29:15: %ASA-6-113005: AAA user authentication Rejected : reason =
AAA failure : server = 192.168.0.40 : user = joeUser
```

Example: Map body values separated by ' : ' and key value separator of ' = '

```
<collectAndSetAttrByRegex src="$_body">
  <regex><![CDATA[AAA user authentication Rejected :\s*<_detail:gPatMes-
gBody>]]></regex>
</collectAndSetAttrByRegex>

<collectFieldsByKeyValuePair sep=" : " kvsep=" = " src="$_detail">
  <attrKeyMap attr="user" key="user"/>
  <attrKeyMap attr="srcIpAddr" key="user IP"/>
</collectFieldsByKeyValuePair>
```

collectFieldsByRegex

Summary: Seems to be an identical construct to: collectAndSetAttrByRegex

Example: Map each key value pair of <someVariable:someRegexMatchGroup> evaluating regex from left to right of the variable $_rawmsg

```
<collectFieldsByRegex src="$_rawmsg">
  <regex><![CDATA[^<_header:gPatMesgBodyMin>%<_vendor:gPatWord>-<_sev:gPatInt>-<_
evtId:gPatInt>:\s+<_body:gPatMesgBody>]]></regex>
</collectFieldsByRegex>
```

collectFieldsBySNMPTrap

Summary: Currently only seen in FireEyeTrapParser.xml, take an SNMP trap log message, map oid defined under key= to a given FortiSIEM event attribute.

Sample Log: Shortened for brevity

```
2016-05-26 07:50:28 0.0.0.0TRAP2, SNMP v2c, community R-OEnWinLog$            . Cold
Start Trap (0) Uptime: 0:00:00.00            DISMAN-EVENT-MIB::sysUpTimeInstance =
Timeticks: (610853754) 70 days, 16:48:57.54  SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-
SMI::enterprises.25597.3.0.1            SNMPv2-SMI::enterprises.25597.1.1.2.1.2.1116 =
Gauge32: 1116  SNMPv2-SMI::enterprises.25597.1.1.2.1.3.1116 = STRING: "malware-
```

```
callback"        SNMPv2-SMI::enterprises.25597.1.1.2.1.4.1116 = STRING: "2016-05-26"
SNMPv2-SMI::enterprises.25597.1.1.2.1.5.1116 = STRING: "11:46:48+00"  SNMPv2-SMI::en-
terprises.25597.1.1.2.1.6.1116 = Counter64: 0      SNMPv2-SMI::en-
terprises.25597.1.1.2.1.7.1116 = IpAddress: 10.1.201.82               SNMPv2-
SMI::enterprises.25597.1.1.2.1.8.1116 = IpAddress: 1.1.1.1             SNMPv2-SMI::en-
terprises.25597.1.1.2.1.9.1116 = STRING: "70:38:ee:91:cc:80"       SNMPv2-SMI::en-
terprises.25597.1.1.2.1.10.1116 = STRING: "58:49:3b:2d:98:11"    SNMPv2-
SMI::enterprises.25597.1.1.2.1.11.1116 = INTEGER: 80    SNMPv2-SMI::en-
terprises.25597.1.1.2.1.12.1116 = INTEGER: 0                SNMPv2-SMI::en-
terprises.25597.1.1.2.1.13.1116 = STRING: "tcp"
```

Example:

```
<collectFieldsBySNMPTrap src="$_body">
  <attrKeyMap attr="_id" key="SNMPv2-MIB::snmpTrapOID"/>
  <attrKeyMap attr="srcMACAddr" key="SNMPv2-SMI::enterprises.25597.1.1.2.1.9"/>
  <attrKeyMap attr="destMACAddr" key="SNMPv2-SMI::enterprises.25597.1.1.2.1.10"/>
  <attrKeyMap attr="destIpAddr" key="SNMPv2-SMI::enterprises.25597.1.1.2.1.38"/>
</collectFieldsBySNMPTrap>
```

Creating a Custom Parser

You should have:

- examples of the logs that you want to parse.
- created any new device/application types, event attribute types, or event types that you want to use in your XML specification.
- already written the XML specification for your parser.
- prepared a test event that you can use to validate the parser.

Parsers are applied in the order they are listed in **ADMIN > Device Support > Parsers**, so it is important to add your custom parser to the list in relation to any other parsers that may be applied to your device logs. If you click **Fix Order**, this will arrange the parsers with system-defined parsers at the top of the list in their original order, and user-defined parsers at the bottom. Be sure to click **Apply** to ensure the change in order is picked up by the back-end module.

Note: Custom parsers can be created only from the Super/Global account in Service Provider FortiSIEM deployments.

1. Go to **ADMIN** > **Device Support** > **Parsers**.
2. Select a parser that is above the location in the list where you want to add your parser, and click **New**.
3. Enter a **Name** for the parser.
4. Select a **Device Type** from the drop-down list to which the parser should apply.
   If the device type doesn't appear in the menu, you should create a new device type.
5. Enter a **Test** containing an example of an event that you want to use to validate the parser.
6. Enter the **Parser XML**.
7. Click **Validate**.
   This will validate the XML.

8. Click **Test**.
   This will send the test event to the parser to make sure it is parsed correctly, and will also test the parsers above and below yours in the list to make sure they continue to parse logs correctly.
9. If the XML for your parser validates and the test event is correctly parsed, select **Enable**.
   If you must continue working on your parser, you can **Save** it without selecting **Enable**.
10. Add a **Description** of the Parser.
11. Click **Save**.
12. Click **Apply** to have the back-end module pick up your parser and begin applying it to device logs.
    You should now validate that events are being parsed by creating some activity that will cause a log to be generated, and then run a query against the new device IP address and validate the parsed results.

Cloning New Parsers

You can clone an existing parser and then use it as the basis for creating a new one. Select the parser you want to clone, and then click **Clone**. Modify the parser as necessary, and then make sure you use the **Up** and **Down** buttons to place it in the list of parsers at the point at which is should be applied.

Ingesting JSON Formatted Events Received via HTTP(S) POST

FortiSIEM can receive, parse, and store JSON formatted events received via HTTP(S) POST. Follow these steps to implement this.

1. Configure the FortiSIEM node with the HTTPS credential for receiving the HTTP(S) POST event.
   a. Identity the FortiSIEM node receiving the events. Most likely, this will be the Collector.
   b. SSH to the Collector and run the command.
      `htpasswd -b /etc/httpd/accounts/passwds <user> '<password>'`
      Note: If the password contains special characters, it is advisable to encode the password in single quotes.
2. Make sure the events are being pushed to the FortiSIEM node using the credentials in Step 1 via this REST API:
   ```
   https://<
   FSMNodeName
   >/rawupload?vendor=<vendor>&model=<model>&reptIp=<reptIp>&reptName=<reptHost>
   ```
   where *FSNNodeName* is the resolvable host name or FQDN in Step 1. The parameters Reporting Vendor (*vendor*), Reporting Model (*model*), Reporting Device (*reptHost*), and Reporting IP (*reptIP*) are needed to create a CMDB entry and populate events.
   Note: If the Model contains whitespace, for example “Model 24”, you must correctly encode spaces and other special characters in the URL parameters.

Argument	Description
vendor	The vendor of the product that the logs originated from.
model	The model of the product that the logs originated from.
reptIp	This is the reporting IP, or the source of the log. The value you specify here will populate the CMDB as a reporting device.
reptName	This is the reporting device name, or the hostname of the device sending the logs.

HTTP Method: POST

HTTP Body: Log in json format

Sample Curl to Send a JSON File

This example is sending a SAP Enterprise Threat Detection log.

```
curl -kv -u ‘user:password’ -d "@json_event.json" -X POST
'https://<FSMNodeName>/rawup-
load?vendor-
=SAP-
&mod-
el=Enterprise%20Threat%20Detection&reptIp=192.168.1.20&reptName=LogForwarder1'
```

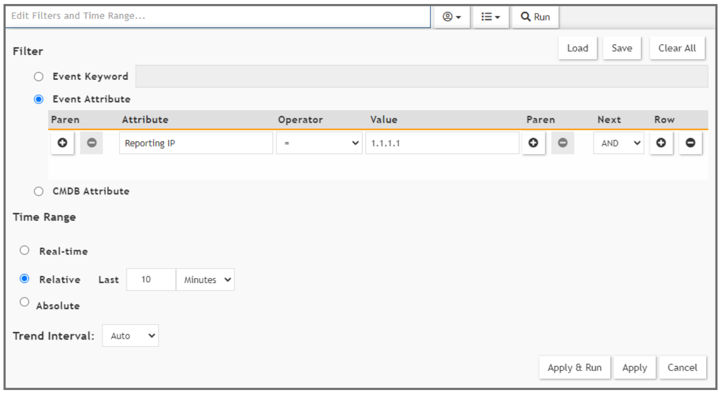
The above sends the JSON event stored in the file `json_event.json` to FortiSIEM. FortiSIEM then processes it, and the resulting event should look similar to the Log Format here, with an added header attached:

Log Format

```
[PH_DEV_MON_CUSTOM_JSON]:[reptVendor]=<vendor>,[reptModel]=<model>,
[reptDevName]=<reptName>,[reptDevIpAddr]=<reptIp>,[json]=<JSON>
```

Where <*JSON*> is the actual JSON log body posted to FortiSIEM.

3. Query the events by using the Reporting Device Name or IP in Step 2 and Event Type in Step 4c.
   a. Go to the **ANALYTICS** tab.
   b. Run a query for the Reporting IP = ‘`#.#.#.#`’ for the last 10 minutes.
   c. Observe the raw event, it should be in the format of.



Filter

● Event Attribute: Reporting IP = 1.1.1.1 AND

Time Range

● Relative Last 10 Minutes

Trend Interval: Auto

4. Create a new parser matching the header format with your provided vendor, model by taking the following steps.
   a. Login to the Supervisor.
   b. Navigate to **ADMIN > Device Support > Parsers**.
   c. Clone `PHCustomJSONParser.xml` and make the changes so that additional event attributes are parsed.
   d. Name your parser appropriately, e.g. *Vendor_Model_Custom_Parser*.
   e. Use a similar event format recoginizer: `<eventFormatRecognizer><![CDATA[\[PH_DEV_MON_CUSTOM_JSON]\:\[reptVendor\]=<vendor>,\[reptModel\]=<model>,]]></eventFormatRecognizer>`
   f. See parser training documentation on making a custom parser for your event.

g. **Validate**, **Test**, and **Save** the parser.
h. Click **Apply All** to deploy the parser changes.

5. If your JSON log events are batched into a single HTTPS POST operation (JSON contains many distinct events), there is a methodology to split the events using the following function `splitJsonEvent()`, and discard the original monolithic event. Observe the `SAPEnterpriseThreatDetectionParser` as an example usage of the function `splitJsonEvent()`.

Deleting or Disabling a Parser

- Deleting Parsers
- Disabling Parsers

Deleting Parsers

You can only delete user-defined parsers.

1. Go to **ADMIN** > **Device Support** > **Parsers**.
2. Select the parser you want to delete.
3. Click **Delete**.
4. Click **Yes** to confirm.

Disabling Parsers

You can disable both system and user-defined parsers.

1. Go to **ADMIN** > **Device Support** > **Parsers**.
2. Select the parser and deselect the tick mark below **Enabled** column.
3. Click **Yes** to confirm.

Parser Inbuilt Functions

The following parser inbuilt functions are available:

- Split JSON Event
- Combining Two or More Strings to Produce a Final String
- Normalize MAC Address
- Compare Interface Security Level
- Convert Hex Number to Decimal Number
- Convert TCP/UDP Protocol String to Port Number
- Convert Protocol String to Number
- Convert Decimal IP to String
- Convert Host Name to IP
- Add Two Numbers
- Divide Two Numbers
- Scale
- Calculate Micro Seconds

- Extract Host from FQDN
- Replace String by Regular Expression
- Replace String in String
- Resolve DNS Name
- Shift Time Sec
- To DateTime
- Trim Attribute
- Get Severity from Syslog Priority
- To Unix Time (with Time Zone)
- Decode Base64
- Unzip String
- Calculate Latency

Split JSON Event

This function allows you to take an array of JSON events, and create an individual log event for each object in the array.

Purpose

Some log events may arrive to FortiSIEM which are actually a list of multiple distinct log objects. This is typically the case with JSON API logs, where a single JSON response from some API contains a batch of log events held somewhere within the JSON structure.

How it Works

You build a parser that catches the monolithic event. You parse the portion of the event containing the array of individual events to a temporary variable.

You pass the JSON to the `splitJsonEvent` function.

- This function will generate an individual log event for each log object in the array of events.
- This function will prepend the optional defined log header string and optional trailing string to the message.
- If drop original event set to true, the SIEM will drop the monolithic event from being processed.

The net result is you will get multiple individual log events for the SIEM to parse vs just the monolithic event.

Note: You can either have the same parser handle both the monolithic event and individual events (Consistent log header for event format recognizer). Alternatively, you can write a parser for the monolithic event, and have a separate parser for the individual event (Easier to do but requires multiple parsers)

Example

Example: `<setEventAttribute attr="_resultCount">splitJsonEvent($_json, "alerts", "CustomHeader", "Optional Custom Trailer", "true")`

Arg1: Variable pointing to the JSON structure, e.g. `$_json` which contains the following: `"{"alerts":[{"event1"},{"event2"},{"event3"}]}"`

Arg2: JSON Array Key Path: The JSON path to the array of events.

- If the structure is exactly a JSON array, such as `[{"event1"},{"event2"},{"event3"}]`, you can leave this empty e.g. `""`
- If the array of individual events is nested under a given JSON key, you specify the key under which it exists. We specify "alerts" in the below example because the JSON array is nested.

Arg3: String header to prepend to the individual message. This must cleanly reference the log source so you can write a parser to parse this log.

Arg4: String trailer to append to the individual message. This is mostly unnecessary, but in some edge cases you may want this. In must cases specify `""` here.

Arg5: Drop Original Event bool flag. If true, the original monolithic event is dropped after splitting the events. If false, the original event is kept in FortiSIEM along with the individual split events.

For a Full Parser example, navigate to **ADMIN > Settings > Device Support > Parsers**, and search for "SAPEnterpriseThreatDetectionParser".

The SAP Parser reference is outlined below with comments.

Scenario

User is ingesting SAP Enterprise Threat logs into FortiSIEM using the HTTPS POST method of ingesting JSON formatted logs. See Ingesting JSON Formatted Events Received via HTTP(S) POST.

The ingested monolithic log looks like this:

```
[
   "PH_DEV_MON_CUSTOM_JSON"
]:[
   "reptVendor"
]"=SAP",
[
   "reptModel"
]"=ETD",
[
   "reptDevName"
]"=sap.edt.device",
[
   "reptDevIpAddr"
]=192.0.20.0
[
   "json"
]"="

{ "alerts": [ { "Version": "1.0", "AlertCreationTimestamp": "2021-09-
21T07:45:45.420Z", "AlertId": 812125, "AlertSeverity": "MEDIUM", "AlertStatus":
"FORWARDED", "AlertSource": { "EventLogType": "SystemLog", "SystemIdActor": "System25"
}, "AlertSystemIds": [ "System25" ], "HostNames": [ "lab1" ], "Category": "Log
```

Failure", "PatternId": "624F0A8BB948854F997942AC0EDB2102", "PatternType": "FLAB", "PatternName": "Low Log Amount per system", "PatternNameSpace": "http://demo", "PatternDescription": "", "MinTimestamp": "2021-09-21T07:44:39.522Z", "MaxTimestamp": "2021-09-21T07:44:39.522Z", "Text": "Measurement 48 exceeded threshold 50 for ('Event, Log Type' = 'SystemLog' / 'System ID, Actor' = 'System25')", "Score": 50, "UiLink": "http://192.0.20.0:80/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show?alert=62037185B38D5449999D57F465F1BBF6", "TriggeringEvents": [{ "Id": "C60C48EF7B4E4D848F45F1904820C2CC", "Timestamp": "2021-09-21T07:44:39.522Z", "TechnicalLogEntryType": "SM21_D01", "TechnicalNumber": "481537", "TechnicalTimestampOfInsertion": "2021-09-21T07:44:40.681Z", "CorrelationId": "120CD18982991EEA9AB8F87143C8DE88", "CorrelationSubId": "00000000000000000000000000000000", "EventCode": "D01", "EventSemantic": "Executable, Run, Cancel", "EventLogType": "SystemLog", "EventMessage": "LMDB_UPLOAD_ERRORS 011", "EventSeverityCode": "50", "EventSourceId": "198.51.100.0", "EventSourceType": "IP Address", "GenericRiskLevel": "3", "NetworkHostnameActor": "test-1", "NetworkHostnameInitiator": "0.0.0.0", "NetworkHostnameReporter": "test-1", "NetworkIPAddressInitiator": "0.0.0.0", "ServiceExecutableName": "00016", "ServiceExecutableType": "B", "ServiceInstanceName": "lab1_BLK_00", "ServiceProgramName": "RLMDB_UPLOAD_BACKGROUND", "ServiceTransactionName": "S000", "SystemIdActor": "System25", "SystemGroupIdActor": "BLN", "SystemGroupIdInitiator": "BLN", "SystemGroupIdIntermediary": "BLN", "SystemIdReporter": "System25", "SystemGroupIdReporter": "BLN", "SystemGroupIdTarget": "BLN", "SystemTypeActor": "ABBA", "SystemGroupTypeActor": "SAP", "SystemGroupTypeInitiator": "SAP", "SystemGroupTypeIntermediary": "SAP", "SystemTypeReporter": "ABBA", "SystemGroupTypeReporter": "SAP", "SystemGroupTypeTarget": "SAP", "UsernameDomainNameActing": "System25", "UsernameDomainTypeActing": "ABBA", "UserPseudonymActing": "BLK_BTC_SMP", "EventName": "ExecutableRunCancel", "EventNamespace": "http://sap.com/secmon", "TechnicalTimestampInteger": "1632210279522" }, { "Id": "765451B9772A4FA580059A7BAD7D149C", "Timestamp": "2021-09-21T07:44:39.522Z", "TechnicalLogEntryType": "SM21_E0A", "TechnicalNumber": "481536", "TechnicalTimestampOfInsertion": "2021-09-21T07:44:40.681Z", "CorrelationId": "120CD18982991EEA9AB8F87143C8DE88", "CorrelationSubId": "00000000000000000000000000000000", "EventCode": "E0A", "EventLogType": "SystemLog", "EventMessage": "&aRLMDB_UPLOAD_DISPLAY_LOG&b000000000000011498140", "EventSeverityCode": "9", "EventSourceId": "198.51.100.0", "EventSourceType": "IP Address", "GenericRiskLevel": "0", "NetworkHostnameActor": "test-1", "NetworkHostnameInitiator": "0.0.0.0", "NetworkHostnameReporter": "test-1", "NetworkIPAddressInitiator":

```
"0.0.0.0", "ServiceExecutableName": "00016", "ServiceExecutableType": "B", "ServiceInstanceName": "lab1_BLK_00", "ServiceProgramName": "RLMDB_UPLOAD_BACKGROUND",
"ServiceTransactionName": "S000", "SystemIdActor": "System25", "SystemGroupIdActor":
"BLN", "SystemGroupIdInitiator": "BLN", "SystemGroupIdIntermediary": "BLN", "SystemIdReporter": "System25", "SystemGroupIdReporter": "BLN", "SystemGroupIdTarget":
"BLN", "SystemTypeActor": "ABBA", "SystemGroupTypeActor": "SAP", "SystemGroupTypeInitiator": "SAP", "SystemGroupTypeIntermediary": "SAP", "SystemTypeReporter": "ABBA", "SystemGroupTypeReporter": "SAP", "SystemGroupTypeTarget":
"SAP", "UsernameDomainNameActing": "System25", "UsernameDomainTypeActing": "ABBA",
"UserPseudonymActing": "BLK_BTC_SMP", "TechnicalTimestampInteger": "1632210279522" } ]
} ] }
```

The parser processes the log header, and stores the data after the "[json]=" key into a variable called "_json".

Upon close inspection, we identify multiple distinct log events (several alerts) under a JSON key called "alerts".

To generate a new log event for each single alert, we pass this JSON to our split json function.

```
<setEventAttribute attr="_resultCount">splitJsonEvent($_json, "alerts", "[PH_DEV_MON_
CUSTOM_JSON]:[reptVendor]=SAP,[reptModel]=ETD,SAP_Individual_Event,json=", "",
"true")</setEventAttribute>
```

The `_resultCount` doesn't do much other than return an integer number of alerts we processed.

If we wanted to, we could do something with this, but mostly this variable is unused.

The arguments are explained above, but repeated below, the info is:

Arg1: our `$_json` var containing our JSON portion of the log.

Arg2: "alerts" - The JSON key holding the array of alert objects. The function will resolve here and treat each object as a new event.

Arg3: "[PH_DEV_MON_CUSTOM_JSON]:[reptVendor]=SAP,[reptModel]=ETD,SAP_Individual_Event,json=" We want the same parser handling the monolithic event to handle the individual events, so we attach this very unique log header.

Arg4: "" - Optional trailing string to append to log, in most cases we don't need this.

Arg5: "true" - String value of true or false to indicate if we should drop (not store or process) the monolithic event. In most cases after processing you don't want the original.

The individual events when triggered will look like this:

```
[PH_DEV_MON_CUSTOM_JSON]:[reptVendor]=SAP,[reptModel]=ETD,SAP_Individual_Event,json=
{"Id":"C60C48EF7B4E4D848F45F1904820C2CC","Timestamp":"2021-09-21T07:44:39.522Z","TechnicalLogEntryType":"SM21_D01","TechnicalNumber":"481537","TechnicalTimestampOfInsertion":"2021-09-
21T07:44:40.681Z","CorrelationId":"120CD18982991EEA9AB8F87143C8DE88","Cor-
```

```
relationSubId":"00000000000000000000000000000000","EventCode":"D01","EventSemantic":"Executable,Run,Cancel","EventLogType":"SystemLog","EventMessage":"LMDB_UPLOAD_ERRORS011","EventSeverityCode":"50","EventSourceId":"198.51.100.0","EventSourceType":"IPAddress","GenericRiskLevel":"3","NetworkHostnameActor":"test-1","NetworkHostnameInitiator":"0.0.0.0","NetworkHostnameReporter":"test-1","NetworkIPAddressInitiator":"0.0.0.0","ServiceExecutableName":"00016","ServiceExecutableType":"B","ServiceInstanceName":"lab1_BLK_00","ServiceProgramName":"RLMDB_UPLOAD_BACKGROUND","ServiceTransactionName":"S000","SystemIdActor":"System25","SystemGroupIdActor":"BLN","SystemGroupIdInitiator":"BLN","SystemGroupIdIntermediary":"BLN","SystemIdReporter":"System25","SystemGroupIdReporter":"BLN","SystemGroupIdTarget":"BLN","Sys-
```

```
temTypeAct-
or":"ABBA","Sys-
temGroupTypeAct-
or":"SAP","Sys-
temGroupTypeIni-
tiat-
or":"SAP","Sys-
temGroupTypeIn-
ter-
medi-
ary":"SAP","Sys-
temTypeRe-
port-
er":"ABBA","Sys-
temGroupTypeRe-
port-
er":"SAP","Sys-
temGroupTypeTar-
get":"SAP","User-
nameDo-
mainNameAct-
ing":"System25","UsernameDomainTypeActing":"ABBA","UserPseudonymActing":"BLK_BTC_
SMP","EventName":"Ex-
ecut-
ableRun-
Cancel","EventNamespace":"ht-
tp://sap.com/secmon","TechnicalTimestampInteger":"1632210279522"}
```

Notice that the contents of the JSON body of the log is the first alert object in the original monolithic event.

We can now parse the individual event via a matching parser (either using the same parser as the original event, or by using a different parser).

Combining Two or More Strings to Produce a Final String

This is accomplished by the **combineMsgId** function.

```
<setEventAttribute attr="eventType">combineMsgId("string-", $_evIdPrefix, "-", $_
evIdSuffix)</setEventAttribute>
_evIdPrefix: prefix
_evIdSuffix: suffix
eventType: string-prefix-suffix
```

Strings can only be wrapped by double quotes " but not single quotes '.

Normalize MAC Address

This is accomplished by the **normalizeMAC** function.

```
<setEventAttribute attr="hostMACAddr">normalizeMAC($_mac)</setEventAttribute>
```

Compare Interface Security Level

This is accomplished by the **compIntfSecVal** function.

```
<setEventAttribute attr="_result">compIntfSecVal($srcIntf, $destIntf)</setEventAttribute>
```

Compare the Security Level of `srcIntf` and `destIntf`. The result may be "LESS", "GREATER" or "EQUAL".

Convert Hex Number to Decimal Number

This is accomplished by the **convertHexStrToInt** function.

```
<setEventAttribute attr="ipConnId">convertHexStrToInt($_ipConnId)</setEventAttribute>
```

Convert TCP/UDP Protocol String to Port Number

This is accomplished by the following **convertStrToIntIpPort** function.

```
<setEventAttribute attr="destIpPort">convertStrToIntIpPort($_dport)</setEventAttribute>
```

Convert Protocol String to Number

This is accomplished by the following **convertStrToIntIpProto** function.

```
<setEventAttribute attr="ipProto">convertStrToIntIpProto($_proStr)</setEventAttribute>
```

Convert Decimal IP to String

This is accomplished by the following **convertIpDecimalToStr** function.

```
<setEventAttribute attr="srcIpAddr">convertIpDecimalToStr($_srcIpAddr)</setEventAttribute>
```

Convert Host Name to IP

This is accomplished by the following **convertHostNameToIp** function.

```
<setEventAttribute attr="srcIpAddr">convertHostNameToIp($_saddr)</setEventAttribute>
```

Add Two Numbers

This is accomplished by the following **add** function.

```
<setEventAttribute attr="totBytes">add($sentBytes, $recvBytes)</setEventAttribute>
```

Divide Two Numbers

This is accomplished by the following **divide** function.

```
<setEventAttribute attr="memUtil">divide($_usedMem, $_totalMem)</setEventAttribute>
```

Scale

This is accomplished by the following **scale** function.

```
<setEventAttribute attr="durationMSec">scale($_durationSec, 1000)</setEventAttribute>
```

Calculate Micro Seconds

This is accomplished by the following **calculateMSec** function.

```
<setEventAttribute attr="durationMSec">calculateMSec($_duration)</setEventAttribute>
_duration: 00:00:15
durationMSec: 15000
```

Extract Host from FQDN

This is accomplished by the following **extractHostFromFQDN** function.

```
<setEventAttribute attr="hostName">extractHostFromFQDN($_fqdn)</setEventAttribute>
_fqdn: host.abc.net
hostName: host
```

If `_fqdn` contains dot, get the string before the first dot; otherwise, get the whole string.

Replace String by Regular Expression

This is accomplished by the following **replaceStringByRegex** function.

```
<setEventAttribute attr="eventType">replaceStringByRegex($_eventType, "\s+", "_")</-
setEventAttribute>
_eventType: Event Type
eventType: Event_Type
```

Replace String in String

This is accomplished by the following **replaceStrInStr** function.

```
<setEventAttribute attr="computer">replaceStrInStr($_computer, "\\", "")</-
setEventAttribute>
```

Resolve DNS Name

This is accomplished by the following **resolveDNSName** function.

```
<setEventAttribute attr="destIpAddr">resolveDNSName($destName)</setEventAttribute>
```

Shift Time Sec

This is accomplished by the following **shiftTimeSec** function.

```
<setEventAttribute attr="logonTime">shiftTimeSec($_mon, $_day, $_year, $_time, $_durationSec)</setEventAttribute>
_mon: 1
_day: 1
_year: 2000
_time: 01:00:10
_durationSec: 10
logonTime: 01:00:00 01/01/2000
```

To DateTime

This is accomplished by the following **toDateTime** function.

```
<setEventAttribute attr="deviceTime">toDateTime($_mon, $_day, $_year, $_time)</setEventAttribute>
<setEventAttribute attr="deviceTime">toDateTime($_mon, $_day, $_time)
</setEventAttribute>
```

Trim Attribute

This is accomplished by the following **trimAttribute** function.

```
<setEventAttribute attr="destName">trimAttribute($destName, ".")
</setEventAttribute>
```

Trim leading and trailing dots in `destName`.

Get Severity from Syslog Priority

This is accomplished by the following **getEventSeverityFromSyslogPriority** function.

```
<setEventAttribute attr="eventSeverity">getEventSeverityFromSyslogPriority($_pri)</setEventAttribute>
_pri: 52
eventSeverity: 5
```

Set severity by syslog priority. The bottom 3 bits of the priority indicates the severity.

http://en.wikipedia.org/wiki/Syslog

To Unix Time (with Time Zone)

This is accomplished by the following **toUnixTime** function.

```
<setEventAttribute attr="deviceTime">toUnixTime($_deviceTime)</setEventAttribute>
_deviceTime: 20130509073221.932817-000
```

Decode Base64

This is accomplished by the following **decodeBase64** function.

```
<setEventAttribute attr="httpFullRequest">decodeBase64($_msg)</setEventAttribute>
```

Unzip String

This is accomplished by the following **unzip** function.

```
<setEventAttribute attr="msg">unzip($_msg)</setEventAttribute>
```

Calculate Latency

This is accomplished by the following **calculateLatency** function.

```
<setEventAttribute attr="_latency">calculateLatency($_evtRecvTime, $deviceTime)</-
setEventAttribute>
```

Calculate the latency. If `_evtRecvTime` is later than `deviceTime`, return the latency in seconds. Otherwise, return 0.

Parser Examples

The followng example is based on **Cisco IOS Syslog Parser**. The objective is to parse this syslog message:

```
<190>91809: Jan  9 02:38:47.872: %SEC-6-IPACCESSLOGP: list testlog permitted tcp
192.168.20.33(3438) -> 69.147.86.184(80), 1 packet
```

Complete these steps to create an appropriate parser.

- Add Device Type
- Create the Parser Specification and Add Local Patterns
- Define the Format Recognizer
- Parse the Syslog Header
- Parse the Syslog Body
- Final Parser
- Parsed Output

Add Device Type

Create a `CiscoIOSParser.xml` file with this content:

```
<eventParser name="CiscoIOSParser">
   <deviceType>
      <Vendor>Cisco</Vendor>
      <Model>IOS</Model>
      <Version>ANY</Version>
   </deviceType>
</eventParser>
```

Create the Parser Specification and Add Local Patterns

Create the parser XML file with this content, and add the pattern definition `patCiscoIOSMod` for detecting IOS modules such as SEC.

```
<eventParser name="CiscoIOSParser">
   <deviceType>
       <Vendor>Cisco</Vendor>
      <Model>IOS</Model>
      <Version>ANY</Version>
   </deviceType>
   <patternDefinitions>
      <pattern name="patCiscoIOSMod" list="begin">  <![CDATA[FW|SEC|SEC_
LOGIN|SYS|SNMP|]]></pattern>
     <pattern name="patCiscoIOSMod" list="continue"><![CDATA
[LINK|SPANTREE|LINEPROTO|DTP|PARSER|]]></pattern>
     <pattern name="patCiscoIOSMod" list="end"><![CDATA[CDP|DHCPD|CONTROLLER|PORT_
SECURITY-SP]]></pattern>
     <pattern name="patStrEndColon"><![CDATA[[^:]*]]></pattern>
     <pattern name="patComm"><![CDATA[[^,]+]]></pattern>
  </patternDefinitions>
</eventParser>
```

Define the Format Recognizer

Add this format recognizer for detecting `%SEC-6-IPACCESSLOGP`, which is a signature of Cisco IOS syslog messages.

```
<eventParser name="CiscoIOSParser">
   <deviceType>
      <Vendor>Cisco</Vendor>
      <Model>IOS</Model>
      <Version>ANY</Version>
   </deviceType>
   <patternDefinitions>
     <pattern name="patCiscoIOSMod" list="begin">  <![CDATA[FW|SEC|SEC_
LOGIN|SYS|SNMP|]]></pattern>
     <pattern name="patCiscoIOSMod" list="continue"><![CDATA
[LINK|SPANTREE|LINEPROTO|DTP|PARSER|]]></pattern>
     <pattern name="patCiscoIOSMod" list="end"><![CDATA[CDP|DHCPD|CONTROLLER|PORT_
SECURITY-SP]]></pattern>
     <pattern name="patStrEndColon"><![CDATA[[^:]*]]></pattern>
     <pattern name="patComm"><![CDATA[[^,]+]]></pattern>
```

```
    </patternDefinitions>
    <eventFormatRecognizer>
      <![CDATA[: %<:patCiscoIOSMod>-<:gPatInt>-<:patStrEndColon>:]]>
    </eventFormatRecognizer>
</eventParser>
```

Parse the Syslog Header

A syslog message consists of a syslog header and a body. For better organization, first parse the syslog header and event type. Subsequent code will include event type specific parsing, which is why event type is extracted in this step. In this example, the header is in boldface.

`<190>91809: Jan 9 02:38:47.872: %SEC-6-IPACCESSLOGP:` `list testlog permitted tcp 192.168.20.33(3438) -> 69.147.86.184(80), 1 packet`

The XML code for parsing the header does the following:

1. Matches the pattern `<190>91809: Jan 9 02:38:47.872: %SEC-6-IPACCESSLOGP:`
2. Sets the `eventType` attribute to `IOS-SEC- IPACCESSLOGP`.
3. Sets `deviceTime`.
4. Sets event severity (1-7 scale in Cisco IOS, 1=> most severe, to normalized 1-10 scale in FortiSIEM where 10=>most severe)
5. Saves the event `list testlog permitted tcp 192.168.20.33(3438) -> 69.147.86.184 (80), 1 packet` in a temporary variable `_body`.

Note that the patterns `gPatSyslogPRI`, `gPatMon`, `gPatDay`, `gPatTime`, `gPatInt`, and `gPatmesgBody` are global patterns that are defined in the `GeneralPatternDefinitions.xml` file:

```
<generalPatternDefinitions>
 <pattern name="gPatSyslogPRI"><![CDATA[<\d+>]]></pattern>
 <pattern name="gPatMesgBody"><![CDATA[.*]]></pattern>
 <pattern name="gPatMon"> <![CDATA[Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec|\d
{1,2}]]></pattern>
 <pattern name="gPatDay"><![CDATA[\d{1,2}]]></pattern>
 <pattern name="gPatTime"><![CDATA[\d{1,2}:\d{1,2}:\d{1,2}]]></pattern>
 <pattern name="gPatInt"><![CDATA[\d+]]></pattern>
</generalPatternDefinitions>
```

This parser file XML fragment for parsing the example syslog message looks like this:

```
<parsingInstructions>
    <collectFieldsByRegex src="$_rawmsg"><regex><![CDATA[<:gPatSys-
logPRI>?<:gPatMon>\s+<:gPatDay>\s+<:gPatTime> %<evIdPrefix:patCiscoIOSMod>-<_sever-
ity:gPatInt>-<_evIdSuffix:patStrEnd
Colon>: <_body:gPatMesgBody>]]></regex>
    </collectFieldsByRegex>
    <setEventAttribute attr="eventType">combineMsgId("IOS-",$_evIdPrefix, "-", $_
evIdSuffix)</setEventAttribute>
    <choose>
        <when test='$_severity IN "6, 7"'>
            <setEventAttribute attr="eventSeverity">1</setEventAttribute>
        </when>
        <when test='$_severity = "1"'>
           <setEventAttribute attr="eventSeverity">10</setEventAttribute>
        </when>
        <when test='$_severity = "2"'>
           <setEventAttribute attr="eventSeverity">8</setEventAttribute>
        </when>
        <when test='$_severity IN "3, 4"'>
          <setEventAttribute attr="eventSeverity">5</setEventAttribute>
      </when>
      <when test='$_severity = "5"'>
          <setEventAttribute attr="eventSeverity">2</setEventAttribute>
      </when>
    </choose>
<parsingInstructions>
```

Parse the Syslog Body

The parsing is done on an `eventType` by `eventType` basis, because the formats are `eventType`-specific. Parsing the syslog body involves three steps:

1. Parsing the action string. Based on the action staring value (`permit` or `denied`), modify the `eventType` by appending the action string value at the end, and also modify the `eventSeverity` values.
2. Parsing the protocol, source, and destination IP, port, and totalPackets.
3. Converting the protocol string to a protocol integer.

```
<choose>
   <when test='$eventType IN "IOS-SEC-IPACCESSLOGP,IOS-SEC-IPACCESSLOGDP, IOS-SEC-
IPACCESSLOGRP"'>
       <collectAndSetAttrByRegex src="$_body">
       <regex><![CDATA[list <_aclName:gPatStr>\s+<_action:gPatWord>\s+<_pro-
to:gPatWord>\s+<srcIpAddr
:gPatIpV4Dot>\(<srcIpPort:gPatInt>\)<:gPatMesgBody>->\s+<destIpAddr:gPat
IpV4Dot>\(<destIpPort:gPatInt>\),\s+<totPkts:gPatInt> <:gPatMesgBody>]]>
                  </regex>
       </collectAndSetAttrByRegex>
       <choose>
          <when test='$_action = "permitted"'>
              <setEventAttribute attr="eventType">combineMsgId("IOS-",$_evIdPrefix, "-
", $_evIdSuffix, "-PERMITTED")</setEventAttribute>
        <setEventAttribute attr="eventSeverity">1</setEventAttribute>
          </when>
          <when test='$_action = "denied"'>
               <setEventAttribute attr="eventType">combineMsgId("IOS-",$_evIdPrefix,
"-", $_evIdSuffix, "-DENIED")</setEventAttribute>
               <setEventAttribute attr="eventSeverity">3</setEventAttribute>
          </when>
       </choose>
       <setEventAttribute attr="ipProto">convertStrToIntIpProto($_pro-
to)</setEventAttribute>
   </when>
</choose>
```

Final Parser

```
<eventParser name="CiscoIOSParser">
    <deviceType>
      <Vendor>Cisco</Vendor>
      <Model>IOS</Model>
      <Version>ANY</Version>
    </deviceType>
    <patternDefinitions>
        <pattern name="patCiscoIOSMod" list="begin"> <![CDATA[FW|SEC|SEC_
LOGIN|SYS|SNMP|]]></pattern>
        <pattern name="patCiscoIOSMod" list="continue"> <![CDATA
[LINK|SPANTREE|LINEPROTO|DTP|PARSER|]]></pattern>
        <pattern name="patCiscoIOSMod" list="end"><![CDATA[CDP|DHCPD|CONTROLLER|PORT_
SECURITY-SP]]></pattern>
        <pattern name="patStrEndColon"><![CDATA[[^:]*]]></pattern>
        <pattern name="patComm"><![CDATA[[^,]+]]></pattern>

      </patternDefinitions>
    <parsingInstructions>
    <!—parse header -->
    <collectFieldsByRegex src="$_rawmsg"><regex><![CDATA[<:gPatSys-
logPRI>?<:gPatMon>\s+<:gPatDay>\s+<:gPatTime>
%<_evIdPrefix:patCiscoIOSMod>-<_severity:gPatInt>-<_evIdSuffix:patStrEnd
Colon>: <_body:gPatMesgBody>]]></regex>
    </collectFieldsByRegex>
    <setEventAttribute attr="eventType">combineMsgId("IOS-",$_evIdPrefix, "-", $_
evIdSuffix)</setEventAttribute>
```

```
    <choose>
        <when test='$_severity IN "6, 7"'>
            <setEventAttribute attr="eventSeverity">1</setEventAttribute>
        </when>
        <when test='$_severity = "1"'>
           <setEventAttribute attr="eventSeverity">10</setEventAttribute>
        </when>
        <when test='$_severity = "2"'>
           <setEventAttribute attr="eventSeverity">8</setEventAttribute>
        </when>
        <when test='$_severity IN "3, 4"'>
          <setEventAttribute attr="eventSeverity">5</setEventAttribute>
      </when>
      <when test='$_severity = "5"'>
          <setEventAttribute attr="eventSeverity">2</setEventAttribute>
      </when>
    </choose>
    <!—parse body -->
    <choose>
      <when test='$eventType IN "IOS-SEC-IPACCESSLOGP,IOS-SEC-IPACCESSLOGDP, IOS-SEC-
IPACCESSLOGRP"'>
          <collectAndSetAttrByRegex src="$_body">
       <regex><![CDATA[list
<_aclName:gPatStr>\s+<_action:gPatWord>\s+<_proto:gPatWord>\s+<srcIpAddr
:gPatIpV4Dot>\(<srcIpPort:gPatInt>\)<:gPatMesgBody>->\s+<destIpAddr:gPat
IpV4Dot>\(<destIpPort:gPatInt>\),\s+<totPkts:gPatInt> <:gPatMesgBody>]]>
                  </regex>
          </collectAndSetAttrByRegex>
          <choose>
              <when test='$_action = "permitted"'>
                 <setEventAttribute attr="eventType">combineMsgId("IOS-", $_evIdPre-
fix, "-", $_evIdSuffix,
"-PERMITTED")</setEventAttribute>
          <setEventAttribute attr="eventSeverity">1</setEventAttribute>
              </when>
              <when test='$_action = "denied"'>
                 <setEventAttributeattr="eventType">combineMsgId("IOS-", $_evIdPrefix,
"-", $_evIdSuffix,
"-DENIED")</setEventAttribute>
                 <setEventAttribute attr="eventSeverity">3</setEventAttribute>
```

```
                </when>
            </choose>
            <setEventAttribute attr="ipProto">convertStrToIntIpProto($_pro-
to)</setEventAttribute>

        </when>
    </choose>
<parsingInstructions>
```

Parsed Output

Input syslog:

```
<190>91809: Jan 9 02:38:47.872: %SEC-6-IPACCESSLOGP: list testlog permitted tcp
192.168.20.33(3438) -> 69.147.86.184(80), 1 packet
```

Parsed fields:

1. **phRecvTime**: the time at which the event was received by FortiSIEM
2. **phDeviceTime**: Jan 9 02:38:47 2010
3. **eventType**: SEC-IPACCESSLOGP-PERMITTED
4. **eventSeverity**: 3
5. **eventSeverityCategory**: LOW
6. **aclName**: testlog
7. **ipProto**: 6
8. **srcIpAddr**: 192.168.20.33
9. **destIpAddr**: 69.147.86.184
10. **srcIpPort**: 3438
11. **destIpPort**: 80
12. **totPkts**: 1

Working with Custom Performance Monitors

Creating a custom performance monitor involves creating a performance object that specifies the monitoring access protocol to use, maps event attributes available for that protocol to FortiSIEM event attribute types, and then associates those attributes to an event type. You can use system or user-defined device types, event attribute types, and event types when creating the performance object. The following sections provide information about working with Performance Monitors:

- Creating a Custom Performance Monitor
- Monitoring Protocol Configuration Settings
- Mapping Monitoring Protocol Objects to Event Attributes
- Managing Monitoring of System and Application Metrics for Devices
- Examples of Custom Performance Monitors

Creating a Custom Performance Monitor

You can create Custom Performance Monitors by defining the performance object that you want to monitor, including the relationship between the performance object and FortiSIEM events and event attributes, and then associating the performance object to a device type.

In Service Provider FortiSIEM deployments, custom performance performance have to be created by the Super-/Global account, and apply to all organizations. In enterprise deployments, custom performance monitors can be created by any user who has access to the **ADMIN** tab.

Prerequisites

- You should review the configuration settings for the monitoring protocols that you will use in your monitor, and be ready to provide the appropriate OIDs, classes, or database table attributes for the access protocol.
- You should have created any new device/application types, event attributes, or event types that you want to use in your Performance Monitor.
- You should have the IP address and access credentials for a device that you can use to test the monitor.

Creating the Performance Object and Applying it to a Device

1. Go to **ADMIN** > **Device Support** > **Monitoring**.
2. Click **New**.
3. Enter a **Name** for the Performance Monitor.
4. For **Type**, select either **System** or **Application**.
5. For **Method**, select the monitoring protocol for the performance monitor.
   See the topics under Monitoring Protocol Configuration Settings for more information about the configuration settings for each type of monitoring protocol.
6. Click **New** next to **List of Attributes**, and create the mapping between the performance object and FortiSIEM event attributes.
   Note that the Method you select will determine the name of this mapping and the configuration options that are available. See Mapping Monitoring Protocol Objects to Event Attributes for more information.
7. Select the **Event Type** that will be monitored. Event Types used for Custom Monitoring must begin with `PH_DEV_MON_CUST_`.
8. Enter the **Polling Frequency** for the monitor.
9. Enter a **Description**.
10. Click **Save**.
11. Under **Enter Device Type to Performance Object Association** section, click **New**.
12. Enter a **Name** for the mapping.
13. Select the **Device Type** from the drop-down for which you want to apply the monitor.
    Whenever a device belonging to the selected device type is discovered, FortiSIEM will attempt to apply the performance monitor to it.
14. Click **Perf Objects** drop-down to select or search the Performance Objects.
15. Click **Save**.

Testing the Performance Monitor

1. Go to **ADMIN** > **Device Support** > **Monitoring**.
2. Select the Performance Monitor.

3. Click **Test**.
4. For **IP**, enter the IP address of the device that you want to use to test the monitor.
   Testing for Multi-Tenant Deployments: If you have a Service Provider FortiSIEM, select the Supervisor or Collector where the device is monitored.
5. Click **Test**.If the test succeeds, click **Close**, and then click **Apply** to register the new monitor with the back-end module.

After you have successfully tested and applied the performance monitor, you should initiate discovery of the device that it will monitor, and then make sure that the new monitor is enabled as described in Managing Monitoring of System and Application Metrics for Devices.

Monitoring Protocol Configuration Settings

These topics describe the configuration settings for monitoring Protocols such as SNMP, WMI, and JDBC that are used for creating custom Performance Monitors.

- JDBC Configuration Settings
- JMX Configuration Settings
- SNMP Configuration Settings for Custom Performance Monitors
- WMI Configuration Settings for Custom Performance Monitors
- Login Configuration Settings for Custom Performance Monitors

JDBC Configuration Settings

Use these settings when configuring JDBC as the access protocol for a custom performance monitor. You might want to review the topic Custom JDBC Performance Monitor for a Custom Table as an example of how to set up a custom performance monitor using JDBC.

Field	Setting/Notes
Method	JDBC
Database Type	Select the type of database to connect to
SQL Query	The SQL Query to execute when connecting
List of Columns	This creates the mapping between columns in the database and FortiSIEM event attributes. See Mapping Monitoring Protocol Objects to Event Attributes for more information.
Where Clause	This indicates whether the database table being queried has a fixed set of rows, or whether it is growing over time. An example of this would be a table containing logs, in which case FortiSIEM would keep track of the last entry and only pull the new ones. There are three options here: 1. There is a fixed set of rows and all rows are needed. Leave all options cleared. 2. There is a fixed set of rows and a fixed number of rows are needed. Select **Fixed records** and enter the number of required rows. 3. The table is growing and only new values are needed.

Field	Setting/Notes
	Select **Retrieve all new values since last retrieve time of column**, and enter the name of the column that represents time in the database. FortiSIEM will keep track of the largest value in this column and only pull entries greater than that value during the next polling interval.
Event Type	Select the **Event Type** from the drop-down for which you want to apply the monitor. Whenever a event belonging to the selected method is discovered, FortiSIEM will attempt to apply the performance monitor to it.
Polling Frequency	Enter the **Polling Frequency** for the monitor.

JMX Configuration Settings

When configuring JMX as the monitoring protocol for a custom performance monitor, use these settings. You may also want to review the topic Custom JMX Monitor for IBM Websphere as an example of creating a custom JMX performance monitor.

Field	Setting/Notes
Method	JMX
MBean	Enter the MBean interface that you want to monitor, or click the downward arrow to browse the JMX tree and select it. Note that the option you select here will determine the objects that are available when you select an **Object Attribute** for the **List of Attributes**. See the next section in this topic for information on how to find MBeans
Event Type	Select the **Event Type** from the drop-down for which you want to apply the monitor. Whenever a event belonging to the selected method is discovered, FortiSIEM will attempt to apply the performance monitor to it.
Polling Frequency	Enter the **Polling Frequency** for the monitor.

Identifying MBean Names and Attributes for Custom Applications

This section discusses how to get MBean names and attributes for custom J2EE based applications.

1. Launch JConsole on your workstation and connect to the application.
2. Select the **MBeans** tab.
3. Browse to the application you want to monitor, and select it.
4. In the right pane, you will see the `MBeanInfo`. Note the `ObjectName`, while the attributes for the application will be listed in the tree view.

SNMP Configuration Settings for Custom Performance Monitors

When configuring SNMP as the access protocol for a custom performance monitor, use these settings. You may also want to review the topics Custom SNMP Monitor for D-Link Interface Network Statistics and Custom SNMP Monitor for D-Link HostName and SysUpTime as example of how to set up a custom performance monitor using SNMP.

Field	Settings/Notes
Method	SNMP
Parent OID	The parent Object Identifier (OID) is used to optimize the number of SNMP GETs required for pulling the various individual OIDs. You can enter this directly, or click the downward arrow to select it from an MIB file. Several different MIB files are available to select from, see Importing OID Definitions from a MIB File for more information.
Parent ID is table	Select **is table** if the OIDs you want to monitor are in a table with at least one row. An example would be interface metrics, such as `ifInOctets` and `ifOutOctets`, since there is an interface metric for each interface.
List of OIDs	The OIDs you want to monitor mapped to FortiSIEM event attributes. The selection you make for **Parent OID** determines the options available in the **OID** menu when you select **New**.

Importing OID Definitions from a MIB File

Many devices include MIB files that you can then use to create a custom performance monitor for the device. This involves creating a configuration file based on information in the MIB file, using that file as input for the `mib2xml` executable, and then placing the resulting output file in the `/data/mibXml` directory of your Supervisor. Once placed in this directory, you can select the file from the **MIB File List** menu to select the parent OID, which will then also affect which OIDs you can select for the OID to event attribute mapping.

Procedure

1. Collect the device OID files you want to use and place them in a directory where the mib2XML resides.
2. Create the input config file with these fields, and name it with the `.cfg` file extension.
   See the attached alcatel.cfg file for an example. (**Note:** the link is available only in the HTML version of the User Guide.)

Field	Description
`group`	This is the number of MIB file group. MIB files must be analyzed as a group because of cross-references within them. The group attribute specifies an ID for each group and needs to be unique for every group.
`mibFile`	The name of the MIB file being analyzed. There can be multiple entries. Be sure to specify the path to the MIB files.
`vendor`	The name of the device vendor for the MIB file.
`model`	The model name or number for the device.
`evtPrefix`	As SNMP trap notification definitions in the MIB file are parsed, an event file is generated for each SNMP trap. This field specifies the event type prefix.
`enterpriseId`	The enterprise ID number for this vendor, which is used for generating the SNMP trap parser.

3. Run `mib2XML <filename>.cfg`.
4. Move the resulting `.mib.xml` file to the `/data/mibXml` directory of your Supervisor.

Example

In this example, a set of MIB files from an Alcatel 7x50 device are used to generate the XML output file. (**Note:** the following links are available only in the HTML version of the User Guide.)

1. Sample MIB files:
   TIMETRA-CHASSIS-MIB.mib
   TIMETRA-GLOBAL-MIB.mib
   TIMETRA-SYSTEM-MIB.mib
   TIMETRA-TC-MIB.mib
2. Information in these files, and the paths to them, are then used to create this config file.
   alcatel.cfg
3. Running `mib2xml alcatel.cfg` generates both an output and an mib2XML file.
   alcatel.out
   TIMETRA-TC-MIB.mib.xml

WMI Configuration Settings for Custom Performance Monitors

When configuring WMI as the monitoring protocol for a custom performance monitor, use these settings. You may also want to review the topic Custom WMI Monitor for Windows Domain and Physical Registry as example of how to set up a custom performance monitor using WMI.

Field	Settings
Method	WMI
Parent Class	WMI metrics are defined in the form of a parent class having multiple attributes. For example, the parent class `Win32_ComputerSystem` has the attributes `Domain` and `TotalPhysicalMemory`.
Is Table	If the parent WMI class is a table with one or more rows, select this option.

LOGIN Configuration Settings for Custom Performance Monitors

From the **Used For** drop-down list, choose **File Monitor**, **Target File**, **Command Output Monitoring**, or **Configuration Monitoring**.

Used For: File Monitor

Field	Settings
File Path	This setting is pre-populated with the **Parent OID/Class/File Path** value.

Used For: Target File

Field	Settings
File Path	This setting is pre-populated with the **Parent OID/Class/File Path** value.
Upload Target File	Click **Upload** and browse to the file you want to upload.

Used For: Command Output Monitoring

Field	Settings
Command	
Regular Expression	Enter a regex expression.
Matched Attribute Count	
Apply Regular Expression to	Select Single Line or Multiple Lines.
List of Attributes	Click **Edit** to edit an existing attribute or **New** to create a new attribute. See Adding Attributes for Command Output Monitoring.

Used For : Configuration Monitoring

Field	Settings
Upload Expect Script	Click **Upload** to browse for the script you want to use.

Adding Attributes for Command Output Monitoring

Click **New** to add a new attribute or **Edit** to modify an existing attribute.

Field	Settings
Matched Position	
Format	Select either **INTEGER**, **DOUBLE**, or **STRING** from the drop-down list.
Type	Select **Counter** or **Raw Value** from the drop-down list.
Event Attribute	Click the drop-down list and select an event attribute from the table.
Transform	For information on adding transforms, see Creating Transforms.

Mapping Monitoring Protocol Objects to Event Attributes

When you select a monitoring protocol for your custom performance monitor, you must also establish the relationship between the objects used by that protocol and event attributes in FortiSIEM. For example, creating a performance monitor that uses SNMP to monitor a device requires that you create a mapping between the SNMP OIDs that you want to monitor, and set of event attributes. This topic describes the configuration settings that you will use to create these object-to-event attribute relationships.

1. When creating your custom performance monitor, after you have selected the **Method**, click **New** next to **List of Attributes**.
   Depending on the monitoring protocol that you select, this table may be named **List of Oids** (SNMP), or **List of Columns** (JDBC).
2. In the first field, enter or select the monitoring protocol object that you want to map to FortiSIEM event attribute. Your options depend on the monitoring protocol you selected for Method.

Monitoring Protocol	Field name	Settings/Notes
SNMP	**OID**	Select an MIB file from the **MIB File List**, and then select the OID that you want to create the mapping for.You must enter an **Event Type** and a **Polling Frequency**.
WMI	**Attributes**	Enter an attribute of the WMI class you entered for **Parent Class**. You must enter an **Event Type** and a **Polling Frequency**.
JMX	**Object Attribute**	The **MBean** you select determines the attributes you can select. You must enter an **Event Type** and a **Polling Frequency**. You will also have to enter a **Name** and **Private Key** for the MBean attribute.
JDBC	**Column Name**	Select the **Database Type**, the **SQL Query** and specify the list of columns. You must enter an **Event Type** and a **Polling Frequency**.
WINEXE	**Matched Position**	Enter the Matched Position. You must enter an **Event Type** and a **Polling Frequency**.
LOGIN	**Used For**	Select **File Monitor**, **Target File**, **Command Output Monitoring**, or **Configuration Monitoring** from the drop-down list.

3. Select the **Format** for the object attribute.
   Your options will depend on the monitoring protocol you selected for Method.
4. For **Type**, select **Raw Value** or **Counter**.
5. For **Event Attribute**, select the FortiSIEM event attribute that the monitoring protocol object should map to.
   If you must create a new event attribute, see Adding an Event Attribute.
6. Create any **Transforms** of the values returned for the monitoring protocol object.
   See the next section for more information how to configure transforms.
7. Click **Save** when you are done creating the mappings, and complete the configuration of your custom performance monitor.

Creating Transforms

You can use a transform to convert the value returned for your monitoring project object into a more physically meaningful or usable metric. You an create multiple transforms, and they will be evaluated in the order shown in the table. Multiple transforms can be selected – they are evaluated in sequential order as shown in the display table.

1. Next to **Transforms**, click **New**.
2. For **Type**, select **system** or **custom**.
3. For **Formula**, either select a system-defined transformation formula from the menu if you selected **System** for **Type**, or enter a formula if you selected **custom**.
4. Click **Save**.

You can use the **Edit**, **Delete** or **Clone** buttons to modify, remove or clone a Transform respectively.

Managing Monitoring of System and Application Metrics for Devices

When FortiSIEM discovers devices, it also discovers the system and application metics that can be monitored for each device, and displays these in the **Monitor Performance** tab of **ADMIN** > **Setup**. Here you can also disable the monitoring of specific metrics for devices, disable devices from being monitored, and change the polling interval for specific metrics. See Checking status of event pulling jobs for checking the status.

1. Go to **ADMIN > Setup > Monitor Performance**.
2. Click **Refresh** icon to make sure you have the latest list of devices.
3. To disable monitoring for a device, clear the **Enable** option for it.
4. To enable or disable monitoring of a specific metrics for a device, click a device to select it, then click **More** and select **Edit System Monitors** or **Edit App Monitors**to view the list of metrics associated with that monitor and device. You can also enable or disable the metrics for a device's monitor type by clicking on the **Edit System Monitoring** or **Edit Application Monitoring** section for the device.
5. To change the polling interval for a metric, in the **More** menu, select **Edit Intervals**. Select the **Monitor Type** and **Device**, and then set the interval.
6. When you are done making changes, click **Save**.

Examples of Custom Performance Monitors

- Custom JDBC Performance Monitor for a Custom Table
- Custom SNMP Monitor for D-Link Interface Network Statistics
- Custom JMX Monitor for IBM Websphere
- Custom SNMP Monitor for D-Link HostName and SysUpTime
- Custom WMI Monitor for Windows Domain and Physical Registry

Custom JDBC Performance Monitor for a Custom Table

- Planning
- Adding New JDBC Performance Objects
- Associating Device Types to Performance Objects
- Testing the Performance Monitor
- Enabling the Performance Monitor
- Writing Queries for the Performance Metrics

Planning

Examining the Table Structure

For this example, consider two custom Oracle tables that you want to monitor.

1. A table called `HEALTH_STATIC_DEMO` that does not have time stamp as a column. The table does not grow with time, and the `HEALTH` column is updated by the application.

```
create table HEALTH_STATIC_DEMO
{
   ID        VARCHAR2 (200) not null,
   HOST_NAME NVARCHAR2 (200) not null,
   HEALTH    NVARCHAR2 (50)
}
```

2. A table called `HEALTH_DYNAMIC_DEMO` that has a time-stamp in the column `create_time`. Only records with a more recent time-stamp than previous ones have to be pulled in, and every time a new record is written, it includes a time stamp.

```
create table HEALTH_DYNAMIC_DEMO
{
   ID          VARCHAR2 (200) not null,
   HOST_NAME   NVARCHAR2 (200) not null,
   HEALTH      NVARCHAR2 (50),
   CREATE_TIME DATE not null
}
```

Creating New Device Types, Event Attribute Types, and Event Types

To create these items, go to **Admin > Device Support**, and select the appropriate tab(s) to start.

In this case, you only need to create two new event types to handle the contents of the two tables.

Naming Custom Event Types

All custom event types must begin with the prefix `PH_DEV_MON_CUST_` .

Event Types

Name	Device Type	Priority
`PH_DEV_MON_CUST_JDBC_PERFORMANCE_STATIC`	Generic	Low
`PH_DEV_MON_CUST_JDBC_PERFORMANCE_DYNAMIC`	Generic	Low

Adding New JDBC Performance Objects

Each table requires its own performance object for monitoring.

Performance Object Configuration for Static Table HEALTH_STATIC_DEMO

<table>
<tr><th>Field</th><th>Setting</th></tr>
<tr><td><b>Name</b></td><td><code>jdbc_static_perfObj</code></td></tr>
<tr><td><b>Type</b></td><td>Application</td></tr>
<tr><td><b>Method</b></td><td>JDBC</td></tr>
<tr><td><b>Database Type</b></td><td>Oracle Database Server</td></tr>
<tr><td><b>SQL Query</b></td><td><code>select * from health_static_demo</code></td></tr>
<tr><td><b>List of Columns</b></td><td><table>
<tr><th>Column Name</th><th>Name</th><th>Format</th><th>Event Attribute</th></tr>
<tr><td>host_name</td><td></td><td>STRING</td><td>hostName</td></tr>
<tr><td>health</td><td></td><td>STRING</td><td>health</td></tr>
</table></td></tr>
<tr><td><b>Where Clauses</b></td><td>Not applicable, since the table doesn't grow over time</td></tr>
<tr><td><b>Event Type</b></td><td><code>PH_DEV_MON_CUST_JDBC_PERFORMANCE_STATIC</code></td></tr>
<tr><td><b>Polling Frequency</b></td><td>180 seconds</td></tr>
</table>

Performance Object Configuration for Dynamic Table HEALTH_DYNAMIC_DEMO

<table>
<tr><th>Field</th><th>Setting</th></tr>
<tr><td><b>Name</b></td><td><code>jdbc_dynamic_perfObj</code></td></tr>
<tr><td><b>Type</b></td><td>Application</td></tr>
<tr><td><b>Method</b></td><td>JDBC</td></tr>
<tr><td><b>Database Type</b></td><td>Oracle Database Server</td></tr>
<tr><td><b>SQL Query</b></td><td><code>select * from health_dynamic_demo</code></td></tr>
<tr><td><b>List of Columns</b></td><td><table>
<tr><th>Column Name</th><th>Name</th><th>Format</th><th>Event Attribute</th></tr>
<tr><td>host_name</td><td></td><td>STRING</td><td>hostName</td></tr>
<tr><td>cpu_util</td><td></td><td>DOUBLE</td><td>cpuUtil</td></tr>
</table></td></tr>
</table>

Field	Setting
	mem_util DOUBLE memUtil create_time STRING createTime
Where Clauses	retrieve all new values since last retrieve time of column create_time
Event Type	`PH_DEV_MON_CUST_JDBC_PERFORMANCE_STATIC`
Polling Frequency	180 seconds

Associating Device Types to Performance Objects

In this example, the Oracle database runs on Microsoft Windows, so you must associate Microsoft Windows device types to the two performance objects. Because the discovered device type has to exactly match one of device types in this association for the discovery module to initiate monitoring, you must add other device types, such as Linux, if you also want to monitor Oracle databases over JDBC on those devices.

Edit Device to Performance Object

Field	Settings
Name	windows_oracle_perf_association
Device Types	• Microsoft Windows • Microsoft Windows 7 • Microsoft Windows 98 • Microsoft Windows ME • Microsoft Windows NT • Microsoft Windows Server 2000 • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • Microsoft Windows Vista • Microsoft Windows XP
Perf Objects	• jdbc_static_perfObj(JDBC) - Default Interval:3mins • jdbc_dynamic_perfObj(JDBC) - Default Interval:3mins

Testing the Performance Monitor

Before testing the monitor, make sure you have defined the access credentials for the database server, created the IP address to credentials mapping, and tested connectivity to the server.

1. Go to **ADMIN** > **Device Support** > **Monitoring**.
2. Select one of the performance monitors you created, and then click **Test**.

3. For **IP**, enter the address of the Oracle database server, and select either the Supervisor or Collector node that will retrieve the information for this monitor.
4. Click **Test**.

   You should see `succeed` under **Result**, and a parsed event attributes in the test result pane.
5. When the test succeeds, click **Close**, and then click **Apply** to register the new monitor with the back-end module.

Enabling the Performance Monitor

1. Discover or re-discover the device you want to monitor.
2. Once the device is successfully discovered, make sure that the monitor is enabled and pulling metrics.

Writing Queries for the Performance Metrics

You can now use a simple query to make sure that that the metrics are pulled correctly. The search results should display the metrics for the event attributes you defined.

1. Create a structured historical search, and in the **Filter Criteria**, enter `Event Type = "PH_DEV_MON_CUST_JDBC_PERFORMANCE_STATIC"; Group by:` [None]
   This should show the entries in the `HEALTH_STATIC_DEMO` table
2. Create a structured historical search, and in the **Filter Criteria**, enter `Event Type = "PH_DEV_MON_CUST_JDBC_PERFORMANCE_SDynamic"; Group by:` [None]
   This should show the entries in the `HEALTH_DYNAMIC_DEMO` table .

Custom SNMP Monitor for D-Link Interface Network Statistics

This example shows how to create a custom performance monitor for network interface statistics for D-link switches. In this case, the result is a table, with one set of metrics for each interface.

- Planning
- Adding the D-Link SNMP Performance Object
- Associating Device Types to Performance Objects
- Testing the Performance Monitor
- Enabling the Performance Monitor
- Writing Queries for the Performance Metrics

Planning

Matching SNMP OIDs to FortiSIEM Event Attribute Types

If you run the command `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.2.2.1` against the D-Link switch, you should see an output similar to this:

```
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifIndex.5 = INTEGER: 5
...
```

To get the interface index, you would run `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.2.2.1.1`:

```
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifIndex.5 = INTEGER: 5
...
```

To get interface queue length (the `outQLen` event attribute in FortiSIEM), you would run `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.2.2.1.21`:

```
IF-MIB::ifOutQLen.1 = Gauge32: 0
IF-MIB::ifOutQLen.2 = Gauge32: 0
IF-MIB::ifOutQLen.3 = Gauge32: 0
IF-MIB::ifOutQLen.4 = Gauge32: 0
IF-MIB::ifOutQLen.5 = Gauge32: 0
...
```

To get interface speed, you would run `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.2.2.1.5`:

```
IF-MIB::ifSpeed.1 = Gauge32: 1000000000
IF-MIB::ifSpeed.2 = Gauge32: 1000000000
IF-MIB::ifSpeed.3 = Gauge32: 1000000000
IF-MIB::ifSpeed.4 = Gauge32: 1000000000
IF-MIB::ifSpeed.5 = Gauge32: 1000000000
...
```

To get received bytes (the `recvBitsPerSec` event attribute in FortiSIEM), you would run `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.2.2.1.10`:

```
IF-MIB::ifInOctets.1 = Counter32: 0
IF-MIB::ifInOctets.2 = Counter32: 1247940872
IF-MIB::ifInOctets.3 = Counter32: 0
IF-MIB::ifInOctets.4 = Counter32: 0
IF-MIB::ifInOctets.5 = Counter32: 0
...
```

Finall,y to get sent bytes (the `sentBitsPerSec` event attribute in FortiSIEM), you would run `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.2.2.1.16`:

```
IF-MIB::ifOutOctets.1 = Counter32: 0
IF-MIB::ifOutOctets.2 = Counter32: 1271371281
IF-MIB::ifOutOctets.3 = Counter32: 0
IF-MIB::ifOutOctets.4 = Counter32: 0
IF-MIB::ifOutOctets.5 = Counter32: 0
...
```

From these outputs you can see that if you want to create a performance monitor for D-Link switch uptime, you must:

1. Create a new device type, since D-Link switches are not supported in this release.
2. Create an event type, `PH_DEV_MON_CUST_DLINK_INTF_STAT`, that will contain the event attribute types `outQLen` , `recvBitsPerSec`, and `sentBitsPerSec`, which are already part of the FortiSIEM event attribute library, and `hostNameSnmpIndx` and `intfSpeed`, which you must create.
3. Create the mapping between the SNMP OIDs and the event attributes:
   1. OID `.1.3.6.1.2.1.2.2.1.1` and `hostNameSnmpIndx`
   2. OID `.1.3.6.1.2.1.2.2.1.5` and `intfSpeed`
   3. OID `.1.3.6.1.2.1.2.2.1.21` and `outQLen`
   4. OID `.1.3.6.1.2.1.2.2.1.10` and `recvBitsPerSec`
   5. OID .1.3.6.1.2.1.2.2.1.16 and `sentBitsPerSec`

Creating New Device Types, Event Attributes, and Event Types

To create these items, go to **ADMIN > Device Support**, and select the appropriate tab(s) to start.

Device Type

Create a new device type with these attributes:

Field	Setting
Vendor	D-Link
Model	DGS
Version	Any
Device/App Group	**Devices > Network Devices > Router Switch**
Biz Service Group	<no selection>
Description	D-Link Switch

Event Attribute Types

Create these event attribute types:

Name	Display Name	Value Type	Display Format Type
hostSnmpIndex	Host Interface SNMP Index	INT64	<left blank>
intfSpeed	Interface Speed in bits/sec	INT64	<left blank>

Event Types

Naming Custom Event Types: All custom event types must begin with the prefix `PH_DEV_MON_CUST_` .

Create this event type:

Name	Device Type	Severity
PH_DEV_MON_CUST_INTF_STAT	D-Link DGS	Low

Adding the D-Link SNMP Performance Object

In this case, you will create one performance object that will map the SNMP OIDs to the FortiSIEM event attribute types, and then associate them with the PH_DEV_MON_CUST_INTF_STAT event type. When you create the recvBitsPerSec and sentBitsPerSec mapping you will also add a sequential transform to convert the cumulative metric to a rate, and then convert bytes per second to bits per second. .

Performance Object Configuration for Event Type PH_DEV_MON_CUST_INTF_STAT

<table>
<tr><th>Field</th><th>Setting</th></tr>
<tr><td><b>Name</b></td><td>D-LinkIntStat</td></tr>
<tr><td><b>Type</b></td><td>System</td></tr>
<tr><td><b>Method</b></td><td>SNMP</td></tr>
<tr><td><b>Parent OID</b></td><td>.1.3.6.1.2.1.2.2.1</td></tr>
<tr><td><b>Parent OID is Table</b></td><td>Selected</td></tr>
<tr><td><b>List of OIDs</b></td><td>
<table>
<tr><th>Object Attribute</th><th>Name</th><th>Format</th><th>Type</th><th>Event Attribute</th></tr>
<tr><td>.1.3.6.1.1.2.1.2.2.1.1</td><td>IntfIndex</td><td>INTEGER</td><td>RawValue</td><td>hostSnmpIndex</td></tr>
<tr><td>.1.3.6.1.1.2.1.1.2.1.5</td><td>intfSpeed</td><td>Gauge32</td><td>RawValue</td><td>intfSpeed</td></tr>
<tr><td>.1.3.6.1.1.2.1.1.2.1.10</td><td>recvBitsPerSec</td><td>Counter32</td><td>Counter</td><td>recvBitsPerSec</td></tr>
<tr><td>.1.3.6.1.1.2.1.1.2.1.16</td><td>sentBitsPerSect</td><td>Counter32</td><td>Counter</td><td>sentBitsPerSect</td></tr>
<tr><td>.1.3.6.1.1.2.1.1.2.1.21</td><td>outInftQ</td><td>Gauge32</td><td>RawValue</td><td>OutQLen</td></tr>
</table>
</td></tr>
<tr><td><b>Event Type</b></td><td>PH_DEV_MON_CUST_INTF_STAT</td></tr>
<tr><td><b>Polling Frequency</b></td><td>60 seconds</td></tr>
</table>

Transform Formula for recvBitsPerSec and sentBitsPerSec Event Attributes

Type	Formula
system	toRate
system	BytesPerSecToBitsPerSec

Associating Device Types to Performance Objects

In this case you would only need to make one association with the D-Link DGS device you created.

Field	Settings
Name	`D-LinkPerfObj`
Device Types	• D-Link DGS
Perf Objects	• D-LinkIntfStat(SNMP) - Default Interval:1mins

Testing the Performance Monitor

Before testing the monitor, make sure you have defined the access credentials for the D-Link device, created the IP address to credentials mapping, and tested connectivity.

1. Go to **ADMIN > Device Support > Monitoring**.
2. Select the performance monitor you created, and then click **Test**.
3. For **IP**, enter the address of the device, and select either the Supervisor or Collector node that will retrieve the information for this monitor.
4. Click **Test**.
   You should see `succeed` under **Result**, and the parsed event attributes in the test result pane.
5. When the test succeeds, click **Close**, and then click **Apply** to register the new monitor with the back-end module.

Enabling the Performance Monitor

1. Discover or re-discover the device you want to monitor.
2. Once the device is successfully discovered, make sure that the monitor is enabled and pulling metrics.

Writing Queries for the Performance Metrics

You can now use a simple query to make sure that that the metrics are pulled correctly. The search results should display the metrics for the event attributes you defined.

Create a structured historical search with these settings:

Filter Criteria	Display Columns	Time	For Organ-izations
Structured `Reporting IP IN <IP Range> AND Event Type =" PH_DEV_MON_CUST_INTF_STAT"; Group by: Host Name, Host Interface`	Host Name,Host Interface SNMP Index,MAX(Out Intf Queue), AVG (Intf Speed), AVG(Sent Bit Rate), AVG(Received Bit Rate)	Last 10 Minutes	All

Custom JMX Monitor for IBM Websphere

- Planning
- Adding New IBM WebSphere Performance Objects
- Associating Device Types to Performance Objects
- Testing the Performance Monitor
- Enabling the Performance Monitor
- Writing Queries for the Performance Metrics

This example illustrates how to write a custom performance monitor for retrieving IBM Websphere thread, heap memory, and non-heap memory metrics.

Planning

Creating New Device Types, Event Attribute Types, and Event Types

To create these items, go to **ADMIN > Device Support**, and select the appropriate tab(s) to start.

In this case, the IBM Websphere device type is already supported by FortiSIEM, but you must create new event attributes and event types for the metrics you want to retrieve.

Event Attribute Types

Name	Display Name	Value Type	Display Format Type
`websphere_heapPCT`	WebSphere HeapPct	INT64	
`websphere_numThreads`	WebSphere NumThreads	INT64	
`websphere_maxThreads`	WebSphere MaxThreads	INT64	
`websphere_threadPct`	WebSphere ThreadPct	INT64	
`websphere_numClass`	WebSphere NumClass	INT64	
`websphere_heapUsed`	WebSphere HeapUsed	INT64	Bytes
`websphere_heapMax`	WebSphere HeapMax	INT64	Bytes

Name	Display Name	Value Type	Display Format Type
websphere_heapCommitted	WebSphere HeapCommitted	INT64	Bytes
websphere_nonHeapUsed	WebSphere NonHeapUsed	INT64	Bytes
websphere_nonHeapMax	WebSphere NonHeapMax	INT64	Bytes
websphere_nonHeapCommitted	WebSphere NonHeapCommitted	INT64	Bytes

Event Types

Naming Custom Event Types: All custom event types must begin with the prefix PH_DEV_MON_CUST_ .

Name	Device Type	Severity
PH_DEV_MON_CUST_WEBSPHERE_HEAPMEMORY	IBM WebSphere App Server	Low
PH_DEV_MON_CUST_WEBSPHERE_NON_HEAPMEMORY	IBM WebSphere App Server	Low
PH_DEV_MON_CUST_WEBSPHERE_THREAD	IBM WebSphere App Server	Low

Adding New IBM WebSphere Performance Objects

Each of the event types requires creating a performance object for monitoring.

Performance Object Configuration for Event Type PH_DEV_MON_CUST_WEBSPHERE_HEAPMEMORY

Field	Setting
Name	websphere_heapMemory_perfObj
Type	Application
Method	JMX
MBean	java.lang:type=Memory

<table>
<tr><th>Field</th><th>Setting</th></tr>
<tr><td><b>List of Attributes</b></td><td>
<table>
<tr><th>Object Attribute</th><th>Private Key</th><th>Name</th><th>Format</th><th>Event Attribute</th></tr>
<tr><td>HeapMemoryUsage</td><td>committed</td><td>committed</td><td>Long</td><td>websphere_heapCommitted</td></tr>
<tr><td>HeapMemoryUsage</td><td>used</td><td>used</td><td>Long</td><td>websphere_heapUsed</td></tr>
<tr><td>HeapMemoryUsage</td><td>max</td><td>max</td><td>Long</td><td>websphere_heapMax</td></tr>
<tr><td></td><td></td><td></td><td>Long</td><td>websphere_heapPCT</td></tr>
</table>
</td></tr>
<tr><td><b>Event Type</b></td><td>PH_DEV_MON_CUST_WEBSPHERE_HEAPMEMORY</td></tr>
<tr><td><b>Polling Frequency</b></td><td>180 seconds</td></tr>
</table>

Performance Object Configuration for Event Type PH_DEV_MON_CUST_WEBSPHERE_THREAD

For the `webSphere_threadPct`**Event Attribute**, you will enter a transform as shown in the second table.

Field	Setting
Name	websphere_thread_perfObj
Type	Application
Method	JMX
MBean	java.lang:type=Threading

<table>
<tr><th>Field</th><th>Setting</th></tr>
<tr><td><b>List of Attributes</b></td><td>
<table>
<tr><th>Object Attribute</th><th>Private Key</th><th>Name</th><th>Format</th><th>Event Attribute</th></tr>
<tr><td>ThreadCount</td><td></td><td>ThreadCount</td><td>Long</td><td>websphere_numThreads</td></tr>
<tr><td>PeakThreadCount</td><td></td><td>PeakThreadCount</td><td>Long</td><td>websphere_maxThreads</td></tr>
<tr><td></td><td></td><td></td><td>Long</td><td>websphere_threadPCT</td></tr>
</table>
</td></tr>
<tr><td><b>Event Type</b></td><td>PH_DEV_MON_CUST_WEBSPHERE_THREAD</td></tr>
<tr><td><b>Polling Frequency</b></td><td>180 seconds</td></tr>
</table>

Transform Formula for websphere_threadPCT Event Attribute

Click **New** next to **Transforms** in the dialog to enter the formula.

<table>
<tr><th>Field</th><th>Settings</th></tr>
<tr><td><b>Object Attribute</b></td><td>&lt;blank&gt;</td></tr>
<tr><td><b>Name</b></td><td>&lt;blank&gt;</td></tr>
<tr><td><b>Private Key</b></td><td>&lt;blank&gt;</td></tr>
<tr><td><b>Format</b></td><td>Long</td></tr>
<tr><td><b>Event Attribute</b></td><td>websphere_threadPct</td></tr>
<tr><td><b>Transforms</b></td><td>
<table>
<tr><th>Type</th><th>Formula</th></tr>
<tr><td>custom</td><td>ThreadCount*100/PeakThreadcount</td></tr>
</table>
</td></tr>
</table>

Performance Object Configuration for Event Type PH_DEV_MON_CUST_WEBSPHERE_NON_HEAPMEMORY

<table>
<tr><th>Field</th><th>Setting</th></tr>
<tr><td><b>Name</b></td><td>websphere_nonHeapMemory_perfObj</td></tr>
<tr><td><b>Type</b></td><td>Application</td></tr>
<tr><td><b>Method</b></td><td>JMX</td></tr>
<tr><td><b>MBean</b></td><td>java.lang:type=Memory</td></tr>
<tr><td><b>List of Attributes</b></td><td>
<table>
<tr><th>Object Attribute</th><th>Private Key</th><th>Name</th><th>Format</th><th>Event Attribute</th></tr>
<tr><td>NonHeapMemoryUsage</td><td>used</td><td></td><td>Long</td><td>websphere_nonHeapUsed</td></tr>
<tr><td>NonHeapMemoryUsage</td><td>committed</td><td></td><td>Long</td><td>websphere_nonHeapCommitted</td></tr>
<tr><td>NonHeapMemoryUsage</td><td>max</td><td></td><td>Long</td><td>websphere_nonHeapMax</td></tr>
</table>
</td></tr>
<tr><td><b>Event Type</b></td><td>PH_DEV_MON_CUST_WEBSPHERE_NON_HEAPMEMORY</td></tr>
<tr><td><b>Polling Frequency</b></td><td>180 seconds</td></tr>
</table>

Associating Device Types to Performance Objects

In this example, IBM WebSphere runs on Microsoft Windows, so you must associate Microsoft Windows device types to the three performance objects. Because the discovered device type has to exactly match one of device types in this association for the discovery module to initiate these monitors, you must add other device types, such as Linux, if you also wanted to monitor IBM Websphere over JMX on those devices.

Edit Device to Performance Object

Field	Settings
Name	windows_oracle_perf_association
Device Types	• Microsoft Windows • Microsoft Windows 7 • Microsoft Windows 98 • Microsoft Windows ME

Field	Settings
	• Microsoft Windows NT • Microsoft Windows Server 2000 • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • Microsoft Windows Vista • Microsoft Windows XP
Perf Objects	• websphere_thread_perfObj(JMX) - Default Interval:3mins • websphere_thread_perfObj(JMX) - Default Interval:3mins • websphere_nonHeapMemory_perfObj (JMX) - Default Interval:3mins

Testing the Performance Monitor

Before testing the monitor, make sure you have defined the access credentials for the server, created the IP address to credentials mapping, and tested connectivity.

1. Go to **ADMIN > Device Support > Monitoring**.
2. Select one of the performance monitors you created, and then click **Test**.
3. For **IP**, enter the address of the Oracle database server, and select either the Supervisor or Collector node that will retrieve the information for this monitor.
4. Click **Test** .
   You should see `succeed` under **Result** , and the parsed event attributes in the test result pane.
5. When the test succeeds, click **Close**, and then click **Apply** to register the new monitor with the back-end module.

Enabling the Performance Monitor

1. Discover or re-discover the device you want to monitor.
2. Once the device is successfully discovered, make sure that the monitor is enabled and pulling metrics.

Writing Queries for the Performance Metrics

You can now use a simple query to make sure that that the metrics are pulled correctly. The search results should display the metrics for the event attributes you defined.

Create a structured historical search with these settings:

Filter Criteria	Display Columns	Time	For Organizations

Structured
`Reporting IP IN <IP Range> AND Event Type CONTAIN "ph_dev_mon_cust_web";`
`Group by: [None]`
	Event Receive Time,Reporting IP, Event	Last 60 Minutes	All

Custom SNMP Monitor for D-Link HostName and SysUpTime

Although D-link switches and routers are not supported in this release of FortiSIEM, you can still use the custom monitor feature to create a system uptime event that will collect basic performance metrics like `hostName` and `SysUpTime`.

- Planning
- Adding New IBM WebSphere Performance Objects
- Associating Device Types to Performance Objects
- Testing the Performance Monitor
- Enabling the Performance Monitor
- Writing Queries for the Performance Metrics

Planning

Mapping SNMP OIDs to FortiSIEM Event Attribute Types

If you run the command `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.1` against the D-Link switch, you should see an output similar to this:

```
SNMPv2-MIB::sysDescr.0 = STRING: DGS-1210-48          2.00.011
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.171.10.76.11
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (157556100) 18 days, 5:39:21.00
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: SJ-Test-Lab-D-Link
SNMPv2-MIB::sysLocation.0 = STRING: San Jose
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (157555949) 18 days, 5:39:19.49
```

To get sysUptime, you would run `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.1.3`:

```
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (157577770) 18 days, 5:42:57.70
```

To get `hostname`, you run `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.1.5`:

```
SNMPv2-MIB::sysName.0 = STRING: SJ-Test-Lab-D-Link
```

From these outputs you can see that if you want to create a performance monitor for D-Link switch uptime, you must:

1. Create a new device type, since D-Link switches are not supported in this release
2. Create an event type, `PH_DEV_MON_CUST_DLINK_UPTIME`, that will contain the event attribute types `hostName` and `SysUpTime`, which are already part of the FortiSIEM event attribute type library.
3. Create the mapping between the SNMP OIDs and the event attributes:
   - OID `.1.3.6.1.2.1.1.5` and `hostName`.
   - OID `.1.3.6.1.2.1.1.5` and `SysUpTime`.

Creating New Device Types, Event Attribute Types, and Event Types

To create these items, go to **ADMIN > Device Support**, and select the appropriate tab(s) to start.

Device Type:

Create a new device type with these attributes:

Field	Setting
Vendor	D-Link
Model	DGS
Version	Any
Device/App Group	**Devices > Network Devices > Router Switch**
Biz Service Group	<no selection>
Description	D-Link Switch

Event Attribute Types and Event Types

Both `sysUptime` and `hostName` are included in the **Event Attribute Types**, so you only need to create a new event type, `PH_DEV_MON_CUST_DLINK_UPTIME`, that will contain them.

Naming Custom Event Types

All custom event types must begin with the prefix `PH_DEV_MON_CUST_` .

Name	Device Type	Severity	Description
`PH_DEV_MON_CUST_DLINK_UPTIME`	D-Link DGS	0 - Low	D-Link Uptime

Adding the D-Link SNMP Performance Object

In this case, you will create one performance object that will map the SNMP OIDs to the FortiSIEM event attribute types `hostName` and `SysUptime`, and then associate them with the `PH_DEV_MON_CUST_DLINK_UPTIME` event type. When you create the `SysUpTime` mapping you will also add a transform to convert system time to centiseconds to seconds as shown in the second table.

Performance Object Configuration for Event Type PH_DEV_MON_CUST_DLINK_UPTIME

Field	Setting
Name	D-LinkUptime
Type	System
Method	SNMP
Parent OID	.1.3.6.1.1.2.1.1

<table>
<tr><th>Field</th><th>Setting</th></tr>
<tr><td><b>Parent OID is Table</b></td><td>&lt;left cleared&gt;</td></tr>
<tr><td><b>List of OIDs</b></td><td>
<table>
<tr><th>Object Attribute</th><th>Name</th><th>Format</th><th>Type</th><th>Event Attribute</th></tr>
<tr><td>.1.3.6.1.1.2.1.1.5</td><td>Host Name</td><td>String</td><td>RawValue</td><td><code>hostName</code></td></tr>
<tr><td>.1.3.6.1.1.2.1.1.3</td><td>Uptime</td><td>Timeticks</td><td>RawValue</td><td><code>SysUpTime</code></td></tr>
</table>
</td></tr>
<tr><td><b>Event Type</b></td><td><code>PH_DEV_MON_CUST_DLINK_UPTIME</code></td></tr>
<tr><td><b>Polling Frequency</b></td><td>10 seconds</td></tr>
</table>

Transform Formula for SysUptime Event Attribute

Type	Formula
custom	uptime/100

Associating Device Types to Performance Objects

In this case you would only need to make one association with the D-Link DGS device you created.

Field	Settings
Name	`D-LinkPerfObj`
Device Types	D-Link DGS
Perf Objects	D-LinkUptime(SNMP) - Default Interval:0.17mins

Testing the Performance Monitor

Before testing the monitor, make sure you have defined the access credentials for the D-Link device, created the IP address to credentials mapping, and tested connectivity.

1. Go to **ADMIN > Device Support > Performance Monitoring**.
2. Select the performance monitor you created, and then click **Test**.
3. For **IP**, enter the address of the device, and select either the Supervisor or Collector node that will retrieve the information for this monitor.
4. Click **Test**.
   You should see `succeed` under **Result**, and the parsed event attributes in the test result pane.
5. When the test succeeds, click **Close**, and then click **Apply** to register the new monitor with the back-end module.

Enabling the Performance Monitor

1. Discover or re-discover the device you want to monitor.
2. Once the device is successfully discovered, make sure that the monitor is enabled and pulling metrics.

Writing Queries for the Performance Metrics

You can now use a simple query to make sure that that the metrics are pulled correctly. The search results should display the metrics for the event attributes you defined.

Create a structured historical search with these settings:

Filter Criteria	Display Columns	Time	For Organizations
Structured `Reporting IP IN <IP Range> AND Event Type = "PH_DEV_MON_CUST_DLINK_UPTIME"; Group by: [None]`	Event	Last 10 Minutes	All

Custom WMI Monitor for Windows Domain and Physical Registry

- Planning
- Adding New IBM WebSphere Performance Objects
- Associating Device Types to Performance Objects
- Testing the Performance Monitor
- Enabling the Performance Monitor
- Writing Queries for the Performance Metrics

Planning

Mapping Windows WMI Classes to FortiSIEM Event Attribute Types

If you run the command `wmic -U <domain>/<user>%<pwd> //<ip> "select * from Win32_ComputerSystem` against a Windows server, you will see an output similar to this:

```
CLASS: Win32_ComputerSystem
AdminPass-
wordStatus::SEP::Auto-
mat-
icMan-
agedPage-
file::SEP::Auto-
mat-
icRe-
setBootOp-
tion::SEP::Auto-
```

maticResetCapability::SEP::BootOptionOnLimit::SEP::BootOptionOnWatchDog::SEP::BootROMSupported::SEP::BootupState::SEP::Caption::SEP::ChassisBootupState::SEP::CreationClassName::SEP::CurrentTimeZone::SEP::DaylightInEffect::SEP::Description::SEP::DNSHostName::SEP::Domain::SEP::DomainRole::SEP::EnableDaylightSavingsTime::SEP::FrontPanelResetStatus::SEP::InfraredSupported::SEP::InitialLoadInfo::SEP::InstallDate::SEP::KeyboardPasswordStatus::SEP::LastLoadInfo::SEP::Manufacturer::SEP::Model::SEP::Name::SEP::NameFormat::SEP::NetworkServerModeEnabled::SEP::Num-berOfLogicalProcessors::SEP::NumberOfProcessors::SEP::OEMLogoBitmap::SEP::OEMStringArray::SEP::PartOfDomain::SEP::PauseAfterReset::SEP::PCSystemType::SEP::PowerManagementCapabilities::SEP::PowerManagementSupported::SEP::PowerOnPasswordStatus::SEP::PowerState::SEP::PowerSupplyState::SEP::PrimaryOwnerContact::SEP::PrimaryOwnerName::SEP::ResetCapability::SEP::ResetCount::SEP::ResetLim-

```
it::SEP::Roles::SEP::Status::SEP::Sup-
portContactDe-
scrip-
tion::SEP::Sys-
temStar-
tupDelay::SEP::Sys-
temStar-
tupOp-
tion-
s::SEP::Sys-
temStar-
tupSet-
ting::SEP::Sys-
temType::SEP::ThermalState::SEP::TotalPhys-
icalMemory::SEP::UserName::SEP::WakeUpType::SEP::Workgroup

1::SEP::True::SEP::True::SEP::True::SEP::3::SEP::3::SEP::True::SEP::Normal
boot::SEP::WIN2008-ADS::SEP::3::SEP::Win32_ComputerSystem::SEP::-
420::SEP::True::SEP::AT/AT COMPATIBLE::SEP::WIN2008-
ADS::SEP::FortiSIEM.net::SEP::5::SEP::True::SEP::3::SEP::False::SEP::NULL::SEP::
(null)::SEP::3::SEP::(null)::SEP::VMware, Inc.::SEP::VMware Virtual Plat-
form::SEP::WIN2008-ADS::SEP::(null)::SEP::True::SEP::1::SEP::1::SEP::NULL::SEP::([MS_
VM_CERT/SHA1/27d66596a61c48dd3dc7216fd715126e33f59ae7],Welcome to the Virtual
Machine)::SEP::True::SEP::3932100000::SEP::0::SEP::NULL::SEP::False::SEP::0::SEP::0::S-
EP::3::SEP::(null)::SEP::Windows User::SEP::1::SEP::-1::SEP::-1::SEP::(LM_Work-
station,LM_Server,Primary_Domain_
Con-
troller,Timesource,NT,DFS)::SEP::OK::SEP::NULL::SEP::0::SEP::NULL::SEP::0::SEP::X86-
based PC::SEP::3::SEP::4293496832::SEP::FortiSIEM\Administrator::SEP::6::SEP::(null)
```

From this output you can see that the `Win32_ComputerSystem` WMI class has two attributes:

- `Domain`
- `TotalPhysicalMemory`

From these outputs you can see that if you want to create a performance monitor for Windows Domain and Physical Registry, you must:

1. Create an event type, `PH_DEV_MON_CUST_WIN_MEM,` that will contain the event attribute types `Domain` and `memTotalMB`, both of which are already contained in the FortiSIEM event attribute types library.

2. Create the mapping between the WMI class attributes and the FortiSIEM event attribute types:
    - WMI class attribute `Domain` and `Domain`.
    - WMI class attribute `TotalPhysicalMemory` (Bytes) and `memTotalMB` (type INT64). Because `TotalPhysicalMemory` returns in bytes, and `memTotalMB` is in `INT64`, a transform will be required to convert the metrics.

Creating New Device Types, Event Attributes, and Event Types

To create these items, go to **ADMIN > Device Support**, and select the appropriate tab(s) to start.

- **Device Type**
  Since Microsoft Windows is supported by FortiSIEM, you don't need to create a new device type.

- **Event Attribute Types and Event Types**
  Both `Domain` and `memTotalMB` are included in the FortiSIEM event attribute type library, so you only need to create a new event type, `PH_DEV_MON_CUST_WIN_MEM`, that will contain them.

- **Naming Custom Event Types**
  All custom event types must begin with the prefix `PH_DEV_MON_CUST_` .

Name	Device Type	Severity	Description
`PH_DEV_MON_CUST_WIN_MEM`	Microsoft Windows	0 - Low	Windows Domain and Memory

Adding the Microsoft Windows WMI Performance Object

In this case, you will create one performance object that will map the WMI Class attributes to the FortiSIEM event attribute types `Domain` and `memTotalMB`, and then associate them with the `PH_DEV_MON_CUST_WIN_MEM` event type. When you create the `memTotalMB` mapping you will also add a transform to convert bytes to INT64 as shown in the second table.

Performance Object Configuration for Event Type PH_DEV_MON_CUST_DLINK_UPTIME

Field	Setting
Name	WinMem
Type	System
Method	WMI
Parent Class	Win32_ComputerSystem
Parent Class is Table	<left cleared>

Field	Setting			
List of Attributes	**Attribute**	**Format**	**Type**	**Event Attribute**
	Domain	String	RawValue	`domain`
	TotalPhysicalMemory	Integer	RawValue	`memTotalMB`
Event Type	`PH_DEV_MON_CUST_WIN_MEM`			
Polling Frequency	20 seconds			

Transform Formula for TotalPhysicalMemory Event Attribute Type

Type	Formula
custom	TotalPhysicalMemory/1024/1024

Associating Device Types to Performance Objects

In this example, you must associate Microsoft Windows device types to the performance object.

Edit Device to Performance Object

Field	Settings
Name	WinMisc
Device Types	• Microsoft Windows • Microsoft Windows NT • Microsoft Windows Server 2000 • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • Microsoft Windows Vista • Microsoft Windows XP
Perf Objects	• WinMem(WMI) - DefaultInterval:0.33mins

Testing the Performance Monitor

Before testing the monitor, make sure you have defined the access credentials for the server, created the IP address to credentials mapping, and tested connectivity.

1. Go to **ADMIN > Device Support > Monitoring**.
2. Select one of the performance monitors you created, and then click **Test**.

3. For **IP**, enter the address of the Microsoft Windows server, and select either the Supervisor or Collector node that will retrieve the information for this monitor.
4. Click **Test**.
   You should see `succeed` under **Result**, and the parsed event attributes in the test result pane.
5. When the test succeeds, click **Close**, and then click **Apply** to register the new monitor with the back-end module.

Enabling the Performance Monitor

1. Discover or re-discover the device you want to monitor.
2. Once the device is successfully discovered, make sure that the monitor is enabled and pulling metrics.

Writing Queries for the Performance Metrics

You can now use a simple query to make sure that that the metrics are pulled correctly. The search results should display the metrics for the event attributes you defined.

Create a structured historical search with these settings:

Filter Criteria	Display Columns	Time	For Organizations
`Host IP = <IP> AND Event Type = " PH_DEV_MON_CUST_WIN_MEM";`**`Group by:`**`[None]`	Event Receive Time,Reporting IP,Domain,Total Memory (MB)	Last 10 Minutes	All

Working with Custom Properties

FortiSIEM includes over 30+ pre-defined global threshold properties that you can edit and use in rules, but you can also create custom threshold properties.

This section provides the procedure to configure Custom Properties.

- Adding a Custom Property
- Modifying a Custom Property

Adding a Custom Property

Complete these steps to add a custom property:

1. Go to **ADMIN** > **Device Support** > **Custom Properties**.
2. Click **New**.
3. Enter a **Name** and **Display Name** for the new property.
4. Enter the **Default Value** for the threshold.
5. Select the **Value Type** of threshold value.
   For most global threshold values, select **Double**. For **Map** thresholds, which apply to disks and interfaces, select the **Item Type** for the threshold value, and select the **Component Type** to which it applies.
6. Click **Save**.

Modifying a Custom Property

Complete these steps to modify a custom property:

1. Select one or more property from the list.
2. Click the required option:
   - **Edit** to modify a property setting.
   - **Delete** to remove a property.
3. Click **Save**.

Creating SNMP System Object Identifiers for Devices

If a new device has to be identified using SNMP System Object Identifiers (OIDs) during discovery, you can create a device type and add the SNMP System OID or this device from the FortiSIEM UI.

Complete these steps to create SNMP Object Identifiers for device discovery:

1. Go to **ADMIN** > **Device Support** > **SNMP SysObjectId**.
2. Click **New**.
3. Select the **Device Type** from the drop-down which lists all the devices added in the system under **Device Support** > **Device/Apps**.
4. Enter the **Hardware Model** of the device.
5. Enter an **SNMP SysObjectId** for the device.
6. Click **Save**.

Analyzing Custom Log Files

Custom CSV formatted log files can be uploaded from the FortiSIEM GUI for detailed analysis. For this, a mapping has to be defined from the CSV file columns to the event attributes. This generates a FortiSIEM event that can be searched, similar to an externally received event.

Complete these steps to upload a custom log file for analysis:

1. Set up a Parsing template:
    a. Go to **ADMIN** > **Device Support** > **Upload File**.
    b. Click **New**.
    c. Upload the log file under **Step 1: CSV file**:
        i. Browse to select the **Sample File** to upload.
        ii. Enter the **Separator** used in the CSV file.
        iii. To include the header, select **Header**.
        iv. Click **Next**.
    d. Map the CSV file columns to the event attributes under **Step 2: Attribute Mapping**:
        i. Select the event attributes to map to the CSV file columns.
        ii. Click **Next**.
    e. Set the template details under **Step 3: Template Details**:
        i. Enter a **Name** for the Template.
        ii. The **Event Type** is automatically updated based on the name.
        iii. Enter any **Description** about the Template.
        iv. Click **Save**.
2. Upload the file.
3. Run Reports.

Configuring Local Syslog File Ingestion from a Directory

Currently, FortiSIEM handles logs either (a) sent to it via Protocols such as Syslog, SNMP trap and so on or (b) pulled from devices via Protocols such as WMI, Checkpoint LEA and so on.

FortiSIEM can process log files copied to a directory on one of the FortiSIEM nodes:

- Copy the files to a specific directory named by the reporting device IP. For Service Provider installations, create this directory on the Collector of the Organization to which these log files belong. The attribute `event_sftp_directory` in `phoenix_config.txt` defines the path. For example, to handle logs from a device with IP: `1.2.3.4`, create log files in `<event_sftp_directory>/1.2.3.4`. A typical example is `opt/phoenix/cache/syslog/1.2.3.4`.
- Each log in the files should be formatted exactly in the same way as sent by the device. If this is a new log source, a new parser may need to be defined.
- Each file should have a distinct time stamp to prevent files from being overwritten.
- Set `event_eps_limit_controls in phoenix_config.txt` to control the EPS burst.
    - If `event_eps_limit_controls` is set to '10', FortiSIEM will process 30 events from this file in 3 seconds.
    - If `event_eps_limit_controls` is set to '0', FortiSIEM will process as many log files as possible and this may inhibit the overall EPS license usage.
    - If you change a `phoenix_config.txt` parameter, then reload the parser on that node.

Note the following:

- The log file is deleted once it has been read. Keep a separate backup if required.
- The system requires write access to the log file directory in order to delete the log file once read. This is important because if the log file cannot be deleted, it is repeatedly read and consumed by FortiSIEM resulting in many duplicate events and extra EPS consumption.

Configuring Local PCAP File Ingestion from a Directory

The configure local PCAP file ingestion from a directory, take the following steps:

Update the phoenix_config file.

1. Go to `/opt/phoenix/config/`.
2. Edit the `/opt/phoenix/config/phoenix_config.txt` file as follows:
   Change:
   ```
   # FSM upgrade preserves customer changes to parameter value
   pcap_file_directory= #/opt/phoenix/cache/PCAP
   ```
   to
   ```
   # FSM upgrade preserves customer changes to parameter value
   pcap_file_directory=/opt/phoenix/cache/PCAP
   ```
3. Save the file.
4. Create and chown the directory by running the following commands.
   ```
   [root@fortisiem ~]# mkdir /opt/phoenix/cache/PCAP
   [root@fortisiem ~]# chown admin:admin /opt/phoenix/cache/PCAP
   ```
5. Restart the application processes to read the configuration changes using the following commands. Note that this will cause a few minutes interruption to event processing, resulting in new events received being lost as the phParser process is restarted.
   ```
   [root@fortisiem PCAP]# phtools --stop phParser
   [root@fortisiem PCAP]# phtools --start phParser
   ```
6. Copy the .pcap file to the directory `/opt/phoenix/cache/PCAP`, using SCP or SFTP to copy the PCAP file to the directory. **Note**: the file will be deleted once ingested, keep another copy if required.
7. Search for the PCAP data by performing an Analytics query for 'Event Type = PH_DEV_MON_PCAP_DATA'. PCAP data is written as JSON formatted events with event type `PH_DEV_MON_PCAP_DATA`. Various attributes are also parsed, and can be used in advanced queries.

Health

The following sections provide procedures to view health information:

Viewing Cloud Health

The **ADMIN** > **Health** > **Cloud Health** page displays the status of the nodes in your deployment and the processes running on them. The top frame displays all of the available clouds and the lower frame provides information about the applications that are contained in the cloud selected in the main frame.

Complete these steps to view the information about Cloud health:

1. Go to **ADMIN** > **Health** > **Cloud Health** tab.
2. Click any node in the first frame to view its process details in the second frame.
   See the FortiSIEM Back-End Processes table for more information about the system role played by each process.

First Frame

Settings	Description
Name	Name of the available clouds
IP Address	IP address of the available clouds
Module Role	Module role, for example, "Super" for Supervisor.
HA/DR Role	High Availability or Disaster Recovery role, for example "Primary Leader".
Health	Current health of the cloud
Last Status Updated	The most recent time the status of the node was updated.
Version	Current version of the cloud
Cores	The number of cores the node has.
Memory Size	The memory size for the node
Swap Size	The swap size for the node
EPS	Events per second
Load Average	Average load of the cloud
CPU	Percentage CPU used

Settings	Description
Memory	Percentage Memory used
Swap	Percentage Swap space used
Disk	Percentage Disk used
Max Disk Read Wait	The maximum disk read/wait time (milliseconds).
Max Disk Write wait	The maximum disk write/wait time (milliseconds).
Upload Buffer	The current upload buffer size (KB) and queue.
Content Version	The content version used by node.

Second Frame

Settings	Description
Process Name	Name of the process
Owner	The owner of the process
Status	Status of the process
Uptime	Total up time of the process
CPU	Measure of the CPU that the process is using
Memory	Measure of the Memory that the process is using
Resident Memory	The amount of memory the process is allocated
Disk Read Rate	The disk read rate speed (KBps)
Disk Write Rate	The disk write rate speed (KBps)
SharedStore Type	SharedStore type (reader, writer)
SharedStore Position	SharedStore location
SharedStore Percent	SharedStore utilization percentage

FortiSIEM Back-End Processes

Process	Function	Present in Supervisor	Present in Worker	Present in Collector
Apache	Webserver for front-ending http (s) requests to AppSvr or other FortiSIEM nodes	x	x	x
AppSvr	Middleware for handling GUI requests, storing and managing PostgreSQL database and serving REST API requests from FortiSIEM nodes	x		
DBSvr	PostgreSQL Database for storing information displayed in FortiSIEM GUI other than events	x		
Node.js-charting	Message			
Node.js-pm2				
phAgentManager	Collects logs and metrics from devices or servers using protocols other than SNMP and WMI.	x	x	x
phCheckpoint	Collects logs from Checkpoint firewalls via LEA			
phDataManager	Stores the parsed events to event store (FortiSIEM EventDB or Elasticsearch)	x	x	
phDataPurger	Archives online event store (FortiSIEM EventDB or Elasticsearch). Implements event retention policy for FortiSIEM EventDB - both online FortiSIEM EventDB and archive.	x		
phDiscover	Discovers devices using various protocols such as SNMP, WMI and SSH	x		x

Process	Function	Present in Supervisor	Present in Worker	Present in Collector
phEventForwarder	Forwards events from FortiSIEM to external Systems	x	x	x
phIpIdentityMaster	Merges Identity and location audit trails from multiple phIpIdentityWorker modules to produce the final Identity and location audit trail. Stores the trail in PostgreSQL Database.			
phIpIdentityWorker	Produces Identity and location audit trail based on its own view of events	x	x	
phMonitor	Monitors the health of FortiSIEM processes. Distributes tasks from AppSvr to various processes on Supervisor and to phMonitor on Worker for further dustribution to processes on Worker nodes.			
phParser	Parses raw events and preparses them for storing into event store (FortiSIEM EventDB or Elasticsearch)	x	x	x
phPerfMonitor	Continually collects performance monitoring and configuration change data after discovery completes	x	x	x
phQueryMaster	Handles Adhoc queries from GUI for FortiSIEM EventDB. Paralellizes queries by sending them to phQueryWorkers and merges individual results to produce the final result.	x		
phQueryWorker	Handles individual FortiSIEM EventDB queries from phQueryMaster	x	x	
phReportLoader	Loads Report data into Report Server.	x		
phReportMaster	Handles individual FortiSIEM EventDB inline reports. Pro-	x		

Process	Function	Present in Supervisor	Present in Worker	Present in Collector
	duces results every 5 minutes.			
phReportWorker	Handles inline event reports FortiSIEM EventDB.Merges individual inline report results multiple phReportMaster modules to produce the final result. Rolls up results from 5 minute intervals to 15 minute intervals and then to 60 minute intervals.	x		
phRuleMaster	Triggers a rule in real time by evaluating rule summaries from individual phRuleWorker modules	x		
phRuleWorker	Evaluates a rule in real time based on events seen by the worker and sends a summary to the phRuleMaster module	x	x	
Redis	In-memory distributed database for holding results returned by Elasticsearch and for distributing CMDB objects between Supervisor and Worker nodes.	x	x	
SVNLite	A light weight version of Subversion, this file revision management tool stores the file change history for windows/linux servers, routers/switches and windows/linux agents. **Note**: • Files are stored in `/svn/repos`. • To conserve space, files are automatically deleted when the disk gets full based on thresholds defined in `svnlite.revisions.purge` on the Supervisor.	x		

Viewing Collector Health

If your FortiSIEM deployment includes Collectors, you can monitor the status of the Collectors in the **ADMIN** > **Health** > **Collector Health** page. You can also upgrade Collectors from this page. Select a Collector and click **Show Processes** to see the processes running on that Collector. Click **Tunnels** to open a Tunnels window to view any open tunnels. If you have upgraded or performed a fresh install of FortiSIEM 6.3.0, you will need to re-configure Tunnels to open them. See Open Tunnel Re-Configuration Required after 6.3.0 or later Upgrade/Fresh Install.
Refer to the 'FortiSIEM Back-End Processes' table below for information about the processes that run on Collectors.

The **Action** menu provides the operations you can perform on a Collector:

- **Start** - to start the Collector.
- **Stop** - to stop the Collector.
- **Download Image** - to download a Collector image.
- **Install Image** - to install a Collector image.
- **Download Update** - to download a Collector image update.
- **Install Update** - to install a Collector image update.

From the Tunnels window (appears when Tunnels is selected), the following operations are available.

- **Close Tunnel** - Select a tunnel, and click **Close Tunnel** to close the tunnel.
- **Close All** - Click to close all open tunnels.

For information on the table, see Properties associated with Tunnels.

Properties Associated with Collector Health

Collector Property	Description
Organization	Name of the organization to which the Collector belongs.
Collector ID	The ID of the Collector.
Collector Name	Name of the Collector.
IP Address	IP address of the Collector.
Health	Health of the Collector based on the health of the modules running on it. If Health is **Critical**, it means that one of the modules is not running on the Collector.
Last Status Updated	The time when the collector last reported its status to the cloud.
Last File Received	The time when the collector last reported its performance status to the cloud.
Collector Type	The Collector type is displayed.

Collector Property	Description
Version	The version of the Collector is displayed.
Cores	The number of cores the Collector has.
Memory Size	The Collector's memory size.
Swap Size	The Collector's disk swap size.
Uptime	Total time that the Collector has been up.
EPS	The number of events per second (EPS) dynamically allocated by the system to this collector.
CPU	Overall CPU utilization of the Collector.
Memory	Overall memory utilization of the Collector.
Swap	Overall swap utilization of the Collector.
Disk	Overall disk utilization of the Collector.
Max Disk Read Wait	The maximum disk read/wait time (milliseconds).
Max Disk Write wait	The maximum disk write/wait time (milliseconds).
Upload Buffer	Upload buffer size utilized.
Last Event Time	The time when the collector last reported events to the cloud.
Upgrade Version	If the Collector has been upgraded, the new version.
Build Date	Date on which the version of FortiSIEM the Collector is running on was built.
Content Version	Version of FortiSIEM the Collector is running on.
Content Update Status	The status of the content update is displayed.
Install Status	If you upgrade the Collector, the status of the upgrade is shown here as either **Success** or **Failed**.
Download Status	If an image was downloaded to the Collector, the status of the download is shown here as **Success** or **Failed**.

Process Properties

Process Property	Description
Process Name	Name of the process.
Owner	The owner of the process.
Status	Status of the process as either **Up** or **Down**.
Uptime	Total time that the process has been up.
CPU Util	Measure of the CPU that the process is using
Memory Util	Measure of the Memory that the process is using
Resident Memory	The amount of memory the process is allocated
Disk Read Rate	The disk read rate speed (KBps)
Disk Write Rate	The disk write rate speed (KBps)

FortiSIEM Back-End Processes

Process	Function	Used by Supervisor	Used by Worker	Used by Collector
phAgentManager	Execute event pulling job	X	X	X
phCheckpoint	Execute checkpoint monitoring	X	X	X
phDiscover	Pulling basic data from target	X		X
phEventForwarder	Responsible for forwarding events and incidents from FortiSIEM to external systems	X	X	X
phEventPackage	Uploading event/SVN file to Supervisor/Worker			X
phMonitorAgent	Monitoring other processes	X	X	X

Process	Function	Used by Supervisor	Used by Worker	Used by Collector
phParser	Parsing event to shared store (SS)	X	X	X
phPerfMonitor	Execute performance job	X	X	X
rsyslogd	Responsible for forwarding locally generated logs to FortiSIEM	X	X	X

Properties Associated with Tunnels

Collector Property	Description
Host IP	The Host IP address of the tunnel.
Super Port	The supervisor port.
Protocol	The protocol used by the tunnel.
Protocol Port	The port used by the protocol.
Collector	The collector with the open tunnel.
PID	The Process ID.
Opened Time	The amount of time the tunnel is open.

Open Tunnel Re-Configuration Required after 6.3.0 or later Upgrade/Fresh Install

After upgrading or doing a fresh install of 6.3.0 and later, the feature - "Connect to" a CMDB device via 'Open Tunnel' will no longer work without a configuration change. When users connect via a tunnel, it will appear that the tunnel is opened. However, the displayed Supervisor's port on which the tunneled connection is running is actually not open so users will not be able to connect either via plugin or directly.

To re-enable this feature, take the following steps:

Edit `sshd_config.tunneluser` on the Supervisor by changing the entry `AllowTcpForwarding` to `yes`.

```
AllowTcpForwarding yes
```

Reload the tunnel sshd configuration using the following command:

```
kill -HUP $(pgrep -f sshd_config.tunneluser)
```

If you have tunnels you had opened after the upgrade, but prior to making the above change, you will need to click on the **Close All** button from **ADMIN > Health > Collector Health > Tunnels** page.

This fix was done to address bug 602294: CVE-2004-1653 SSH port forwarding exposes unprotected internal services.

Viewing Agent Health

If your FortiSIEM deployment includes agents, you can monitor the status of your Windows and Linux agents in the **ADMIN** > **Health** > **Agent Health** page. You can also install and upgrade your Windows and Linux agents here.

The **Search...** field allows you to filter agents by name.

The **Action** menu provides the operations you can perform on an Agent:

- **Download Image** - to download a Windows Agent or Linux Agent image.
- **Install Image** - to install a Windows Agent or Linux Agent image.

The **Columns** drop-down list allows you select what agent properties you want to appear in the table.

You can filter agents by organization that appear in the table by using the drop-down list next to the **Columns** drop-down list.

The refresh drop-down list allows you to refresh the status with any of the following options: Refresh Now, 15 seconds, 30 seconds, 1 minute, 2 minutes, 3 minutes.

Properties Associated with Agent Health

Agent Property	Description
Name	The name of the agent device is displayed. Clicking on the name will take you to the **CMDB > Devices** page for that device, where you can edit the device's configuration or view other information.
IP Address	The IP address of the agent is displayed.
Device Type	The operating system running the agent is displayed.
Agent Type	The agent server type is listed.
Agent Version	The version that the agent is running on is displayed.
Agent Status	The agent's current status is displayed.
Event Status	The event status reported by the agent is displayed.
Monitor Status	The monitor status is displayed. This is for performance monitoring.

Agent Property	Description
Agent Policy	The name of the policy configured for the agent is displayed.
Status	The status of an agent's last action is displayed.
Discovered	The date when an agent was discovered is displayed.
Agent ID	The ID of the agent is displayed.
Upgrade Status	The status of the upgrade is displayed.

Event Receive Status

Displays device receiving event status metric information.

Monitor Status

Monitor Status displays metric information based on your server and protocol configuration. See **What is Discovered and Monitored** for your specific server in the External Systems Configuration Guide for more information.
Note: This table does not appear if there is no monitoring configuration.

Viewing Elasticsearch Health

The Elasticsearch Health page displays two frames of information.

Complete these steps to view Elasticsearch health details:

1. Go to **ADMIN** > **Health** > **Elasticsearch Health** tab.
2. Click **Columns** tab under both frames to select the required information to display.

Frame 1 Column Name	Description
Cluster	The name of the Elasticsearch cluster.
IP Address	The IP address of the Elasticsearch cluster.
Status	The current status of the Elasticsearch cluster.
Nodes	The number of nodes in the Elasticsearch cluster.
Data Nodes	The number of data nodes.
Shards	The number of shards in Elasticsearch cluster.
Active Shards	The number of active shards in Elasticsearch cluster.
Configured Nodes	The number of configured nodes.

Frame 1 Column Name	Description
Indices	The number of indices in the Elasticsearch cluster.

Frame 2 Column Name	Description
Name	The name of the node.
IP Address	The IP address of the node.
Role	The node's roles are listed.
Status	The current status.
Version	The version of Elasticsearch running on the node.
Uptime	The period of time the node has been operational.
Load	The load setting for the node.
OS	The OS being used.
Total Memory	The total memory of the node.
Used Memory	The used amount of memory of the node.
Used Swap	The used swap space.
FS Total	The total file system space.
Available	The amount of available space for the node.

Viewing Replication Health

Disaster Recovery involves replicating CMDB (in PostgreSQL database), Configuration (in SVN-lite), Profiles (in SQLite database) and Event data (in FortiSIEM EventDB or Elasticsearch) from Primary to Secondary. This page shows the replication health in terms of delay in synching these databases from Primary to Secondary.

Note: This page is not continuously updated. To manually refresh, click the refresh button on the top right.

Complete these steps to view Replication health details:

1. Go to **ADMIN** > **Health** > **Replication Health** tab.

CMDB Replication	Description
Status	The status can be Critical, Warning, or Normal. **Critical**: If replication paused or delay greater than 30 minutes **Warning**: Delay between 15 minutes and 30 minutes

CMDB Replication	Description
	Normal: Delay less than 15 minutes
Last Synched	The time when PostgreSQL database was last synched.
Delay	Displays how many bytes remained to be synched and the amount of time needed to synch.

Configuration Replication	Description
Status	The status is based on the progress calculated as the ratio of Secondary Bytes and Primary Bytes. **Critical**: Progress less than 10% **Warning**: Progress between 10% and 75% **Normal**: Progress greater than 75%
Last Synched	The time when SVN-lite was last synched.
Delay	Displays how many bytes remained to be synched .

Profile Replication	Description
Status	The status is based on the progress calculated as the ratio of Secondary Bytes and Primary Bytes. **Critical**: Progress less than 10% **Warning**: Progress between 10% and 75% **Normal**: Progress greater than 75%
Last Synched	The time when SQlite was last synched.
Delay	Displays how many bytes remained to be synched .

EventDB Replication	Description
Status	The status is based on the progress calculated as the ratio of Secondary Bytes and Primary Bytes. **Critical**: Progress less than 10% **Warning**: Progress between 10% and 75% **Normal**: Progress greater than 75%

EventDB Replication	Description
Last Synched	The time when FortiSIEM EventDB was last synched.
Delay	Displays how many bytes remained to be synched .

Elasticsearch Replication	Description
Status	The status is based on the progress calculated as the ratio of Secondary Bytes and Primary Bytes. **Critical**: Progress less than 10% **Warning**: Progress between 10% and 75% **Normal**: Progress greater than 75%
Last Synched	The time when Elasticsearch indices were last synched.
Delay	Displays how many bytes remained to be synched .

License

The following sections provide procedures to view License information:

Viewing License Information

The License displays information associated with your current FortiSIEM license under **ADMIN** > **License** > **General** tab.

The Top Heading shows you the following:

- Serial Number
- Hardware ID
- License Type
- FIPS Mode

The table displays the value and expiry date for each of the following attributes.

- Devices
- Endpoint Devices
- Additional EPS
- Total EPS
- Agents
- UEBA
- IOC Service
- Maintenance and Support

You can use the **Upload** button on the top-right to upload a new License. For more information, refer to FortiSIEM Licensing Guide.

Viewing License Usage

The **Usage** tab displays information on your license usage. Select the desired time period from the top-right drop-down to **Last 1 Hour**, **Last 1 Day**, or **Last 1 Week**.

The current License information is displayed under various tabs:

- **Device Usage** - Organization, Licensed, and Used devices
- **Agent Usage** - Organization, Windows Agents, Linux Agents, and total agents used for an organization
- **EPS Usage** - Total Licensed EPS, Used EPS and Unused Events
- **EPS Usage by Node** - EPS Usage based on each Node
- **EPS Usage by Organization** - EPS Usage based on each Organization

To print the monthly usage report, click the **Print Monthly Usage Report** button on the top-right corner.

- About Events Per Second
- EPS Usage By Node
- EPS Usage by Organization
- Used EPS (Global)
- Notes

About Events Per Second

Events per second (EPS) is a key monitoring metric. Since it is tied to licensing, only the following events are included in EPS:

1. External logs – includes logs sent directly to FortiSIEM, logs pulled via FortiSIEM nodes, e.g. AWS CloudTrail, and logs sent by FortiSIEM Windows/Linux agents.
2. Performance monitoring logs (e.g. event type beginning with PH_DEV_MON)

EPS Usage By Node

This metric provides the MAX EPS handled by a FortiSIEM node, over the chosen time period in GUI. The trend line shows the MAX EPS over smaller intervals in the trend graph.

For a Collector node, EPS Usage is the incoming EPS at the Collector. For Supervisor/Worker node, EPS Usage consists of two elements:

1. EPS sent by the Collectors to Supervisor/Worker node
2. EPS from external devices that may be directly sending to that Supervisor/Worker node.

Every 3 minutes, the event PH_SYSTEM_EPS_NODE is generated. The data shown on this page is based on the system report "FortiSIEM Received EPS By Node" that uses this event.

See PH_SYSTEM_EPS_NODE in the Log Reference Guide for a description of the event.

Examples

3 Collectors 25 EPS each, sending to 2 Workers in a load balanced way. Then EPS usage of each Collector is 25. EPS Usage of Worker is 3*25/2 = 37.5. EPS Usage of Supervisor is 0.

3 Collectors 25 EPS each, sending to Supervisor. External devices are sending 10 EPS to Supervisor. Then, EPS usage of each Collector is 25, and EPS Usage of Supervisor is 85.

EPS Usage by Organization

For Enterprise case, there is only one Org - Supervisor/Local. For Service Provider case, there can be many Orgs. Typically, a Collector belongs to one Org. But a Collector belonging to Supervisor/Local Organization may handle many Orgs. EPS Usage by Org is derived by mapping the EPS usage of each Collector to Orgs they belong to.

Every 3 minutes, the event PH_SYSTEM_EPS_ORG is generated. The data shown on this page is based on the system report "FortiSIEM Received EPS By Organization" that uses this event.

See PH_SYSTEM_EPS_ORG in the Log Reference Guide for a description of the event.

Example

3 Collectors receiving 25 EPS each. Each Collector sends to 2 Workers in a load balanced way. 2 Collectors belong to Org1 and 1 Collector belongs to Org2. Then:

- EPS Usage of Org1 is 50
- EPS Usage of Org2 is 25
- EPS Usage of Supervisor/Local is 0.

Used EPS (Global)

This is the total EPS handled by the FortiSIEM cluster.

Every 3 minutes, the event PH_SYSTEM_EPS_GLOBAL is generated. The data shown on this page is based on the system report "FortiSIEM Event Processing Statistics" using this event.

See PH_SYSTEM_EPS_GLOBAL in the Log Reference Guide for a description of the event.

Example

3 Collectors receives 25 EPS each and then sends to 2 Workers in a load balanced way. Each Worker receives 10 EPS each from external devices. In this case, the Used EPS is 95.

Notes

1. Using MAX EPS versus Average EPS: EPS varies over time and has many peaks and valleys. Reasons are varied:
    a. During business hours, EPS is high while it goes down after hours. During the early part of the day, say 8AM - 9AM, EPS tends to be higher than the rest of the day.
    b. If there is a new device that is brought under management and the device generates significant EPS, then it will immediately show a spike.
    c. If events are pulled from AWS S3 bucket, then it may depend on how often it is written to the buckets.

   Because of peaks and valleys, Avg EPS is typically much smaller than MAX EPS. Since a SIEM is designed to not lose events, MAX EPS over smaller intervals is a better way to judge the system usage than Average EPS.
2. Being a distributed system, the EPS is calculated in different nodes in 3 minute intervals, but the intervals at different nodes may not always line up. So, the aggregate numbers may be a little off.

Working with Nodes

A FortiSIEM node is part of an Analytics cluster and can be of four types:

- Supervisor node: this can be of 3 sub-types
    - Primary Leader - this node is instantiated when the system is installed
    - Primary Follower (can be instantiated if High Availability is enabled)
    - Secondary Supervisor (can be instantiated if Disaster Recovery is enabled)
- Worker node

The following features are available from the **License > Nodes** page.

- Viewing a Node
- Adding a Node
- Editing a Node
- Deleting a Node

Viewing a Node

The **Nodes** tab displays information on your existing nodes. You can refresh this page by clicking on the refresh icon. If you are working with nodes for ClickHouse, see the ClickHouse Configuration page for specific ClickHouse information on handling nodes.View, add, edit, or delete nodes from this page.

The Nodes table allows you to view the following information.

Settings	Description
Host Name	The host name of the node.
IP Address	The IP address of the node.
Mode	Displays what the node is working as - Worker or Supervisor.
HA/ DR Role	High Availability (HA) Role shows what role a node is acting as in a Supervisor Cluster. A node will either be **Primary Leader**, or a **Primary Follower** in an Supervisor Cluster configuration. Disaster Recovery (DR) Role shows what role a node is acting as in Disaster Recovery, either **Primary** or **Secondary**.
HA/DR Status	Displays the status of the node. For Disaster Recovery, **Active** indicates that the Primary and Secondary nodes are in sync and that Disaster Recovery is working. If the status is **Inactive** in either the Primary or Secondary nodes involved with Disaster Recovery, it means that the Primary and Secondary are NOT in sync, and that Disaster Recovery is not working. For a Supervisor node not in Disaster Recovery or a Worker node, the Replication Status appears as **N/A**.
Leader	Displays who the leader node is for the follower node in a High Availability Supervisor Cluster configuration.
Licensed	Displays the current license status of the node.

Adding a Node

When the system is installed, a Primary Leader node is instantiated.

- Adding a Worker Node
- Adding a Primary Follower Node (with High Availability Node)
- Adding a Secondary Supervisor Node (with Disaster Recovery Enabled)

Adding a Worker Node

Complete these steps to add a Worker:

1. Go to **ADMIN** > **License** > **Nodes** tab.
2. Click **Add**.
3. From the **Type** drop-down list, select **Worker**.
4. In the **Worker IP Address** field, enter the Worker IP Address.
5. If your storage solution is ClickHouse, the following options are available:
    a. From the **Storage Tiers** drop-down list, select the number of storage tiers.
    b. In Hot Tier, under **Disk Path**, enter the mount point.
    c. In Warm Tier, under **Disk Path**, if multiple storage tiers is selected, under Disk Path, enter the mount point.
    d. Click **+** to add another Hot Tier or Warm Tier field.
    e. Click **Test** to verify the mount point(s).
    f. Click **Save** when done.
6. Click **OK**.

Note: If you are doing Real time Archive to HDFS, then remember to go to **ADMIN > Setup > Storage > Archive** and click **Test** and **Save**. This will prepare the newly added worker for real time archive.

Adding a Primary Follower Node (with High Availability Node)

See Adding Primary Follower in Configuring and Maintaining Active-Active Supervisor Cluster.

Adding a Secondary Supervisor Node (with Disaster Recovery Enabled)

See Set Up Disaster Recovery and Failover in Disaster Recovery.

Editing a Node

- Editing a Worker Node
- Editing the Primary Leader Node
- Editing a Primary Follower Node
- Editing Secondary Supervisor (with Disaster Recovery Enabled)

Editing a Worker Node

Complete these steps to edit a Worker:

1. Go to **ADMIN** > **License** > **Nodes** tab.
2. Select a Worker.
3. Click **Edit**.

4. Make any changes needed.
5. If your storage solution is ClickHouse, the following options are available:
   Click **+** to add another Hot Tier or Warm Tier field.
   Click **-** to remove a Hot Tier or Warm Tier field.
   a. From the **Storage Tiers** drop-down list, select the number of storage tiers.
   b. In Hot Tier, under **Disk Path**, enter the mount point.
   c. In Warm Tier, under **Disk Path**, if multiple storage tiers is selected, under Disk Path, enter the mount point.
   d. Click **Test** to verify the mount point(s).
   e. Click **Save** when done.
6. Click **OK**.

Editing the Primary Leader Node

Complete these steps to edit your Primary Leader.

1. Go to **ADMIN** > **License** > **Nodes** tab.
2. Select the Primary Leader.
3. Click **Edit**.
4. Make any necessary changes needed to the available fields.
5. Click **Save**.

Editing a Primary Follower Node

1. Go to **ADMIN > License > Nodes** tab.
2. Select the Primary Follower.
3. Click **Edit**.
4. Make any necessary changes needed to the available fields.
5. Click **Save**.

Editing Secondary Supervisor (with Disaster Recovery Enabled)

Complete these steps to edit your Disaster Recovery Setup:

1. Go to **ADMIN** > **License** > **Nodes** tab.
2. Select the Secondary.
3. Click **Edit**.
4. Make any changes needed to the Disaster Recovery Setup. See Configuring Disaster Recovery for more information.
5. Click **OK**.

Deleting a Node

- Deleting Worker Node
- Deleting Primary Follower Node

Deleting Worker Node

Complete these steps to delete a Worker:

1. Go to **ADMIN** > **License** > **Nodes** tab.
2. Select a Worker.
3. Click **Delete**.
4. Click **OK**.

Deleting Primary Follower Node

1. Go to **ADMIN** > **License** > **Nodes** tab.
2. Select the Primary Follower.
3. Click **Delete**.
4. Ensure the Supervisor node is shut down.
5. Click **Yes** to confirm the deletion.

Configuring and Maintaining Active-Active Supervisor Cluster

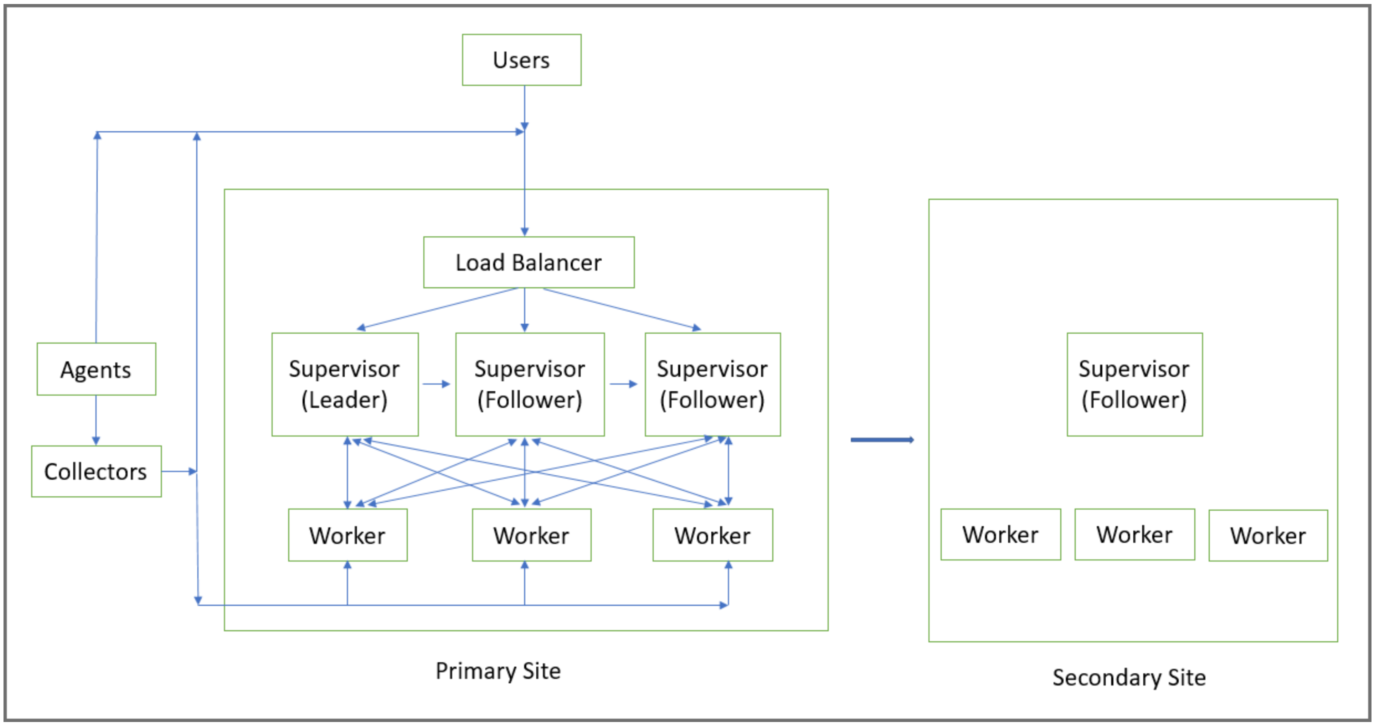
You can setup multiple Supervisors in Active-Active mode with an external Load Balancer in front. This enables you to log in to any Supervisor node and perform any GUI operation. Supervisor node functionalities are distributed across the available Supervisor nodes. An Active-Active Supervisor Cluster provides resilience against Supervisor failures, allows higher number of GUI users, Agents, Collectors, and higher volume of rule and query processing.

This document covers the following topics:

- Operational Overview
- Configuration
  - Adding Primary Leader
  - Adding Primary Follower
  - Load Balancer Setup
  - Collecting UUID and SSH Public Key
  - External Load Balancer Configuration
- Maintenance
  - Failover Operations
  - Adding a Failed Supervisor back to Cluster
  - Checking Cluster Replication Health
  - Maintenance Operations
  - Upgrade

Operational Overview

An Active-Active Supervisor cluster is built around the concept of Leader and Follower Supervisor nodes, set up as a linked list.



1. The first Supervisor where you install License, is the Leader. The Leader's UUID matches the UUID in the installed FortiCare License. On the Leader, Redis and PostGreSQL database services run in Master mode. That means that all PostGreSQL database writes from all Supervisors go to the Leader node.
2. Next, you add a Primary Follower, which follows the Leader, in the sense that its PostGreSQL database is replicated from that of the Leader. On the Follower node, both Redis and PostGreSQL database services run in Follower (that is, read only) mode.
3. You can add another Primary Follower and it will follow the Supervisor node added in Step 2. Its PostGreSQL database is replicated from the Supervisor created in Step 2. On this node, both Redis and PostGreSQL database services run in Follower (that is, read only) mode. A replication chain is formed: Leader -> Follower in Step 2 -> Follower in Step 3.
4. You can add more Primary Follower nodes by successfully chaining from the last Follower node in the chain (in this case, the Follower node created in Step 3).

It is recommended that you put a Load Balancer in front of the Active-Active Supervisor cluster and define the Load Balancer in FortiSIEM GUI (**ADMIN > Settings > Cluster Config > Supervisors**). Then Collectors, Agents and GUI users can reach any of the Supervisors through the Load Balancer. Make sure that the Load Balancer address or host name is reachable from the Collectors, Agents and GUI users.

If you decide to not use a Load Balancer, you can list the Supervisors individually in **ADMIN > Settings > Cluster Config > Supervisors**. Make sure that the Supervisor addresses or host names are reachable from the Collectors, Agents and GUI users. A GUI user can log in to any Supervisor and use FortiSIEM.

Note that Workers to Supervisors communication is maintained internally – Workers are aware of the Supervisors and their Leader/Follower role and communicate to the appropriate node in a load balanced manner.

If the Leader Supervisor fails, then you need to login to the Follower Supervisor in the chain and promote that node to be the Leader by following the instructions in Failover Operations.

The Disaster Recovery feature works with Active-Active Supervisor Cluster. You can login to any Active-Active Supervisor and define the Supervisor for Disaster Recovery. The Primary Leader will replicate the PostGreSQL database, Profile database and SVN-lite files to the Secondary.

FortiSIEM Manager feature also works with Active-Active Supervisor Cluster. You can login to any Active-Active Supervisor and define the FortiSIEM Manager.

To upgrade an Active-Active Supervisor cluster, upgrade the Leader first and then the Followers. See the Upgrade Guide for more information.

Configuration

The following topics are available for configuration.

- Adding Primary Leader
- Adding Primary Follower
- Load Balancer Setup
- Collecting UUID and SSH Public Key
- External Load Balancer Configuration

Adding Primary Leader

Installation

Follow the appropriate Installation Guide, available at the FortiSIEM Doc Library here. During the installation process, select **1 Supervisor** at the **Config Target** window and complete the Installation.

Configuration

When the license is installed, the FortiSIEM unit will be recognized as the Leader. No special configuration is required. For steps on acquiring the UUID, see Collecting UUID and SSH Public Key.

Adding Primary Follower

Installation

Note that you need a High Availability License to add a Follower.

Follow the appropriate Installation Guide, available at the FortiSIEM Doc Library here. During the installation process, select **5 Supervisor Follower** at the **Config Target** window and complete the installation.

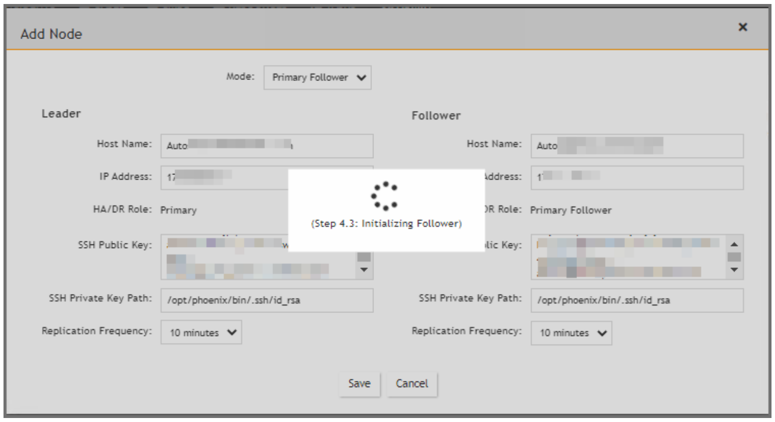
Configuration

Note that the Primary Follower node will be added to the end of linked list of currently configured Supervisors. For example, if you currently have only one Supervisor node, then the new Follower node will follow the currently installed Supervisor (which is the Leader). If you currently have one Supervisor and one Follower node, e.g. Leader -> Follower1, then the new Follower node will follow the last Follower node, e.g. Leader -> Follower1 -> Follower2.

When you add a Follower node via the GUI, FortiSIEM will automatically detect the last Follower node and configure the new node to follow the last Follower node, which can be considered its Leader. The new Follower node needs to get the Profile database and SVN-Lite configuration from the Leader via rsync (using SSH keys). Before you begin to add the Follower node, please obtain its UUID and SSH public key using the information described. See Collecting UUID and SSH Public Key for the steps to acquire this.

To add a Follower node, take the following steps.

1. Login to GUI and navigate to **ADMIN > License > Nodes**.
2. On the **Add Node** window, in the **Mode** drop-down list, select **Primary Follower**. FortiSIEM will automatically detect the Leader for this new node. The Leader node configuration fields appear in the left column, and the Follower node configuration fields appear in the right column.
3. Under the **Follower** column, enter the following information.
   a. In the **Host Name** field, enter the host name of the Follower node.
   b. In the **IP Address** field, enter the IP of the Follower node.
   c. In the **SSH Public Key** field, enter/paste the SSH Public Key of the Follower node that you obtained earlier.
4. For the **SSH Private Key Path**, enter the following into the field:
   `/opt/phoenix/bin/.ssh/id_rsa`
5. For **Replication Frequency**, select a value indicating how frequently Profile database and SVN-lite files will be rsynced by the Follower node. The default 10 minutes is adequate for most operations.
6. Click **Save**.
   At this point, the Primary Follower is being linked to the Primary Leader. The progress will be displayed in the GUI.



Add Node

Mode: Primary Follower

Leader

Host Name: Auto[redacted]

IP Address: 17[redacted]

HA/DR Role: Primary

SSH Public Key: [redacted]

SSH Private Key Path: /opt/phoenix/bin/.ssh/id_rsa

Replication Frequency: 10 minutes

Follower

Host Name: Auto[redacted]

IP Address: 1[redacted]

HA/DR Role: Primary Follower

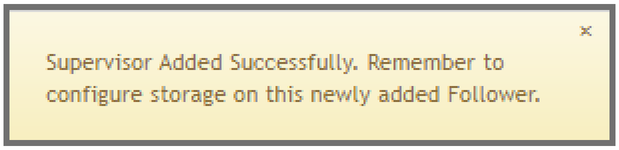
SSH Public Key: [redacted]

SSH Private Key Path: /opt/phoenix/bin/.ssh/id_rsa

Replication Frequency: 10 minutes

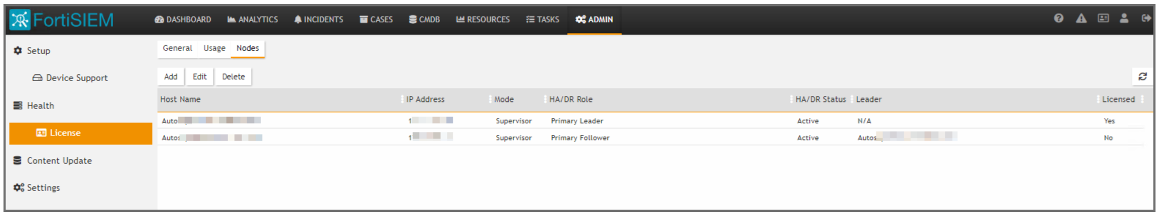
(Step 4.3: Initializing Follower)

When completed, the message "Supervisor Added Successfully" will appear.



Supervisor Added Successfully. Remember to configure storage on this newly added Follower.

The Follower node will be added in the **ADMIN > License > Nodes** page.



Host Name	IP Address	Mode	HA/DR Role	HA/DR Status	Leader	Licensed
Auto[redacted]	1[redacted]	Supervisor	Primary Leader	Active	N/A	Yes
Auto[redacted]	1[redacted]	Supervisor	Primary Follower	Active	Autos[redacted]	No

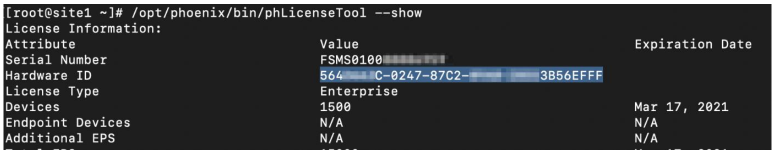
7. If you are running ClickHouse or a Local disk setup, then you need to set up Local disk for the Primary Follower. In these cases, the Primary Follower local disk setup should be identical to that of the Primary Leader. Take the following steps:
   a. Login to GUI and navigate to **ADMIN > Setup > Storage**.
   b. Click **Online** and add a Local disk.
   c. Click **Test**, then **Deploy**.
8. If you have NFS Archive setup, then you need to set up NFS Archive on the Primary Follower. The setup should be identical to that of the Primary Leader. Take the following steps:
   a. Login to GUI and navigate to **ADMIN > Setup > Storage**.
   b. Click **Archive**, choose **NFS** and add the mount point.
   c. Click **Test**, then **Deploy**.
9. If you are running real-time Archive with HDFS, and have added Workers after the real-time Archive has been configured, then you will need to perform a **Test** and **Deploy** for HDFS Archive again from the GUI. This will enable `HDFSMgr` to know about the newly added Workers.
   If you have set up real-time to HDFS, then you need to take the following steps to let HDFSMgr know about the Primary Follower.
   a. Login to GUI.
   b. Navigate to **ADMIN > Setup > Storage**.
   c. Click **Archive**, and choose **HDFS**.
   d. Click **Test**, then **Deploy**.

Load Balancer Setup

1. First set up an external Load Balancer in front of the Active-Active Supervisors. See External Load Balancer Configuration for a sample FortiWeb Load Balancer configuration.
2. Login to GUI and navigate to **ADMIN > Settings > Cluster Config > Supervisors** and add Load Balancer Host Name or IP.

Collecting UUID and SSH Public Key

1. For the UUID, obtain the Hardware ID value through an SSH session by running the following command on FortiSIEM.
   `/opt/phoenix/bin/phLicenseTool --show`
   For example:



```
[root@site1 ~]# /opt/phoenix/bin/phLicenseTool --show
License Information:
Attribute                          Value                                   Expiration Date
Serial Number                      FSMS0100[redacted]
Hardware ID                        564[redacted]C-0247-87C2-[redacted]3B56EFFF
License Type                       Enterprise
Devices                            1500                                    Mar 17, 2021
Endpoint Devices                   N/A                                     N/A
Additional EPS                     N/A                                     N/A
```

2. Enter/paste the Hardward ID into the UUID field for FortiSIEM.
3. Under Configuration and Profile Replication, generate the SSH Public Key and SSH Private Key Path by entering the following in your SSH session from FortiSIEM:
   ```
   su - admin
   ssh-keygen -t rsa -b 4096
   ```
   Leave the file location as default, and press enter at the passphrase prompt.
   The output will appear similar to the following:

```
Generating public/private rsa key pair.
Enter file in which to save the key (/opt/phoenix/bin/.ssh/id_rsa):
Created directory '/opt/phoenix/bin/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /opt/phoenix/bin/.ssh/id_rsa.
Your public key has been saved in /opt/phoenix/bin/.ssh/id_rsa.pub.
The key fingerprint is:
a9:43:88:d1:ed:b0:99:b5:bb:e7:6d:55:44:dd:3e:48 admin@site1.fsmtesting.com
The key's randomart image is:
+--[ RSA 4096]----+
|      ....|
|      . .    E. o|
```

4. For the SSH Public Key, enter the following command, and copy all of the output.
   `cat /opt/phoenix/bin/.ssh/id_rsa.pub`
5. Exit the admin user in the SSH session by entering the following command.
   `exit`

External Load Balancer Configuration

This section provides guidance on how to configure FortiWEB load balancer to work with FortiSIEM Active-Active Supervisor cluster. Most load balancers can also be used. For additional information on FortiWEB configuration, see the FortiWeb documentation library. The example configuration here assumes FortiWeb will have at a minimum, two interfaces.

Port1: External network / subnet - This is where collector / user traffic connects to.

Port2: Internal network / subnet - This is where appServers and Workers reside.

In this example, VMware interfaces map to FortiWeb virtual interfaces when you deploy OVF

Virtual interface 1 is port1 in FortiWeb - 172.30.57.88/22 .1 GW

Virtual interface 2 is port2 in FortiWeb - 10.65.148.3/22

The default route: 172.30.56.1

The general configuration step are:

- Define Virtual IPs
- Define Virtual Server
- Define Supervisor Health Check
- Define Server Pool
- Define Server Policy
- Define Static Routes in FortiWeb

Define Virtual IPs

1. Navigate to **Network > Virtual IP**.
   This is the Load Balancer IPs.

2. Define one unique free IP in the external subnet for AppServer Load Balancer and Worker Load Balancer
3. Click **Create New**.
4. In the **Name** field, enter a name, for example, " AppServerLB".
5. In the **IPV4 Address** field, enter your IP address. In our example, "172.30.57.89/32".
6. In the **Interface** field, enter/select your port. In our example,"port1".
7. Repeat steps 1 through 7 here in Define Virtual IPs for the Worker Load Balancer, then proceed to Define Virtual Server.

Define Virtual Server

1. Navigate to **Server Objects > Server > Virtual Server**.
2. Click **Create New**.
3. In the **Name** field, enter a name for the virtual server, for example, "AppServer_VS".
4. Click **OK**.
5. Under this setup, click **Create New**.
6. Select the Virtual IP that was created earlier.
7. Click **OK**.
8. In **Status** select **Enable**.
9. Leave other options default, and click **OK**.

Define Supervisor Health Check

1. Navigate to **Server Objects > Server > Health Check**.
2. Click **Create New**.
3. In the **Name** field, enter a name for the Health Check trigger, for example, "AppServerHealthCheck".
4. For **Relationship**, select **And**.
5. Click **OK**.
6. In **Rule List**, click **Create New**.
7. For **Type**, select **TCP SSL** and leave the options as default.
8. Click **OK**.
9. In **Rule List**, click **Create New** again.
10. For **Type**, select **HTTP**.
11. In the **URL Path** field, enter "/phoenix/login.html"
12. For **Method** , select **GET**.
13. For **Match Type**, select **Response Code**.
14. For **Response Code**, enter "200".
15. Click **OK** on each page.

Define Server Pool

1. Navigate to **Server Objects > Server > Server Pool**.
2. Click **Create New**.
3. In the **Name** field, enter a name for the server pool, for example, "AppServerPool".
4. For **Proto** , select **HTTP**.
5. For **Type**, select Reverse Proxy.

6. For **Single Server / Server Balance**, select **Server Balance**.
7. For **Server Health Check**, from the drop-down list, select the server health check you created in Define Supervisor Health Check.
8. For **Load Balancing Algorithm**, from the drop-down list, select **Least Connection** or **Round Robin**.
9. Click **OK**.
10. At the bottom of the page, click **Create New**.
11. For each Server in your server pool, in this example AppServer Pool, do the following.
    a. For **Status**, select **Enable**.
    b. For **Server Type**, select **IP**.
    c. For **IP / Domain**, enter the IP address range, for example, "#.#.#.#/32".
    d. For **Port**, enter "443".
    e. For **SSL**, check it, but ignore client certificate.
    f. Click **OK**.

Define Server Policy

1. Navigate to **Policy > Server Policy**.
2. In the **Name** field, enter a name for the server policy, for example, "AppServerPolicy".
3. For **Deployment Mode**, select **Single Server/Server Balance**.
4. For **Virtual Server**, select the virtual server you created in Define Virtual Server.
5. For **Server Pool**, select the server pool you created in Define Server Pool.
6. For **HTTP Service**, select **HTTP**.
7. For **HTTPS Service**, select **HTTPS**.
8. For **Monitor Mode**, enable it.
9. For **Enable Traffic Log**, enable it.
10. Click **OK**.

Define Static Routes in FortiWeb

For FortiWeb to route non HTTP/HTTPS traffic through FortiWeb, create two policy routes.

1. Navigate to **Network > Route**. (See https://docs.fortinet.com/document/fortiweb/7.0.2/administration-guide/55130/configuring-the-network-settings)
2. Select **Policy Route**.
3. Configure the following rules to allow non HTTP/HTTPS traffic inbound.
    a. For **If traffic matches** Incoming Interface, select your port.
    b. For If traffic matches Source address/mask (IPv4/IPv6), enter the IP range.
    c. For If traffic matches Destination address/mask (IPv4/IPv6), enter the IP range.
    d. For **Force traffic to** Action, select **Stop Policy Routing**.
    e. For **Force traffic to** Priority, enter "200".
    f. Click **OK**.
4. Configure the following rules to allow outbound traffic.
    a. For **If traffic matches** Incoming Interface, select your port.
    b. For If traffic matches Source address/mask (IPv4/IPv6), enter the IP range.
    c. For If traffic matches Destination address/mask (IPv4/IPv6), enter the IP range.
    d. For **Force traffic to** Action, select **Stop Policy Routing**.

   e. For **Force traffic to** Priority, enter "100".
   f. Click **OK**.

For each "AppServerIP" defined in the server pool, a FortiSIEM leader/follower cluster should use those IPs.

Maintenance

The following maintenance topics are available:

- Failover Operations
- Adding a Failed Supervisor back to Cluster
- Checking Cluster Replication Health
- Planned Shutdown Procedures
- Upgrade

Failover Operations

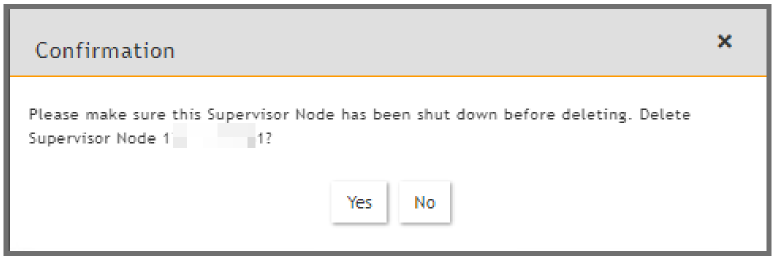
Note that the Supervisors are set up as a linked list: Leader -> Follower1 -> Follower2 -> Follower3…

Case 1: Leader Node Fails

If the Leader node fails, for example, because of a hardware issue, then you need to take the following steps.

Step 1: Promote Follower1 as new Leader by following these steps.

1. SSH to Follower1 and run the following command.
   `phfollower2primary <ownIP>`
   After the script finishes, Follower1 will be the new Leader and the chain becomes: Leader (old Follower1) -> Follower2 -> Follower3
2. Login to GUI. Load Balancer will likely route to any Follower.
3. Navigate to **ADMIN > License > Nodes**.
4. Select the old Leader node and click **Delete**.
5. Click **Yes** to confirm.



Confirmation

Please make sure this Supervisor Node has been shut down before deleting. Delete Supervisor Node 1[redacted]1?

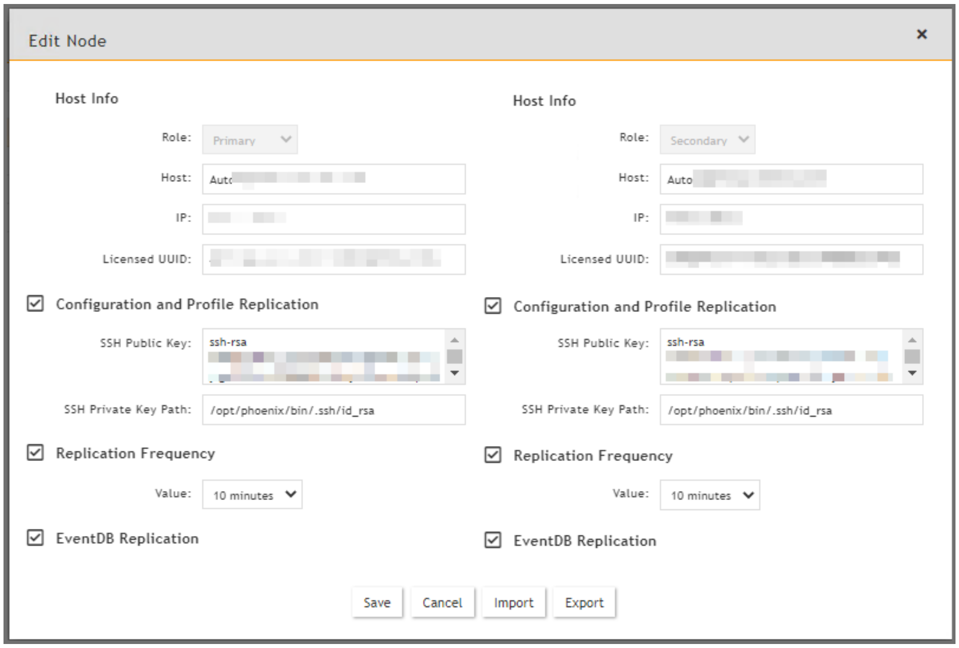
Step 2: If Disaster Recovery is enabled, then change Leader for Secondary node.

1. Login to (new Leader) Follower1 GUI.
2. Navigate to **ADMIN > License > Nodes**.
3. Choose Secondary node, and click **Edit**.
4. Enter the (new Leader) Follower1 information in the Primary column.
   a. Change the **Host Name** field to the Follower1 Host Name.
   b. Change the **IP Address** field to the Follower1 IP Address.

c. DO NOT change the License UUID yet. Do this after you have done a new license with Follower1's UUID in Step 4.4.

d. Set **SSH Parameters** (SSH Public Key, SSH Private Key Path) to that of Follower1.

e. Click **Save**.



Edit Node ×

Host Info

Role: Primary

Host: Auto[redacted]

IP: [redacted]

Licensed UUID: [redacted]

☑ Configuration and Profile Replication

SSH Public Key: ssh-rsa [redacted]

SSH Private Key Path: /opt/phoenix/bin/.ssh/id_rsa

☑ Replication Frequency

Value: 10 minutes

☑ EventDB Replication

Host Info

Role: Secondary

Host: Auto[redacted]

IP: [redacted]

Licensed UUID: [redacted]

☑ Configuration and Profile Replication

SSH Public Key: ssh-rsa [redacted]

SSH Private Key Path: /opt/phoenix/bin/.ssh/id_rsa

☑ Replication Frequency

Value: 10 minutes

☑ EventDB Replication

Step 3: Install a new license with new Leader (Follower1) UUID.

Since the license is tied to failed Leader’s UUID, you will repeatedly see a message prompting you to install a new license with new Leader’s UUID within a 2 weeks grace period from the time of failure. To resolve this, take the following steps.

1. Login to (new Leader) Follower1 GUI. If you go through Load Balancer, then you may end up in Follower2 GUI which does not allow this operation.
2. Navigate to **ADMIN > License > General**.
3. Click **Upload** and provide the license file with matching (new leader) Follower1’s UUID.
   Note: You cannot add new Followers to the system during the 2 weeks grace period when the Primary Leader's UUID does not match the License.

Step 4: If Disaster Recovery is enabled, update Licensed Primary UUID for Secondary node.

1. Login to (new Leader) Follower1 GUI.
2. Navigate to **ADMIN > License > Nodes**.
3. Choose Secondary node and click **Edit**.
4. Update the Licensed UUID for the Primary node.

Case 2: Follower Node Fails

If any follower node fails, take the following steps.

Step 1: Remove the failed Follower node from the Cluster.

1. Login to GUI and navigate to **ADMIN > License > Nodes**.
2. Select the node
3. Click **Delete**.

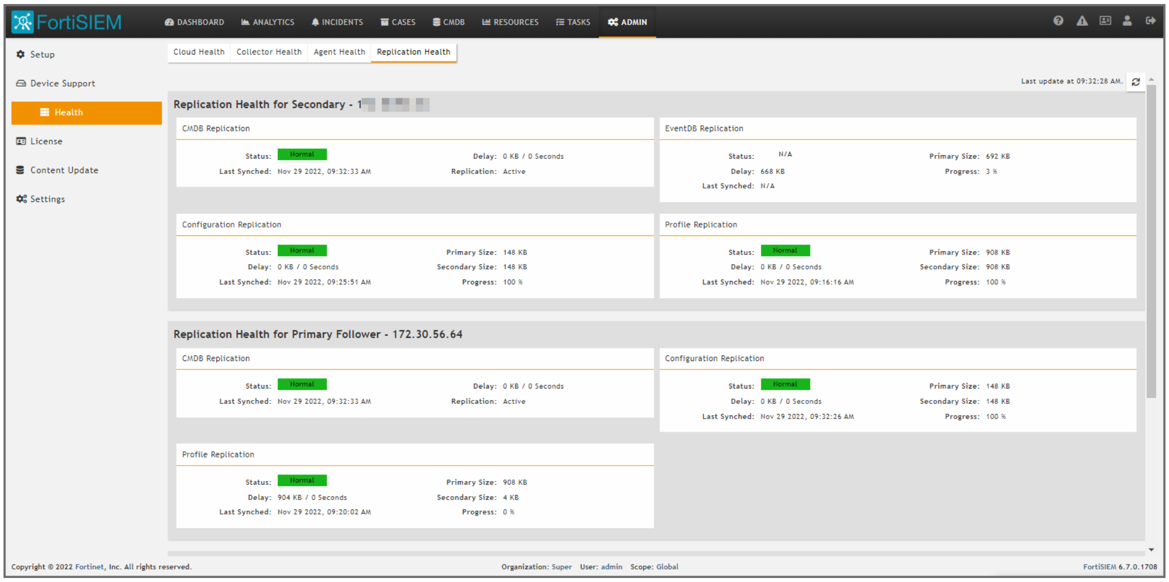
Case 3: Adding a Failed Supervisor back to Cluster

If you want to add a failed Supervisor back to the Cluster, then follow these steps.

1. Navigate to `/opt/phoenix/deployment/jumpbox`.
2. Clean the state data by running the following script, using its own IP.
   `phresetclusternode <myip>`
   Note: After completion, this script will reboot your appliance.
3. Once this appliance is up and running again, if the storage is Local, format the disk if you would like to reuse it, otherwise add a new disk.
4. Add the node as a Follower by following the steps in Adding Primary Follower.

Checking Cluster Replication Health

Cluster Replication health can be viewed in **ADMIN > Health > Replication Health** and **ADMIN > Health > Cloud Health**.



Last update at 09:32:28 AM.

Replication Health for Secondary - 1[redacted]

CMDB Replication
Status: Normal
Last Synched: Nov 29 2022, 09:32:33 AM
Delay: 0 KB / 0 Seconds
Replication: Active

EventDB Replication
Status: N/A
Delay: 668 KB
Last Synched: N/A
Primary Size: 692 KB
Progress: 3 %

Configuration Replication
Status: Normal
Delay: 0 KB / 0 Seconds
Last Synched: Nov 29 2022, 09:25:51 AM
Primary Size: 148 KB
Secondary Size: 148 KB
Progress: 100 %

Profile Replication
Status: Normal
Delay: 0 KB / 0 Seconds
Last Synched: Nov 29 2022, 09:16:16 AM
Primary Size: 908 KB
Secondary Size: 908 KB
Progress: 100 %

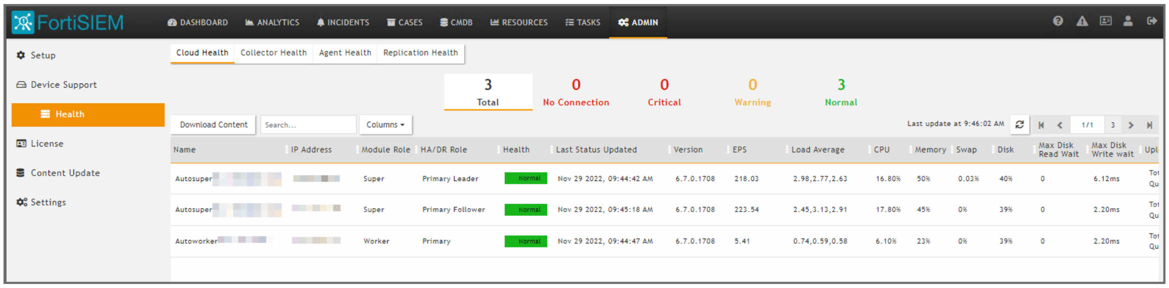
Replication Health for Primary Follower - 172.30.56.64

CMDB Replication
Status: Normal
Last Synched: Nov 29 2022, 09:32:33 AM
Delay: 0 KB / 0 Seconds
Replication: Active

Configuration Replication
Status: Normal
Delay: 0 KB / 0 Seconds
Last Synched: Nov 29 2022, 09:32:26 AM
Primary Size: 148 KB
Secondary Size: 148 KB
Progress: 100 %

Profile Replication
Status: Normal
Delay: 904 KB / 0 Seconds
Last Synched: Nov 29 2022, 09:20:02 AM
Primary Size: 908 KB
Secondary Size: 4 KB
Progress: 0 %

Copyright © 2022 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global FortiSIEM 6.7.0.1708



3 Total | 0 No Connection | 0 Critical | 0 Warning | 3 Normal

Last update at 9:46:02 AM 1/1 3

Name	IP Address	Module Role	HA/DR Role	Health	Last Status Updated	Version	EPS	Load Average	CPU	Memory	Swap	Disk	Max Disk Read Wait	Max Disk Write wait	Upl
Autosuper[redacted]	[redacted]	Super	Primary Leader	Normal	Nov 29 2022, 09:44:42 AM	6.7.0.1708	218.03	2.98,2.77,2.63	16.80%	50%	0.03%	40%	0	6.12ms	Tot Qu
Autosuper[redacted]	[redacted]	Super	Primary Follower	Normal	Nov 29 2022, 09:45:18 AM	6.7.0.1708	223.54	2.45,3.13,2.91	17.80%	45%	0%	39%	0	2.20ms	Tot Qu
Autoworker[redacted]	[redacted]	Worker	Primary	Normal	Nov 29 2022, 09:44:47 AM	6.7.0.1708	5.41	0.74,0.59,0.58	6.10%	23%	0%	39%	0	2.20ms	Tot Qu

Maintenance Operations

Extra care must be taken to restart or shutdown a Leader node, since it contains the Master PostGreSQL database.

Case 1: Restarting Supervisor Leader

This should be avoided as much as possible, since the Leader contains the Master PostGreSQL database. App Server or any other modules on the Leader can be restarted normally.

1. Check Cluster health to make sure that Leader and Follower health are good and replication is up to date.
2. Make sure users are logged out.
3. Shutdown or Reboot the Leader node.
4. After Leader is up (that is, all processes are up), then users can login to the Leader.
5. Log on to each Follower and restart the App Server process on that node. After the App Server process is up on a Follower, users can log on to the Follower node.

Case 2: Restarting Supervisor Follower

This can be done normally. The user can login to any other Supervisor node. While the Follower node is down, the local PostGreSQL database will fall behind. If the Follower node comes back up within a reasonable time period, then PostGreSQL database replication will catch up and the system will become normal.

Case 3: Restarting a Process on any Supervisor

For any process other than DB Server on the Primary Leader, this can be done normally, and the Cluster should be up and users should be able to login. To restart the DB Server on Primary Leader, follow these steps:

1. Check Cluster health to make sure that Leader and Follower health are good and replication is up to date.
2. Make sure users are logged out.
3. Restart the DB Server on the Leader node.
4. After the DB Server on the Leader is up, restart the App Server. After both App Server and DB Server are up, then users can login to the Leader.
5. Log on to each Follower and restart the App Server process on that node. After the App Server process is up on a Follower, users can log on to the Follower node.

Case 4: Restarting Worker

This can be done normally.

Upgrade

Follow the Upgrade 6.x.7/x Cluster Deployment section from the Upgrade Guide here.

Configuring Disaster Recovery

Configuring Disaster Recovery for ClickHouse

For ClickHouse based deployments, see the following topics from the High Availability and Disaster Recovery - ClickHouse Guide:

General Information: High Availability and Disaster Recovery - ClickHouse

Configuration: Configuring Disaster Recovery

Operation: Disaster Recovery Operations

Configuring Disaster Recovery for Elasticsearch

For Elasticsearch based deployments, see the following topics from the High Availability and Disaster Recovery - Elasticsearch Guide:

General Information: High Availability and Disaster Recovery - Elasticsearch

Configuration: Configuring Disaster Recovery

Operation: Disaster Recovery Operations

Configuring Disaster Recovery for EventDB

For EventDB based deployments, see the following topics from the High Availability and Disaster Recovery - EventDB Guide:

General Information: High Availability and Disaster Recovery - EventDB

Configuration: Configuring Disaster Recovery

Operation: Disaster Recovery Operations

Content Update

The **ADMIN** > **Content Update** page displays the FortiSIEM version that is running and can be used to check if there are available updates. If any updates are available, they can be downloaded and installed. Content Updates must be done in the following order:

1. Upgrade FortiSIEM Manager.
2. Upgrade FortiSIEM Supervisor.
3. Upgrade FortiSIEM Worker.

Specific Content Pack Updates information can be found here.

The following topics are available:

- Content Update Notification
- Viewing Content Updates
- Checking for Content Updates
- Viewing Content Update History
- Installing Content Update

Content Update Notification

If a Content Update is available, the following icon will appear in the top header: ☁

Clicking this icon anywhere from the FortiSIEM GUI will redirect the user to the **ADMIN > Content Update** page.

Viewing Content Updates

The current running version is displayed in **Running Version**. Any available versions that can be applied in an update are displayed in **Available Versions**.

The Content Update table provides the following information.

Settings	Description
Version	The version of released content is displayed.
Release Date	The release date of the content is displayed.
Content Description	Information about a content update is provided here.

Checking for Content Updates

To check for any available content updates, click the **Check Now** button. If any content update is available, the **Install** button will be active. If more than one new version is found, then the button name will appear as **Install All**.

Viewing Content Update History

To check your FortiSIEM content update history, take the following steps:

1. Click the **History** button. A **Content Update History** window will appear.
2. Select **Relative** or **Absolute Time**, and input or select the time frame you wish to view.
   Click **OK**.

   The following information is provided, if available.

Settings	Description
Update Time	The time the content update was applied is displayed.
Source IP	The IP address from where the update was downloaded is displayed.
User	The user who performed the update is displayed.
Version	The version of the content update is displayed.

3. When done viewing the information, click **Close**.

Installing Content Update

This section allows you to update content for your Supervisor, Workers and Collectors without needing to update your FortiSIEM version. When the content installation occurs, all new content is pushed to all available nodes (Supervisor, Workers, Collectors).

- Content Update Installation for Supervisor and Workers
- Content Update Installation for Collectors

Content Update Installation for Supervisor and Workers

Install Content Updates for Supervisor and Workers

Note: Any changes that have occurred during an installation CANNOT be reverted.

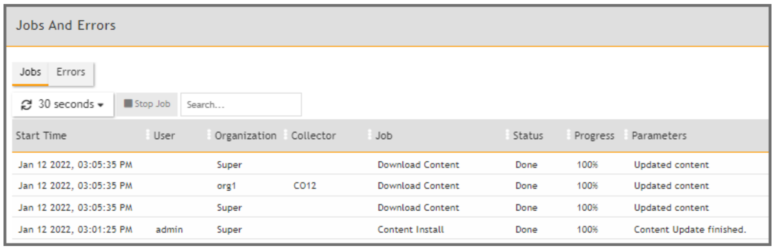
1. Click the **Install** button.

   Note: If more than one update is available an **Install All** button will appear instead. In this situation, click **Install All** to perform all installations.

A progress bar will appear as installation begins. When the progress bar is complete, the installation is done.

You can also click on the Jobs/Errors icon (⚠) and select the **Jobs** tab to view the progress of the content installation. When the **Status** column shows "Done", and **Progress** column is "100%", installation for the Supervisor and Workers is complete.

Example: The Supervisor and Worker content update (The first and third lines) are shown as "Done".



Jobs And Errors

Start Time	User	Organization	Collector	Job	Status	Progress	Parameters
Jan 12 2022, 03:05:35 PM		Super		Download Content	Done	100%	Updated content
Jan 12 2022, 03:05:35 PM		org1	CO12	Download Content	Done	100%	Updated content
Jan 12 2022, 03:05:35 PM		Super		Download Content	Done	100%	Updated content
Jan 12 2022, 03:01:25 PM	admin	Super		Content Install	Done	100%	Content Update finished.

If you register/power on any Collector after the Supervisor has had a Content Update, then proceed to Content Update Installation for Collectors.

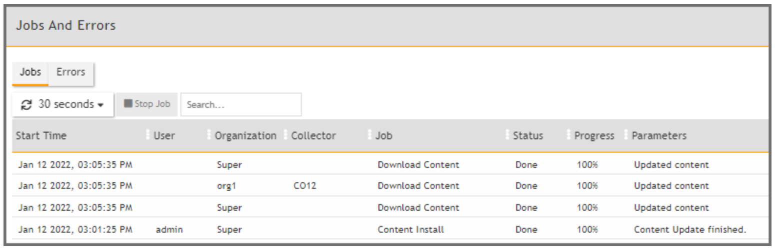
Note: You can click **Abort** to stop the installation.

Content Update Installation for Collectors

Install Content Updates to Collectors

1. Navigate to **ADMIN > Health > Collector Health**.
2. Click on the **Action** drop-down list and select **Download Content**.
   Click on the Jobs/Errors icon (⚠) and select the **Jobs** tab to view the progress of the content installation.

   When the **Status** column shows "Done", and **Progress** column is "100%", for the Collector job, the content update is complete.
   Example: The second line shows the Collector Content Update as "Done" for Collector CO12.



Jobs And Errors

Start Time	User	Organization	Collector	Job	Status	Progress	Parameters
Jan 12 2022, 03:05:35 PM		Super		Download Content	Done	100%	Updated content
Jan 12 2022, 03:05:35 PM		org1	CO12	Download Content	Done	100%	Updated content
Jan 12 2022, 03:05:35 PM		Super		Download Content	Done	100%	Updated content
Jan 12 2022, 03:01:25 PM	admin	Super		Content Install	Done	100%	Content Update finished.

Settings

This section contains information on monitoring the health of your FortiSIEM deployment, general system settings such as language, date format, and system logos, and how to add devices to a maintenance calendar.

- System Settings
  - UI Settings
  - Email Settings
  - Image Server Settings
  - Cluster Config

- General Settings
  - External Authentication Settings
  - Incident Notification Settings
  - External System Integration Settings
  - Case Escalation Settings
  - Configuring SSL Socket Certificates
  - Cloud Machine Learning

System Settings

The following section describes the procedures for system settings:

- UI Settings
- Email Settings
- Image Server Settings
- Cluster Config
- Lookup Settings
- Kafka Settings
- Dashboard Slideshow Settings
- Dashboard Ownership
- PAYG Report
- Trusted Hosts

UI Settings

There are two locations where you can change UI settings in FortiSIEM. One location is in the user profile. The other is in the administrator settings.

- User Profile UI Settings
- Administrator UI Settings

User Profile UI Settings

The initial view of FortiSIEM UI after login can be configured using the UI settings including dashboard, logos, and theme.

Click the **User Profile** icon (🪪) in the upper right corner of the UI. The dialog box contains three tabs:

Basic - Use the **Basic** tab to change your password into the system.

Contact - Use the **Contact** tab to enter your contact information.

UI Settings - Use the **UI Settings** tab to set the following:

Settings	Guidelines
Home	Select the tab which opens when you log in to the FortiSIEM UI.

Settings	Guidelines
Incident Home	Select the Overview, List (by Time, by Device, by Incident), Risk, Explorer, or MITRE ATT&CK ICS or IT (Rule Coverage, Incident Coverage, Incident Explorer) display for the **INCIDENTS** tab.
Dashboard Home	Select the Dashboard to open by default under the **DASHBOARD** tab from this drop-down list.
Dashboard Settings	Select the type of dashboards to be visible/hidden using the left/right arrows. The up/down arrows can be used to sort the Dashboards.
Language	Specify which language will be used for the UI display. Many UI items have been translated into the languages in the drop-down list, including buttons, labels, top-level headings, and breadcrumbs. Items that are data-driven are not translated.
Theme	Select Dark or Light theme for FortiSIEM UI. Save and refresh the browser to view the change.
Date Format	Select one of the following formats for displaying date and time information. • Local/Simple Date Format - Display the time in AM/PM format. • ISO 8601 - Display the date and time in ISO 8601 format, the International Standards Organization's standard for date and time representation. • UTC - Display the date and time in Coordinated Universal Time (UTC).

When done configuring, click **Save**.

Note: All of the above settings will take effect when you log in again or when you refresh the browser in the same login session.

Administrator UI Settings

Click **ADMIN > Settings > System > UI** to access the administrator UI settings.

FortiSIEM only accepts SVG format for logos. All other image formats must be converted to SVG format first.

The image resolution is restricted to 160 x 40.

The following site can be used to help convert PNG/JPG/GIF into SVG: https://onlineconvertfree.com/convert/svg/

Settings	Guidelines
UI Logo	Click the edit icon to enter the path to the image file for the logo that will be used in the

Settings	Guidelines
	UI.
Report Logo	Click the edit icon to enter the path to the image file for the logo that will be used in reports.
Google Maps API Key	Click the edit icon to enter the API key to access Google Maps.
Login Banner	Administrators can choose a login banner to display to users after login. Click the **Enabled** checkbox to display a login banner. In the field below **Login Banner**, enter the text that you want to appear. Some simple BBCode tags are allowed in this message input: “b” - bold “i” - italic “u” - underline “url” - url HTML tags are not allowed. Nested tags are not allowed. When done, click **Save**. In addition to the banner, the user will see the following: • Last login time and IP address location • Changes to the account (if any) since last login. This includes whether the user was assigned a new role for any organization, or if a role definition has changed. Changes appear in the next login. This is a global setting for all users.

Email Settings

The system can be configured to send email as an incident notification action or send scheduled reports. Use these fields to specify outbound email server settings.

Complete these steps to customize email settings:

1. Go to **ADMIN** > **Settings** > **System** > **Email** tab.
2. Enter the following information under **Email Settings**:

Settings	Guidelines
Email Gateway Server	[Required] Holds the gateway server used for email.
Server Port	Port used by the gateway server.
Secure Connection (TLS)	Protocol used by the gateway server. This can be Exchange or SMTP.

Settings	Guidelines
Server Account ID	[Required] The account name for the gateway.
Default Email Sender	Default email address of the sender.
Authentication	Select **Basic** or **OAuth**. If **Basic** is selected, the following field must be configured. • **Account password** - Enter the password for the account. If **OAuth** is selected, the following fields must be configured. • **OAuth Provider** - Select the OAuth Provider from the drop-down list. • **Client ID** - Enter the Client ID for OAuth. • **Client Secret** - Enter the Client Secret associated with the Client ID. After OAuth configuration, click **Re-authenticate** to confirm authentication settings.
Enable S/MIME	Add a check mark to enable Secure/Multipurpose Internet Mail Extensions (S/MIME) to encrypt your emails. To add a S/MIME certificate, go to **CMDB > Users > Ungrouped**, create or edit a user, select **Contact Info**, ensure the **Email** field is filled out, and upload the certificate in the **Certificate** field.
Send Without Key	If this option is selected, then email is sent to a user, even if no S/MIME certificate is defined for that user. The email is encrypted with a default certificate and the user cannot read this email. If this option is unselected, then email is not sent to the user without a S/MIME certificate. Therefore, to use the S/MIME option, **certificates must be defined for all users configured to receive email**.

3. Click **Test Email** button to test the new email settings.
4. Click **Save**.

Customizing the Incident Email Template

Use the following procedure to customize the incident email template.

1. Click **New** under the section **Incident Email Template**.
2. Enter the **Name** of the template.
3. Select the **Organization** from the list.
4. Enter the **Email Subject**. You can also choose the incident attribute variables from **Insert Content** drop-down as part of Email Subject.
5. Enter the **Email Body** by selecting the attribute variables from **Insert Content** drop-down into your template, rather than typing. If required, enable **Support HTML** for HTML content support.

Incident Attribute	Description
Organization	Organization to which this Incident belongs.
Status	Incident Status – Active (0), Auto Cleared (1), Manually Cleared (2), System Cleared (3)
Host Name	Host Name from Incident Target. If not found then gathered from Incident Source
Incident ID	Incident ID – assigned by FortiSIEM and is unique – this attribute has an URL which takes user to this incident after login
Incident ID Without Link	Incident ID – assigned by FortiSIEM and is unique – this attribute does not have an URL
First Seen Time	First time the incident occurred
Last Seen Time	Last time the incident occurred
Incident Category	Security, Performance, Availability or Change
Incident Severity	A number from 0-10
Incident Severity Category	HIGH (9-10), MEDIUM (5-8) and LOW (1-4)
Incident Count	Number of times the same incident has happened with the same group by parameters
Rule Name	Rule Name
Rule Remediation Note	Remediation note defined for each rule
Rule Description	Rule Description
Incident Source	Source IP, Source Name in an Incident
Incident Target	Destination IP, Destination Host Name, Host IP, Host Name, User in an Incident
Incident Detail	Any group by attribute in an Incident other than those in Incident Source and Incident Target
Affected Business Service	Comma separated list of all business services to which Incident Source, Incident Target or Reporting Device belongs

Incident Attribute	Description
Identity	Identity and Location for Incident Source
Notify Policy ID	Notification Policy ID that triggered this email notification
Triggering Attributes	List of attributes that trigger a rule – found in Rule > Sub pattern > Aggregate
Raw Events	Triggering events in raw format as sent by the device (up to 10)
Incident Cleared Reason	Value set by user when clearing a rule
Device Annotation	Annotation for the device in Incident Target – set in CMDB
Device Description	Description for the device in Incident Target – set in CMDB
Device Location	Location for the device in Incident Target – set in CMDB
Incident Subcategory	Specific for each category – as set in the Rule definition
Incident Resolution	None, True Positive, False Positive

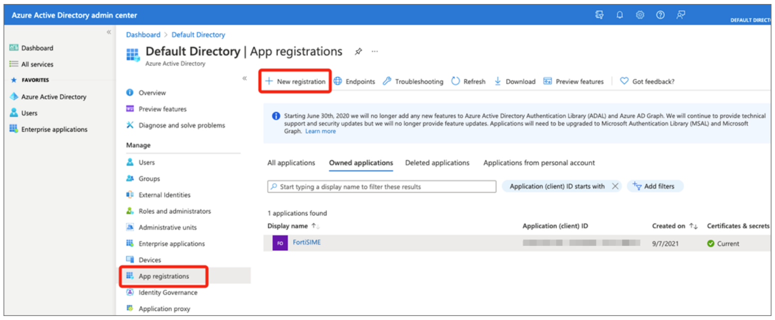
6. Click **Preview** to preview the email template.
7. Click **Save** to apply the changes.

To set an email template as default, select the template in the list, and then click **Set as Default**. When you are creating a notification policy and must select an email template, if you leave the option blank, the default template will be used. For Service Provider deployments, to select a template as default for an Organization, first select the Organization, then set the default email template for that organization.

Example Registering FortiSIEM with Azure via OAUTH

Here is an example of registering FortiSIEM to use Azure email server via OAUTH.

1. Login to Microsoft 365.
2. Go to **App registrations**.
3. Click **+ New registration**.



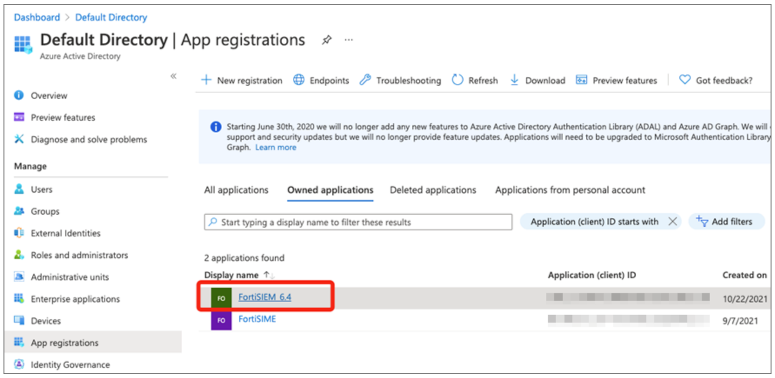
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

1 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
FO FortiSIME	[redacted]	9/7/2021	Current

4. In the **Name** field, enter a name, such as "FortiSIEM", and choose an account type.

5. Under **Owned applications**, select your FortiSIEM application.

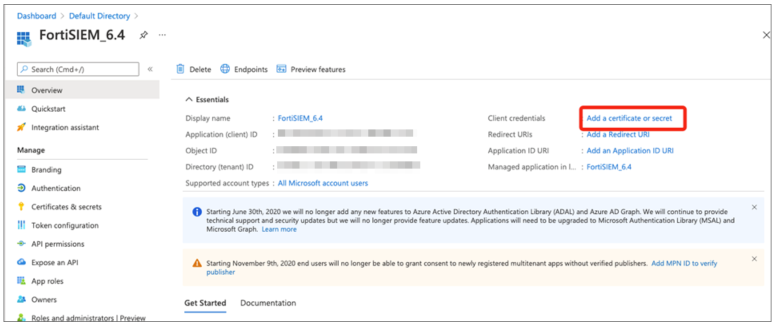


Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library Graph. Learn more

2 applications found

Display name	Application (client) ID	Created on
FO FortiSIEM_6.4	[redacted]	10/22/2021
FO FortiSIME	[redacted]	9/7/2021

6. On the App registration page for your app, make note of the **Application (client) ID** for your FortiSIEM configuration. Then, at **Client credentials**, click **Add a certificate or secret**.



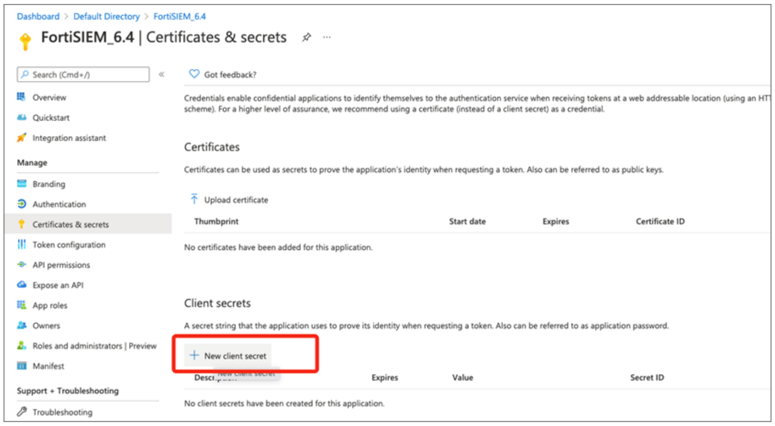
Display name : FortiSIEM_6.4
Application (client) ID : [redacted]
Object ID : [redacted]
Directory (tenant) ID : [redacted]
Supported account types : All Microsoft account users

Client credentials : Add a certificate or secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : FortiSIEM_6.4

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. Add MPN ID to verify publisher

7. Under **Client secrets**, click **+ New client secret**.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTT scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	Certificate ID

No certificates have been added for this application.

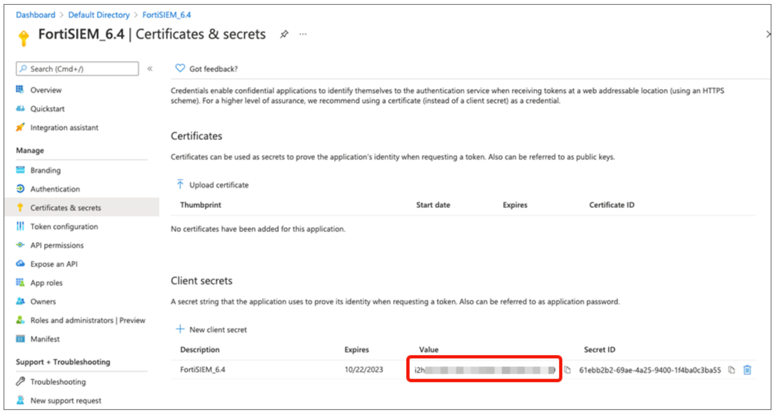
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID

No client secrets have been created for this application.

8. Copy the value from the **Value** column. This is your Client Secret for authentication.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	Certificate ID

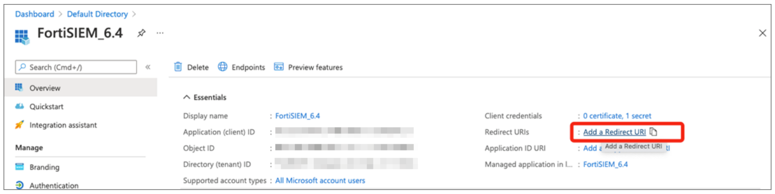
No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

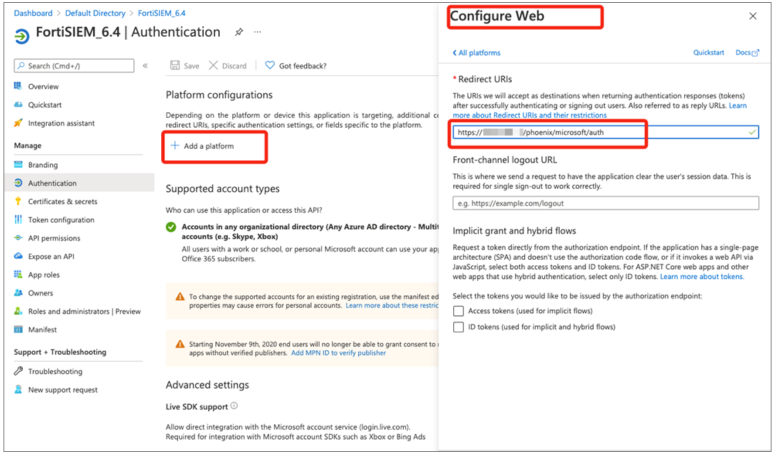
Description	Expires	Value	Secret ID
FortiSIEM_6.4	10/22/2023	i2h[redacted]	61ebb2b2-69ae-4a25-9400-1f4ba0c3ba55

9. At **Redirect URIs**, click **Add a Redirect URI**.



Display name : FortiSIEM_6.4
Application (client) ID : [redacted]
Object ID : [redacted]
Directory (tenant) ID : [redacted]
Supported account types : All Microsoft account users
Client credentials : 0 certificate, 1 secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add a
Managed application in l... : FortiSIEM_6.4

10. Under **Platform configurations**, click **+ Add a platform**.
11. Click **Web**.
12. In the **Redirect URIs** section, enter/paste the URI, which is your FortiSIEM Supervisor IP or host name.



Platform configurations

Depending on the platform or device this application is targeting, additional c redirect URIs, specific authentication settings, or fields specific to the platform.

Supported account types

Who can use this application or access this API?

Accounts in any organizational directory (Any Azure AD directory - Multit accounts (e.g. Skype, Xbox)
All users with a work or school, or personal Microsoft account can use your ap Office 365 subscribers.

To change the supported accounts for an existing registration, use the manifest ed properties may cause errors for personal accounts. Learn more about these restric

Starting November 9th, 2020 end users will no longer be able to grant consent to apps without verified publishers. Add MPN ID to verify publisher

Advanced settings

Live SDK support

Allow direct integration with the Microsoft account service (login.live.com). Required for integration with Microsoft account SDKs such as Xbox or Bing Ads

* Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

https://[redacted]/phoenix/microsoft/auth

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout

Implicit grant and hybrid flows

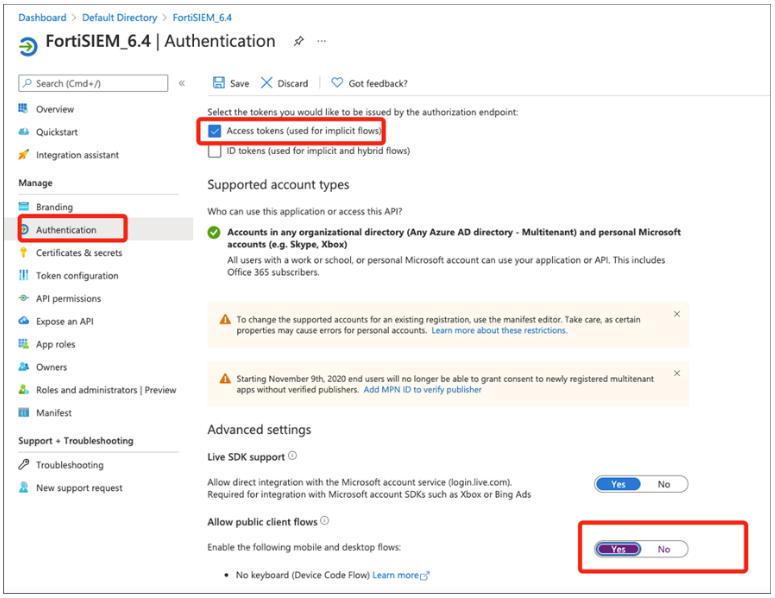
Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.

Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)
☐ ID tokens (used for implicit and hybrid flows)

In the left pane, navigate to **Manage > Authentication**.

13. Configure the two following Authentication settings:
    - **Access tokens (used for implicit flows)** checkbox must be checked.
    - Under **Advanced settings**, **Allow public client flows** must be set to **Yes**.



Select the tokens you would like to be issued by the authorization endpoint:

☑ Access tokens (used for implicit flows)

□ ID tokens (used for implicit and hybrid flows)

Supported account types

Who can use this application or access this API?

✓ **Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)**

All users with a work or school, or personal Microsoft account can use your application or API. This includes Office 365 subscribers.

To change the supported accounts for an existing registration, use the manifest editor. Take care, as certain properties may cause errors for personal accounts. Learn more about these restrictions.

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. Add MPN ID to verify publisher

Advanced settings

Live SDK support

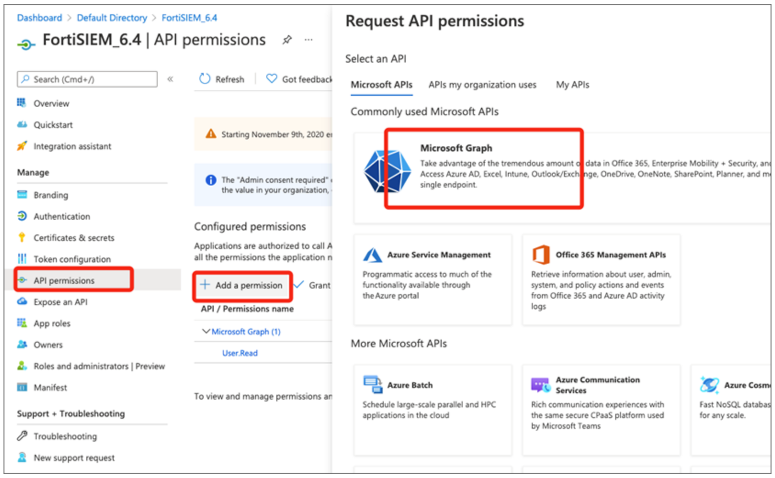
Allow direct integration with the Microsoft account service (login.live.com). Required for integration with Microsoft account SDKs such as Xbox or Bing Ads [✓ Yes] No

Allow public client flows

Enable the following mobile and desktop flows: [✓ Yes] No

- No keyboard (Device Code Flow) Learn more

14. Navigate to **Manage > API permissions**.
15. Under **Configured permissions**, click **+ Add a permission**.
16. From the **Request API permissions** pane, select the **Microsoft APIs** tab, and click **Microsoft Graph**.



Starting November 9th, 2020 e

The "Admin consent required" the value in your organization,

Configured permissions

Applications are authorized to call A all the permissions the application n

To view and manage permissions an

Microsoft Graph
Take advantage of the tremendous amount o data in Office 365, Enterprise Mobility + Security, an Access Azure AD, Excel, Intune, Outlook/Exch nge, OneDrive, OneNote, SharePoint, Planner, and m single endpoint.

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

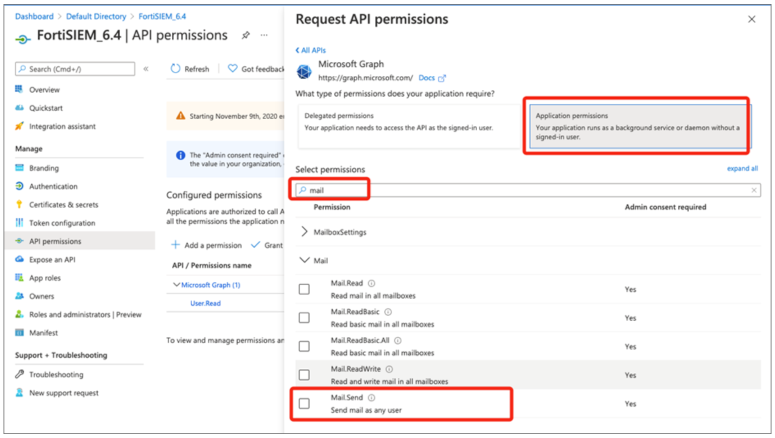
Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

Azure Batch
Schedule large-scale parallel and HPC applications in the cloud

Azure Communication Services
Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

Azure Cosm
Fast NoSQL databas for any scale.

17. Under **What type of permissions does your application require?** select **Application permissions**.
18. In the **Select permissions** search field, enter "mail".
19. From the **Permission** column, expand **Mail**, and configure Mail.Send (Send mail as any user) so **Admin consent required** is set to **Yes**.



Request API permissions

Microsoft Graph
https://graph.microsoft.com/

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

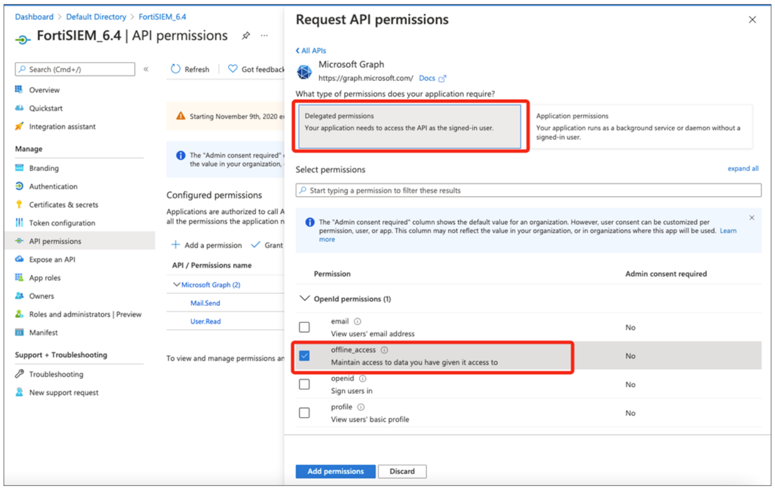
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

mail

Permission	Admin consent required
MailboxSettings	
Mail	
□ Mail.Read Read mail in all mailboxes	Yes
□ Mail.ReadBasic Read basic mail in all mailboxes	Yes
□ Mail.ReadBasic.All Read basic mail in all mailboxes	Yes
□ Mail.ReadWrite Read and write mail in all mailboxes	Yes
□ Mail.Send Send mail as any user	Yes

20. Now, under **Microsoft Graph > What type of permissions does your application require?** select **Delegated permissions**.
21. Under the **Permission** column, expand **OpenId permissions**.
22. Click the **offline_access** checkbox so that **offline_access** is checked.



Request API permissions

Microsoft Graph
https://graph.microsoft.com/

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

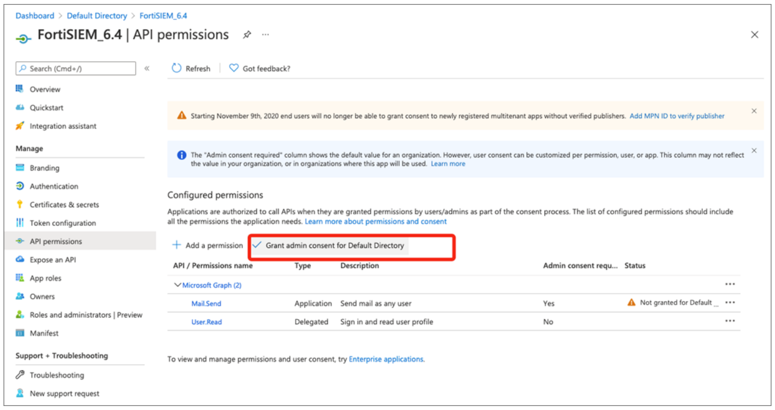
Select permissions

Start typing a permission to filter these results

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Permission	Admin consent required
OpenId permissions (1)	
□ email View users' email address	No
☑ offline_access Maintain access to data you have given it access to	No
□ openid Sign users in	No
□ profile View users' basic profile	No

23. Under **Configured permissions**, click **Grant admin consent for Default Directory**.



Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. Add MPN ID to verify publisher

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

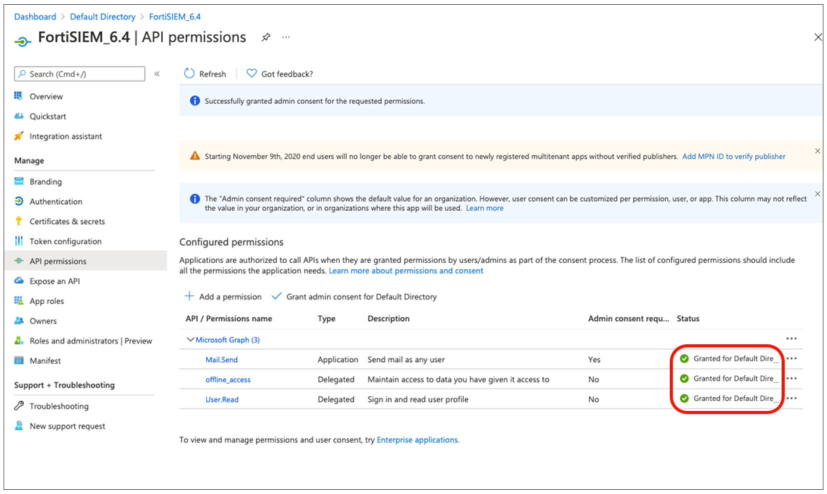
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2)				
Mail.Send	Application	Send mail as any user	Yes	Not granted for Default ...
User.Read	Delegated	Sign in and read user profile	No	

To view and manage permissions and user consent, try Enterprise applications.

Check the **Status** column. The following permissions should be granted.

- Mail.Send
- offline_access
- User.Read



Successfully granted admin consent for the requested permissions.

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. Add MPN ID to verify publisher

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

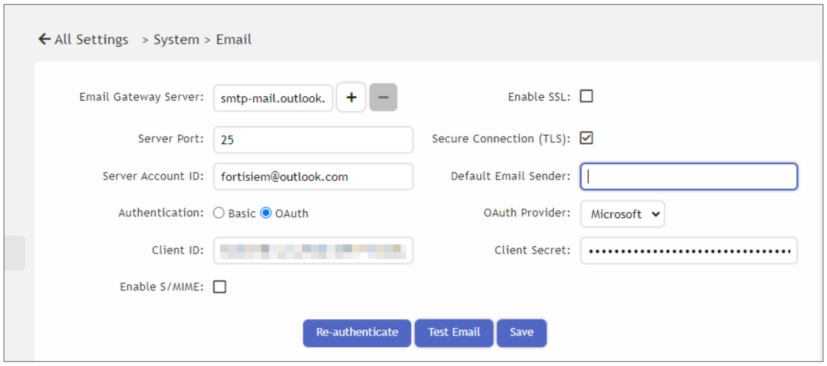
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Mail.Send	Application	Send mail as any user	Yes	Granted for Default Dire...
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Default Dire...
User.Read	Delegated	Sign in and read user profile	No	Granted for Default Dire...

To view and manage permissions and user consent, try Enterprise applications.

On FortiSIEM, take the following steps:

1. Navigate to **Admin > Settings > System > Email**.
2. In the **Email Gateway Server** field, enter the IP address/host name of your email gateway server.
3. In the **Server Port** field, enter the Server Port number.
4. In the **Server Account ID** field, enter the server account ID.
5. For **Authentication**, select **OAuth**.
6. In the **OAuth** drop-down list, select **Microsoft**.
7. In the **Client ID** field, enter/paste the Application (Client) ID of the App from Step 6 in Example Registering FortiSIEM with Azure via OAUTH.
8. In the **Client Secret** field, enter/paste the value from Step 8 in Example Registering FortiSIEM with Azure via OAUTH.
9. Click **Re-authenticate**, **Test Email** then **Save**.

Your OAuth settings should look similar to the following in FortiSIEM.



Email Gateway Server:	smtp-mail.outlook.	Enable SSL:	□
Server Port:	25	Secure Connection (TLS):	☑
Server Account ID:	fortisiem@outlook.com	Default Email Sender:	
Authentication:	○ Basic ● OAuth	OAuth Provider:	Microsoft
Client ID:	[redacted]	Client Secret:	••••••••••••••••••••••••••••••••
Enable S/MIME:	□		

If you still receive a “SendAs” in “SendAsDeniedException” error, you may need to go to your Office365 account and configure “Send email on behalf of another user”. This error occurs if the email address used for authentication is different than the FROM email address. The solution is to update your Office365 account settings to allow for sending on behalf of the FROM email address.

Image Server Settings

This section allows you to set up the Supervisor as an Image Server for upgrading Collectors and Agents. This mechanism provides an easy way to upgrade a large number of Collectors and Agents from one place.

- Upgrading Collectors
- Upgrading Linux Agents
- Upgrading Windows Agents
- Custom Update

Upgrading Collectors

Step 1: Download the Correct Collector Image from the Fortinet Support Site into your Workstation

As an example, Collector 6.4.0 image file name is `FSM_Upgrade_All_6.4.0_build1412.zip` and matches the hash in the support site to the locally computed hash. This ensures that the file has not been corrupted in transit.

Step 2: Upload the Image to the Supervisor Node

Note: In this step, you will upload the image to the Supervisor, which will then internally create a URL for the Collectors to download the image. It is critical to set the host name in the URL correctly so that a Collector can resolve the host name. Otherwise, the image download in Step 3 will fail.

There are two solutions.

Solution 1	By default, the Supervisor's host name in **ADMIN > License > Nodes** is used to create the URL. If the host name is a Fully Qualified domain name and is resolvable by the Collectors, then there is nothing to do. For example, a host name like `c2-52-35-20-68.us-west-2.compute.amazonaws.com` is resolvable to an external IP address. A host name like `2-52-35-20-68.us-west-2.compute` is likely not resolvable. If the hostname is not resolvable, either create a DNS entry to allow the Collector to resolve the hostname, or add an entry to the Collector `/etc/hosts` file in the following format: *`<ip> <host name>`* For example: `10.0.1.21 2-52-35-20-68.us-west-2.compute`
Solution 2	If there is a load balancer in front of the Supervisors, or you want to override the Supervisor host name in the default image download URL, then you can enter the appropriate host name or IP after going to **ADMIN > Settings > Systems > Image Server > Custom Update** and then clicking **Save**. If you have entered a host name here, make sure that it is a Fully Qualified domain name and is resolvable by Collectors. Do this step first before proceeding to the remaining of Step 2. Note that if you create an entry in Custom Update, then it applies to ALL Collectors and Agents. This means that every Collector and Agent will the get the URL with the Custom Update entry.

1. Go to **ADMIN > Settings > Systems > Image Server**.
2. Under **Collector**, in the **Version** field, enter the version you downloaded in Step 1. The format is #.#.#. Example: 6.4.0.
3. Under **Collector**, click **Select File** and select the Collector upgrade image you downloaded in Step 1.
4. Under **Collector**, click **Upload File** to upload the Collector upgrade image to the Supervisor. This may take a while depending on the network connection between your workstation and Supervisor node. FortiSIEM will validate the image hash and upload the image to Supervisor if the hash matches.
5. Run the following SQL and make sure ImageSetup task is completed.

```
# psql phoenixdb phoenix -c "select type, progress from ph_task where type =
'ImageSetup'"
    type | progress
------------+----------
 ImageSetup | 100
 ImageSetup | 100
 ImageSetup | 100
(3 rows)
```

Step 3: Download the Image to the Collector

1. Go to **ADMIN > Health > Collector Health**.
2. From the **Columns** drop-down list, ensure **Download Status** is selected. If not, select it so the **Download Status** column is displayed.
3. Select the Collector(s) you wish to download the image to.
   Note: Starting with release 6.4.0, you can choose multiple Collectors for downloading images.
4. From the **Action** drop-down list, select **Download Image**.
5. Check that the **Download Status** column shows **finished** to confirm that the download has been completed for the selected Collectors.

Step 4: Upgrade the Collector

1. Go to **ADMIN > Health > Collector Health**.
2. From the **Columns** drop-down list, ensure **Version** is selected. If not, select it so the **Version** column is displayed.
3. Select the Collector(s) you wish to upgrade.
   Note: Starting with release 6.4.0, you can choose multiple Collectors for installing images.
4. From the **Action** drop-down list, select **Install Image**.
5. Check that the **Version** columns shows the correct version number, in this example 6.4.0, to confirm that the Collector(s) have upgraded successfully.

Upgrading Linux Agents

Step 1: Download the Correct Linux Agent Image from the Fortinet Support Site into your Workstation.

As an example, a Linux Agents 6.4.0 image file name is `fortisiem-linux-agent-installer-6.4.0.1412.sh` and matches the hash in the support site to the locally computed hash. This ensures that the file has not been corrupted in transit.

Step 2: Upload the Image to the Supervisor Node

Note: In this step, you will upload the image to the Supervisor, which will then internally create a URL for the Agents to download the image. It is critical to set the host name in the URL correctly, so that an Agent can resolve the host name. Otherwise, the image download in Step 3 will fail.

There are two solutions.

Solution 1	By default, the Supervisor host name in **ADMIN > License > Nodes** is used to create the URL. If the host name is a Fully Qualified domain name and is resolvable by the Agents, then there is nothing to do. For example, a host name like `c2-52-35-20-68.us-west-2.compute.amazonaws.com` is resolvable to an external IP address. A host name like `2-52-35-20-68.us-west-2.compute` is likely not resolvable.
Solution 2	If there is a load balancer in front of the Supervisors, or you want to override the Supervisor host name in the default image download URL, then you can enter the appropriate host name or IP after navigating to **ADMIN > Settings > Systems > Image Server > Custom Update**, and then clicking **Save**. If you have entered a host name here, make sure that it is a Fully Qualified domain name and is resolvable by Agent. Do this step first before proceeding to the remaining of Step 2. Note that if you create an entry in Custom Update, then it applies to ALL Collectors and Agents. This means that every Collector and Agent will the get the URL with the Custom Update entry.

1. Go to **ADMIN > Settings > Systems > Image Server**.
2. Under **Linux Agent**, in the **Version** field, enter the version you downloaded in Step 1. The format is #.#.#. Example: 6.4.0.
3. Under **Linux Agent**, click **Select File** and select the Linux Agent upgrade image you downloaded in Step 1.
4. Under **Linux Agent**, click **Upload File** to upload the Linux Agent upgrade image to the Supervisor. This may take a while depending on the network connection between your workstation and Supervisor node. FortiSIEM will validate the image hash and upload the image to Supervisor if the hash matches.

Step 3: Download the Image to the Linux Agent

1. Go to **ADMIN > Health > Agent Health**.
2. From the **Columns** drop-down list, ensure **Upgrade Status** is selected. If not, select it so the **Upgrade Status** column is displayed.
3. Select the Linux Agent(s) you wish to download the image to.
   Note: Starting with release 6.4.0, you can choose multiple Linux Agents for downloading images.
4. From the **Action** drop-down list, select **Download Image**.
5. Check that the **Upgrade Status** column shows **Download Succeeded** to confirm that the download has been completed for the selected Linux Agents.

Step 4: Upgrade the Linux Agents

1. Go to **ADMIN > Health > Agent Health**.
2. From the **Columns** drop-down list, ensure **Version** is selected. If not, select it so the **Version** column is displayed.
3. Select the Linux Agent(s) you wish to upgrade.
   Note: Starting with release 6.4.0, you can choose multiple Linux Agents for installing images.
4. From the **Action** drop-down list, select **Install Image**.
5. Check that the **Upgrade Status** column shows **Upgrade Succeeded** to confirm that the Linux Agent(s) have upgraded successfully. Check that the **Version** column shows the correct version number, in this example 6.4.0, to confirm that the Linux Agent(s) have upgraded to the correct version.

Upgrading Windows Agents

Step 1: Download the Correct Windows Agent Images from the Fortinet Support Site into your Workstation.

1. Download the image file into your desktop. It is a .zip file, e.g. `FSMLogAgent-v4.2.1-build0225.zip`.
2. Compute the MD5 checksum and make sure that locally, the computed checksum matches the checksum in the Support Site. This ensures that the file is not corrupted in transit.
3. Unzip the file. You will see that there are two files – `AutoUpdate.exe` and `FSMLogAgent.exe`. You will need to upload these files in Step 2.3 and Step 2.4 below.

Step 2: Upload the Image to the Supervisor Node

Note: In this step, you will upload the image to the Supervisor, which will then internally create a URL for the Agents to download the image. It is critical to set the host name in the URL correctly, so that an Agent can resolve the host name. Otherwise, the image download in Step 3 will fail.

There are two solutions.

Solution 1	By default, the Supervisor host name in **ADMIN > License > Nodes** is used to create the URL. If the host name is a Fully Qualified domain name and is resolvable by the Agents, then there is nothing to do. For example, a host name like `c2-52-35-20-68.us-west-2.compute.amazonaws.com` is resolvable to an external IP address. A host name like `2-52-35-20-68.us-west-2.compute` is likely not resolvable.
Solution 2	If there is a load balancer in front of the Supervisors or you want to override the Supervisor host name in the default image download URL, then you can enter the appropriate host name or IP after going to **ADMIN > Settings > Systems > Image Server > Custom Update**, then clicking **Save**. If you have entered a host name here, make sure that it is a Fully Qualified domain name and is resolvable by Agent. Do this step first before proceeding to the remaining of Step 2. Note that if you create an entry in Custom Update, then it applies to ALL Collectors and Agents. This means that every Collector and Agent will the get the URL with the Custom Update entry.

1. Go to **ADMIN > Settings > Systems > Image Server**.
2. Under **Windows Agent**, in the **Version** field, enter the version you downloaded in Step 1. The format is #.#.#. Example: 4.2.1.
   Note: For Windows Agent, two files are required, the FSMLogAgent executable (FSMLogAgent.exe) and an AutoUpdate executable (AutoUpdate.exe, or AutoUpdate32.exe).
3. Under **Windows Agent**, click **Select File** and select one of the two Windows Agent upgrade image you downloaded in Step 1.
4. Under **Windows Agent**, click **Select File** and select the second Windows Agent upgrade image you downloaded in Step 1.
5. Under **Windows Agent**, click **Upload File** to upload the Windows Agent upgrade images to the Supervisor. This may take a while depending on the network connection between your workstation and Supervisor node. FortiSIEM will validate the image hash and upload the image to Supervisor if the hash matches.

Step 3: Download the Images to the Windows Agent

1. Go to **ADMIN > Health > Agent Health**.
2. From the **Columns** drop-down list, ensure **Upgrade Status** is selected. If not, select it so the **Upgrade Status** column is displayed.

3. Select the Windows Agent(s) you wish to download the image to.
   Note: Starting with release 6.4.0, you can choose multiple Windows Agents for downloading images.
4. From the **Action** drop-down list, select **Download Image**.
5. Check that the **Upgrade Status** column shows **Download Succeeded** to confirm that the download has been completed for the selected Windows Agents.

Step 4: Upgrade the Windows Agents

1. Go to **ADMIN > Health > Agent Health**.
2. From the **Columns** drop-down list, ensure **Version** is selected. If not, select it so the **Version** column is displayed.
3. Select the Windows Agent(s) you wish to upgrade.
   Note: Starting with release 6.4.0, you can choose multiple Windows Agents for installing images.
4. From the **Action** drop-down list, select **Install Image**.
5. Check that the **Upgrade Status** column shows **Upgrade Succeeded** to confirm that the Windows Agent(s) have upgraded successfully. Check that the **Version** column shows the correct version number, in this example 4.2.1, to confirm that the Windows Agent(s) have upgraded to the correct version.

Custom Update

To allow Load Balancers in front of the Supervisor to work, Fortinet allows you to perform a custom upgrade through a configured IP/Host Name.
Note: The current upgrade URL for Collectors and Agents were auto generated by the App Server based on the Supervisor host name.

To perform a custom update, take the following steps.

1. Navigate to **ADMIN > Settings > System > Image Server**.
2. Under **Custom Update**, in the **IP/Host Name** field, enter the IP address or host name to use as the public download URL.
   Note: Make sure the Collector or Agent can either ping the new IP address or host name.
3. Click **Save**.
4. Upload the secure image file. (Following the steps from the appropriate instructions: Upgrading Collectors, Upgrading Linux Agents, Upgrading Windows Agents.)
   Note: If you re-update to a new URL/host name, the secure image must be re-uploaded, otherwise downloading the image will fail because the previously uploaded image retains the old IP/Hostname.
5. Download Image file. (Following the steps from the appropriate instructions: Upgrading Collectors, Upgrading Linux Agents, Upgrading Windows Agents.)
6. Install Image. (Following the steps from the appropriate instructions: Upgrading Collectors, Upgrading Linux Agents, Upgrading Windows Agents.)

Cluster Config

A Load Balancer or Supervisors, and Collectors can be added into a cluster configuration here. For more information on Supervisor Cluster, see Configuring and Maintaining Active-Active Supervisor Cluster.

For Supervisors or Load Balancer configuration, take the following steps:

1. Navigate to **ADMIN > Settings > System > Cluster Config**.
2. Under **Supervisors**, in the **Address** field, enter the Supervisor or Load Balancer Host Name or IP address.

3. (Optional) Click **+** to add a Supervisor, or **-** to remove one, and repeat step 2 to configure any additional Supervisor or Load Balancer.
4. Click **Save** when done.

For Collectors:

Collectors upload events and configurations to Worker nodes.

There are three cases:

- Explicit list of Worker IP addresses or host names - Collector forwards to this list in a round robin manner.
- If you are not using Workers and using only a Supervisor and Collector(s) – specify the Supervisor IP addresses or host name. The Collectors will upload directly to the Supervisor node.
- Host name of a load balancer - Collector forwards this to the load balancer which must be configured to distribute events to the workers.

Any Hostnames specified in the Worker Upload must be resolvable by the Collector and similarly, any specified IP addresses must have connectivity from the Collector.

Complete these steps to configure Worker upload settings:

1. Navigate to **ADMIN > Settings > System > Cluster Config**.
2. Under **Event Upload Workers**, in the **Address** field, enter the Worker Host Name or IP address.
3. (Optional) Click **+** to add a Worker, or **-** to remove one, and repeat step 2 to configure any additional Workers.
4. Click **Save** when done.

Lookup Settings

Lookup setting can be used to find any IP or domain by providing the link.

Complete these steps for lookup:

1. Go to **ADMIN** > **Settings** > **System** > **Lookup** tab.
2. Enter the **Name**.
3. Select the **Client Type** to **IP** or **Domain**.
4. Enter the **Link** for look-up.
   You must enter "`<ip>`" in the link. FortiSIEM will replace "`<ip>`" with a proper IP during lookup.
   For example, to lookup the following URL:
   `http://whois.domaintools.com/8.8.8.8`
   Enter the following link in FortiSIEM:
   `http://whois.domaintools.com/<ip>`
5. Click **Save**.

Kafka Settings

FortiSIEM events found in system event database can be exported to an external system via Kafka message bus.

FortiSIEM supports both forwarding events to an external system via Kafka message bus as a 'Producer' and receiving events from a third-party system to FortiSIEM via Kafka message bus as a 'Consumer'.

As a Producer:

- Make sure you have set up a Kafka Cloud (here) with a specific Topic for FortiSIEM events.
- Make sure you have identified a set of Kafka brokers that FortiSIEM is going to send events to.
- Make sure you have configured Kafka receivers which can parse FortiSIEM events and store in a database. An example would be Logstash receiver (see here) that can store in an Elastic Search database.
- Configure event forwarding in order for FortiSIEM to send events to an external Kafka consumer.
- Supported Kafka version: 0.8

As a Consumer:

- Make sure you have set up a Kafka Cloud (here) with a specific Topic, Consumer Group and a Consumer for sending third party events to FortiSIEM.
- Make sure you have identified a set of Kafka brokers that FortiSIEM will receive events from.
- Supported Kafka version: 0.8

Setting up Consumer

Complete these steps to configure Kafka for authentication.

Note: Tested with

- kafka_2.11-0.11.0.2.tgz (Kafka 0.11, Scala 2.11)
- kafka_2.13-2.7.0.tgz (Kafka 2.7, Scala 2.13 which is the latest as of March 2021)

1. Download the source code tarball (either one).
   https://archive.apache.org/dist/kafka/0.11.0.2/kafka_2.11-0.11.0.2.tgz
   https://archive.apache.org/dist/kafka/2.7.0/kafka_2.13-2.7.0.tgz
2. Uncompress the files and enter the "config" folder.
3. Modify the configuration files by appending the following to the end of the files:

```
# zookeeper.properties
authProvider.1=org.apache.zookeeper.server.auth.SASLAuthenticationProvider
requireClientAuthScheme=sasl
jaasLoginRenew=3600000

# zookeeper_jaas.conf
Server {
org.apache.zookeeper.server.auth.DigestLoginModule required
   user_super="zookeeper"
   user_alice="alice-secret";
};
Notice the last line is user_{username}="{password}"
If the username is ‘admin’, the line will be
user_admin="admin-password";


# server.properties
host.name=192.0.2.0
port=9092
security.inter.broker.protocol=SASL_PLAINTEXT
sasl.mechanism.inter.broker.protocol=SCRAM-SHA-512
sasl.enabled.mechanisms=SCRAM-SHA-512
authorizer.class.name=kafka.security.auth.SimpleAclAuthorizer
allow.everyone.if.no.acl.found=true
auto.create.topics.enable=true
listeners=SASL_PLAINTEXT://192.0.2.10:9092
advertised.listeners=SASL_PLAINTEXT://192.0.2.10:9092
ssl.client.auth=required
Note: Change the IP addresses to actual

# kafka_server_jaas.conf
KafkaServer {
org.apache.kafka.common.security.scram.ScramLoginModule required
username="alice"
password="alice-secret"
user_alice="alice-secret";
};
Client {
org.apache.zookeeper.server.auth.DigestLoginModule required
username="alice"
password="alice-secret";
};

# kafka_client_jaas.conf
KafkaClient {
org.apache.kafka.common.security.scram.ScramLoginModule required
username="alice"
password="alice-secret"
user_alice="alice-secret";
};
Client {
org.apache.zookeeper.server.auth.DigestLoginModule required
username="alice"
password="alice-secret";
};

# consumer.properties
security.protocol=SASL_PLAINTEXT
sasl.mechanism=SCRAM-SHA-512
sasl.jaas.config=org.apache.kafka.common.security.scram.ScramLoginModule
required username="alice" password="alice-secret";
```

4. Start zookeeper.

```
cd ..
export KAFKA_OPTS="-Djava.security.auth.login.config=$(\pwd)/config/zookeeper_
jaas.conf"
bin/zookeeper-server-start.sh config/zookeeper.properties
(In another shell window)
```

```
bin/kafka-configs.sh --zookeeper localhost:2181 --alter --add-config 'SCRAM-SHA-
512=[password=alice-secret]' --entity-type users --entity-name alice
```

5. Start the server (In another shell window)

   ```
   export KAFKA_OPTS="-Djava.security.auth.login.config=$(pwd)/config/kafka_server_
   jaas.conf"
   bin/kafka-server-start.sh config/server.properties
   ```

6. Create topic (name=test1) (In another shell window)

   ```
   bin/kafka-topics.sh --create --topic test1 --zookeeper localhost:2181 --par-
   titions 3 --replication-factor 1
   ```

7. Start consumer.

   ```
   export KAFKA_OPTS="-Djava.security.auth.login.config=$(pwd)/config/kafka_client_
   jaas.conf"
   bin/kafka-console-consumer.sh --topic test1 --bootstrap-server=192.0.2.10:9092 -
   -consumer.config=config/consumer.properties
   ```

   At this point, when FortiSIEM forwards events to this client, contents can be seen in the consumer window.

8. (Optional) Start producer.

   ```
   export KAFKA_OPTS="-Djava.security.auth.login.config=$(pwd)/config/kafka_client_
   jaas.conf"
   bin/kafka-console-producer.sh --topic test1 --broker-list 192.0.2.10:9092 --pro-
   ducer.config config/producer.properties
   ```

Setting Up FortiSIEM

Complete these steps for configuring Kafka settings in FortiSIEM:

1. Go to **ADMIN** > **Settings** > **System** > **Kafka** tab.
2. Click **New**.
3. Enter the **Name** and **Topic**.
4. Select or search the **Organization** from the drop-down.
5. Add **Brokers** by clicking **+** icon.
   a. Enter IP address or Host name of the broker.
   b. Enter Broker port (default 9092).
6. Click **Save**.
7. Select the **Client Type** to **Producer** or **Consumer**.
8. If the Consumer is selected in step 7, enter the **Consumer Name** and **Group Name** fields.
9. Enable Authentication if you want to apply Kafka authentication by adding a checkmark to the **Authentication** checkbox, then take the following steps:
   a. **Protocol** should be set as **SASL_PLAINTEXT**.
   b. Select your authentication mechanism: **PLAIN**, **SCRAM-SHA-256**, or **SCRAM-SHA-512**.
   c. In the **User Name** field, enter the user name to authenticate for the Kafka servers.
   d. In the **Password** field, enter the password associated with the user name to authenticate for the Kafka servers.

   e. In the **Confirm Password** field, re-enter the password associated with the user name to authenticate for the Kafka servers.

10. Click **Save**.

Dashboard Slideshow Settings

Dashboard Slideshow settings are used to select a set of dashboards and display them in a slideshow mode on big monitors to cover the entire display. This is useful for Network and Security Operation Centers.

Complete these steps to create a Dashboard Slideshow:

1. Go to **ADMIN** > **Settings** > **System** > **Dashboard Slideshow** tab.
2. Click **New** to create a slideshow.
3. Enter a **Name** for the slideshow.
4. Select the **Interval** for switching between dashboards.
5. Select the **Dashboards** from the list and move to the **Selected** list.
   These dashboards will be displayed in a slideshow mode.
6. Click **Save**.

For all the above System settings, use the **Edit** button to modify or **Delete** button to remove any setting from the list.

Dashboard Ownership

Dashboard Ownership settings are used to transfer editing rights from the current owner of a shared dashboard to another person. It requires that the owner to whom the rights are being transferred to, to have the same exact role permissions as the current owner. This feature can be useful if the current owner is no longer available, and another person is required to handle the shared dashboard of that individual.

Complete these steps to transfer Dashboard Ownership:

1. Go to **ADMIN** > **Settings** > **System** > **Dashboard Ownership** tab.
2. Select the Dashboard you wish to transfer ownership of.
3. Click **Transfer**.
4. In the Transfer Ownership window, select the new owner from the **To:** drop-down list.
5. Click **Save**.

You can verify the transfer by looking at the user in the **User** column.

PAYG Report

If applicable, you can generate a daily or monthly Pay as you Go (PAYG) report.

Complete these steps to generate a daily or monthly PAYG report:

1. Go to **ADMIN** > **Settings** > **System** > **PAYG Report** tab.
2. In the **Partner ID** field, enter the Partner ID.
3. Take the following steps to enable Daily Reports.
   a. Check the Daily Report checkbox.
   b. In the **Email** field, enter the email address for a person to whom a daily report should be sent.
   c. Click **+** to add another Email field entry.
   d. Repeat steps b and c to input additional entries.

4. Take the following steps to enable Monthly Reports.
    a. Check the Monthly Report checkbox.
    b. In the **Email** field, enter the email address for a person to whom a monthly report should be sent.
    c. Click **+** to add another Email field entry.
    d. Repeat steps b and c to input additional entries.
5. When done, click **Test** to verify your email address distribution.
6. Click **Save**.
7. To enable Month Reports, click the Monthly Report checkbox.
8. In the Transfer Ownership window, select the new owner from the **To:** drop-down list.
9. Click **Save** to finish.

Trusted Hosts

You can restrict GUI Login by defining a set of IP addresses here. If the field is empty, then GUI login from any IP addresses are allowed. However once defined, new logins are disallowed from IP addresses outside of the defined range. Existing logins are not affected. To force a logout, click on👤 in the GUI, select a user, and click **Log Out** or **Log Out and Lock Out**.

Note: If you have defined Trusted Hosts, then remember to include the Collectors and the Agents, else they will not be able to register.

Take the following steps to configure:

1. Navigate to **ADMIN > Settings > System > Trusted Hosts**.
2. In the **Trusted Hosts** field, enter a single IP address or CIDR range, for example 172.0.20.1/24.
3. Click **+** to add another Trusted Hosts field to configure if needed.
   Note: Click **-** to remove an existing Trusted Hosts field.
4. Click **Save** when done.

Analytics Settings

The following section describes the procedures for Analytics settings:

- Scheduled Reports
    - Scheduling Report Alerts
    - Scheduling Report Copy
- Incident Notification
    - Setting Incident HTTP Notification
    - Setting Incident SNMP Traps
    - Setting Remedy Notification
- Setting a Subcategory
- Setting Risk Filters
- Setting UEBA Higher Risk Entities
- UEBA Tags
- Tags

Scheduled Reports

Scheduled Reports allows you to schedule report notifications when a scheduled report is run, and also send a copy of a report to a remote location when a scheduled report is sent.

- Scheduling Report Alerts
- Scheduling Report Copy

Scheduling Report Alerts

You can schedule reports to run and send email notifications to specific individuals. This setting is for default email notifications that will be sent when any scheduled report is generated.

1. Go to **ADMIN** > **Settings** > **Analytics** > **Scheduled Report** tab.
2. Select the required action under **Scheduled Report Alerts** section.
   - **Do not send scheduled emails if report is empty** - Sometimes a report may be empty because there are no matching events. If you don't want to send empty reports to users, select this option. If you are running a multi-tenant deployment, and you select this option while in the Super/Global view, this will apply only to Super/Global reports. If you want to suppress delivery of empty reports to individual Organizations, configure this option in the Organizational view.
3. Enter the email address in **Deliver notification via** filed. Click **+** to add more than one email address, if needed.
4. Click **Save**.
5. To receive email notifications, go to **ADMIN** > **Settings** > **System** > **Email** and configure your mail server.

Scheduling Report Copy

Reports can be copied to a remote location when the scheduler runs any report. Note that this setting only supports copy to Linux remote directory.

1. Go to **ADMIN** > **Settings** > **Analytics** > **Scheduled Report** tab.
2. Enter the following information under **Scheduled Report Copy** section.
3. Enter the **Host** - IP address or name.
4. Enter the **Path** - absolute path, such as `/abc/def`.
5. Enter the **User Name** and **Password**, and enter **Confirm Password** to reconfirm the password.
6. Click **Test** to check the connection.
7. Click **Save**.

Note: For all of the above configurations, use the **Edit** button to modify any setting or **Delete** to remove any setting.

Incident Notification

Incident Notification allows you configure incident notifications in the following ways.

- Incident HTTP Notification
- Incident SNMP Traps
- Remedy Notification

Setting Incident HTTP Notification

You can configure FortiSIEM to send an XML message over HTTP(s) when an incident is triggered by a rule.

1. Go to **ADMIN** > **Settings** > **Analytics** > **Incident Notification** tab.
2. Enter the following information under **Incident HTTP Notification** section.
3. For **HTTP(S) Server URL**, enter the URL of the remote host where the message should be sent.
4. Enter the **User Name** and **Password** to use when logging in to the remote host, and enter **Confirm Password** to reconfirm the password.
5. Click **Test** to check the connection.
6. Click **Save**.

Incidents are sent out in XML format. For details, see here.

Setting Incident SNMP Traps

You can define SNMP traps that will be notified when an event triggers an incident.

1. Go to **ADMIN** > **Settings** > **Analytics** > **Incident Notification** tab.
2. Enter the following information under **Incident SNMP Traps** section.
   a. **SNMP Trap IP Address**
   b. **SNMP Community String** - to authorize sending the trap to the SNMP trap IP address.
3. Select the **SNMP Trap Type** and **SNMP Trap Protocol** options.
4. Click **Test** to check the connection.
5. Click **Save**.

For the SNMP MIB definition, see here.

Setting Remedy Notification

You can set up Remedy to accept notifications from FortiSIEM and generate tickets from those notifications.

Configuring Remedy to Accept Tickets from FortiSIEM Incident Notifications

Before configuring Remedy to accept tickets, make sure you have configured the Remedy Notifications in FortiSIEM.

1. In Remedy, create a new form, **FortiSIEM_Incident_Interface**, with the incident attributes listed in the table at the end of this topic as the form fields.
2. When you have defined the fields in the form, right-click the field and select the **Data Type** that corresponds to the incident attribute.
3. After setting the form field data type, click in the form field again to set the **Label** for the field.
4. When you are done creating the form, go to **Servers** > **localhost** > **Web Service** in Remedy, and select **New Web Service**.
5. For **Base Form**, enter **FortiSIEM_Incident_Interface**.
6. Click the **WSDL** tab.
7. For the **WSDL Handler URL**, enter `http://<midtier_server->/arsys/WSDL/public/<servername>/FortiSIEM_Incident_Interface`.
8. Click the **Permissions** tab and select **Public**.
9. Click **Save**.

You can test the configuration by opening a browser window and entering the WSDL handler URL from step 7 above, substituting the Remedy Server IP address for `<midtier_server>` and `localhost` for `<servername>`. If you see an XML page, your configuration was successful.

Incident Attributes for Defining Remedy Forms

Incident Attribute	Data type	Description
biz_service	text	Name of the business services affected by this incident
cleared_events	text	Events which cleared the incident
cleared_reason	text	Reason for clearing the incident if it was cleared
cleared_time	bigint	Time at which the incident was cleared
cleared_user	character varying (255)	User who cleared the incident
comments	text	Comments
cust_org_id	bigint	Organization id to which the incident belongs
first_seen_time	bigint	Time when the incident occurred for the first time
last_seen_time	bigint	Time when the incident occurred for the last time
incident_count	integer	Number of times the incident triggered between the first and last seen times
incident_detail	text	Incident Detail attributes that are not included in incident_src and incident_target
incident_et	text	Incident Event type
incident_id	bigint	Incident Id
incident_src	text	Incident Source
incident_status	integer	Incident Status
incident_target	text	Incident Target
notif_recipients	text	Incident Notification recipients
notification_action_status	text	Incident Notification Status

Incident Attribute	Data type	Description
orig_device_ip	text	Originating/Reporting device IP
ph_incident_category	character varying (255)	FortiSIEM defined category to which the incident belongs: Network, Application, Server, Storage, Environmental, Virtualization, Internal, Other
rule_id	bigint	Rule id
severity	integer	Incident Severity 0 (lowest) - 10 (highest)
severity_cat	character varying (255)	LOW (0-4), MEDIUM (5-8), HIGH (9-10)
ticket_id	character varying (2048)	Id of the ticket created in FortiSIEM
ticket_status	integer	Status of ticket created in FortiSIEM
ticket_user	character varying (1024)	Name of the user to which the ticket is assigned to in FortiSIEM
view_status	integer	View status
view_users	text	View users

Complete these steps to set up the routing to your Remedy server.

1. Go to **ADMIN** > **Settings** > **Analytics** > **Incident Notification** tab.
2. Enter the following information under **Remedy Notification** section.
3. For **WSDL**, enter the URL of the Remedy Server.
4. Enter the **User Name** and **Password** associated with your Remedy server, and enter **Confirm Password** to reconfirm the password.
5. Click **Test** to check the connection.
6. Click **Save**.

Setting a Subcategory

FortiSIEM Incidents are grouped into different categories – Availability, Change, Performance, Security and Other. A Category is assigned to every Rule and you can search any Incidents using these Categories. FortiSIEM extends this concept to include Subcategories. A Subcategory is defined for every system-defined rule. You can add a Subcategory for custom rules and also create new Subcategories. Incidents can be searched using both Categories and Subcategories.

Creating a Subcategory

1. Go to **ADMIN > Settings > Analytics > Subcategory**.
2. Select the **Category** from the left-hand panel where you want to create a Subcategory.
3. Click **Add** in the right-hand panel.
4. Enter a name for the new Subcategory.
5. Click the checkmark icon or click **Save All**.

Modifying a Subcategory

You can modify only user-defined Subcategories. You cannot modify system-defined Subcategories.

1. Select the Subcategory you want to modify.
2. Click the edit icon.
3. Modify the name in the **Subcategory** field.
4. Click the checkmark icon or **Save All**.

Deleting a Subcategory

You can delete only user-defined Subcategories. You cannot delete system-defined Subcategories.

1. Select the Subcategory you want to delete.
2. Click the **-** icon.
3. Click **Save All**.

Setting Risk Filters

A Risk Filter allows you to include or exclude certain rules from the Risk Score calculation. For more information on Risk Scores, see Risk View. (Note we also have an Entity Risk Score topic which is empty)

In the SP model, you can create a global Risk Filter or filters for individual organizations. A global Risk Filter can include only system rules, and is available to all organizations. You can create only one Risk Filter for an organization. Multiple filters are not allowed. This Risk Filter includes the filter defined for the organization itself and the global filter if one exists.

The VA model allows only one filter.

The Risk Filter view contains a table with three columns. The **Scope** column lists the organization the filter belongs to. The **Included Rules** column lists the rules that will be included in the calculation of the risk score. The **Excluded Rules** columns lists the rules that will not be included in the calculation of the Risk Score.

Creating a Risk Filter

Follow these steps to create a Risk Filter.

1. Go to **ADMIN > Settings > Analytics > Risk Filter** to open the Risk Filter view.
2. Click **New**.
3. In the New Risk Filter dialog box, select **Super/Local** or the name of an organization from the **Add filter for** drop-down list.
4. Click **Next**.

5. In the next dialog box, **Include** is selected by default. Open the **Rules** tree under **Groups** and shuttle the rules you want to include in the filter from the **Rules** column to the **Selection** column.
6. Select **Exclude** and repeat the process described in the previous step to exclude rules from the filter.
7. Click **Save**. Your rule selections will appear in the **Included Rules** and **Excluded Rules** columns of the table.

Editing a Risk Filter

Follow these steps to edit a Risk Filter.

1. Go to **ADMIN > Settings > Analytics > Risk Filter** to open the Risk Filter view.
2. Click **Edit**.
3. In the dialog box, **Include** is selected by default. Shuttle the rules you do not want to be included in the Risk Score from the **Selection** column to the **Rules** column.
4. Select **Exclude** and repeat the process described in the previous step to exclude rules from the filter.
5. Click **Save**.

Deleting a Risk Filter

Follow these steps to delete a Risk Filter.

1. Go to **ADMIN > Settings > Analytics > Risk Filter** to open the Risk Filter view.
2. Select the row in the table containing the filter you want to delete.
3. Click **Delete**.

Viewing Risk Filter Results

To see the impact of the filters you defined, go to **INCIDENTS**. Click the Risk icon (📈 Risk) to open the Risk View. For a description of the Risk View, see Risk View.

Tags

Tags allow you to create a keyword or phrase, the "tag", that can be associated with rules that trigger incidents. After creating a tag, you associate it with a rule (See Creating a Rule: Step 3: Define Actions). After this configuration, you can view tags on the Incidents List View page by doing any of the following.

- Add the **Tag** column to view tags that were part of a rule triggered incident.
- Search for tag related incidents by including **Incident Tag** as part of your search.

Creating a Tag

Follow these steps to create a new tag.

1. Navigate to **ADMIN > Settings > Analytics > Tags**.
2. Click **New**.
3. In the **Add New Tag** window, take the following steps:
   a. In the **Tag** field, enter your the name of the tag you wish to create.
   b. In the **Color** field, select a color for the tag: Red, Yellow, or Green.
   c. (Optional) In the **Description** field, add any information you wish to convey about the tag, such as its

intent.

d. When done, click **Save**.

At this point, you tag will be saved, and be available from the Tags drop-down list when creating or editing a Rule.

Editing a Tag

Follow these steps to edit a tag.

1. Navigate to **ADMIN > Settings > Analytics > Tags**.
2. Select the tag you wish to edit, and click **Edit**.
3. In the **Edit Tag: <*Name of Tag*>** window, make any changes to the **Tag**, **Color**, and **Description** fields.
4. When done, click **Save**.

Deleting a Tag

Follow these steps to delete a tag.

1. Navigate to **ADMIN > Settings > Analytics > Tags**.
2. Select the tag you wish to delete.
3. Click **Delete**.

UEBA Settings

The AI module runs on Super and Worker nodes. All Agent activity is routed to one node in a sticky manner. If a Worker is down, Agent events are routed to another Worker. If a Worker is added, then new Agents are routed to that Worker. Additionally, AI models are now persisted across AI module restarts.

AI alerts can be monitored in the **UEBA** View in the **INCIDENTS** page. See UEBA View.

- Setting UEBA Higher Risk Entities
- Setting UEBA Tags

Setting UEBA Higher Risk Entities

UEBA Higher Risk Entities allow you to prioritize AI alerts that are most relevant to you by increasing the weight of events to High. This weighting will influence the AI model, similar to UEBA Tags. You can identify high-risk or business-critical entities, including file types, file paths, users, and groups.

Follow these steps to specify important entities:

1. Click **ADMIN > Settings > Analytics > UEBA Higher Risk Entities**.
2. The **UEBA Higher Risk Entities** dialog box contains the following fields. All of the fields are optional. In each field, use the **+** and **-** buttons to add or remove entries.
    - **File Types** - Enter the type of file you want to monitor, for example, `.exe`.
    - **File Paths** - Enter the path to the folder you want to monitor.
    - **User Accounts** - Enter the name of the Windows Agent-side user account you want to monitor.
    - **Group Names** - Enter the name of the Windows Agent-side group you want to monitor.
3. Click **Save**.

Setting UEBA Tags

AI inspects the events for specific characteristics, as defined in the AI tag definitions, and applies the appropriate tags to events that match.

Follow these steps to set tags:

1. Click **ADMIN > Settings > Analytics > UEBA Tags**.
2. Provide values for the following fields:
    a. **Enabled** - Select this option to allow FortiSIEM to monitor the alert.
    b. **ID** (required) - A user-defined ID. Only these characters are allowed: **a-z**, **A-Z**, **0-9**, and the underbar character (_).
    c. **Name** (required) - The user-defined name for the entity. Only these characters are allowed: **a-z**, **A-Z**, **0-9**, and white space.
    d. **Description** - An optional description of the alert.
    e. **Weight** - Select a value from the drop-down list. The values can range from **Never Alert** (-5) to **Always Alert** (+5).
    f. **Rules**
        i. **Field** - Choose a value from the drop-down list. Available values are **Machine ID**, **User**, **Application**, **Activity**, **Resource**, and **Resource Filename**.

  ii. **Relation** - Choose a value from the drop-down list. Available values are **=**, **!=**, **CONTAIN**, **NOT CONTAIN**, **MATCH**, **NOT MATCH**, **START WITH**, **NOT START WITH**, **END WITH**, and **NOT END WITH**.
  iii. **Value** - A comma-separated list of values. These values can be user-defined.
  iv. Click **+** or **-** to add or delete rows in the **Rules** list.

3. Click **Save**.

Discovery Settings

This section describes the procedures for the following Discovery settings:

- Generic
- Device Filter
- Application Filter
- Location
- CMDB Groups

Generic

Before you initiate discovery, you should configure the Discovery Settings in your Supervisor as required for your deployment.

1. Go to **ADMIN** > **Settings** > **Discovery** > **Generic** tab.
2. Enter the following information under **Generic Settings** section. In a SP deployment, you must define all these

settings for each Organization by logging in to the Organization directly.

Setting	Description
Virtual IPs	Often a common virtual IP address will exist in multiple machines for load balancing and fail-over purposes. When you discover devices, you must have these virtual IP addresses defined within your discovery settings for two reasons: • Listing the virtual IP addresses ensures that two or more devices with the same virtual IP will not be merged into one device during device discovery, so each of the load-balanced devices will maintain their separate identity in the CMDB • The virtual IP will not be used as an access IP during discovery, since the identity of the device when accessed via the virtual IP is unpredictable Enter the **Virtual IP** and click **+** to add more, if required.
Excluded Shared Device IPs	An enterprise often has servers that share credentials, for example mail servers, web proxies, and source code control servers, and a large number of users will authenticate to these servers to access their services. Providing a list of the IP addresses for these servers allows FortiSIEM to exclude these servers from user identity and location calculations in the **Analytics** > **IdentityandLocation** report. For example, suppose user A logs on to server B to retrieve his mail, and server B authenticates user A via Active Directory. If server B is not excluded, the **Analytics > Identity and Location Report** will contain two entries for user A: one for the workstation that A logs into, and also one for server B. You can eliminate this behavior by adding server B to the list of Server IPs with shared credentials. Enter the **Excluded Shared Device IPs** and click **+** to add more, if required.
Virtual Device Hardware Serial Numbers	If two or more devices have identical hardware serial number, specify them here. In general, hardware serial number is used to uniquely identify a device and therefore two devices with identical hardware serial number is merged into a single device in CMDB. If a hardware serial number is present in the Virtual Hardware Serial Numbers list, then it is excluded for merging purposes. Enter the **Virtual Device Hardware Serial Numbers** and click **+** to add more, if required.
Allow Incident Firing on	This setting allows you to control incident firings based on approved device status. If the **Approved Devices Only** option is selected, the following logic

Setting	Description
	is used: (a) If at least one Source, Destination or Host IP is approved, the incident triggers. (b) Else if at least one incident reporting device is approved, the incident triggers. (c) Else the incident does not trigger. **Note:** System devices (Super, Worker, and Collectors) will always be considered to be approved devices. In other words, incidents will fire for these system devices even if **Approved Devices Only** option is selected. Select **All Devices** or **Approved Devices Only** accordingly.

3. Click **Save**.

Device Filter

This setting allows you to limit the set of devices that the system automatically learns from logs and Netflows. After receiving a log from a device, the system automatically learns that device and adds it to CMDB. When a TCP/UDP service is detected running on a server from Netflow analysis, the server along with the open ports are added to CMDB.

Sometimes, you may not want to add all of these devices to CMDB. You can create filters to exclude a specific set of devices from being added to CMDB. Each filter consists of a required **Excluded IP Range** field and an optional **Except** field.

1. Go to **ADMIN** > **Settings** > **Discovery** > **Device Filter** tab.
2. Click **New**.
3. In the **Range Definition** dialog box, enter the following information:
   a. **Excluded IP Ranges** - A device will not be added to CMDB if it falls in the range defined in the Excluded IP Range field. For example, if you wanted to exclude the `172.16.20.0/24` network from CMDB, add a filter with `172.16.20.0-172.16.20.255` in its **Excluded IP Range** field.
   b. **Except** - This field allows you to specify some exceptions in the excluded range. For example, if you wanted to exclude the `172.16.20.0/24` network without excluding the `172.16.20.0/26` network, add a filter with `172.16.20.0-172.16.20.255` in the **Excluded IP Range** field, and `172.16.20.192-172.16.20.255` in the **Except** field.

   You can add multiple values for these fields by clicking the **+** icon or remove an entry by clicking the **-** icon.
4. Click **Save**.

Application Filter

This setting allows you to limit the set of applications/processes that the system automatically learns from discovery. You may be more interested in discovering and monitoring server processes/daemons, rather than client processes, that run on a server. To exclude client processes from being discovered and listed in the CMDB, enter these applications here. An application/process will not be added to CMDB if it matches one of the entries defined in this table.

1. Go to **ADMIN** > **Settings** > **Discovery** > **Application Filter** tab.
2. Click **New**.

3. In the **Process Definition** dialog box, enter the **Process Name** and any **Parameters** for that process that you want to filter.
   Matching is exact and case-insensitive based on Process Name and Parameter. If **Parameter** is empty, then only **Process Name** is matched.
4. Select the **Organization** from the drop-down list.
5. Click **Save**.

Location

This setting allows you to set location information for devices in CMDB. Location information can be defined for a set of IP addresses. When applied, this information will overwrite the existing Location information in the CMDB. Future discoveries will not overwrite this information. Use this method to update locations of multiple devices with private IP addresses only. It is not necessary to update locations for public address space in this manner, because this information can also be obtained from a separate built-in database location.

1. Go to **ADMIN** > **Settings** > **Discovery** > **Location** tab.
2. Click **New**.
3. In the **Location Definition** dialog box, select or enter the following information:
   - Organization Type
   - IP/IP Range
   - Location
   - Update Manual Devices (This enables the system to overwrite the location information for manually defined devices in CMDB.)
4. Click **Save**.
5. Select the new location from the list and click **Apply**.

CMDB Groups

This setting allows you to write rules to add devices in CMDB Device Group and Business Service Groups of your choice. When a device is discovered, the policies defined here are applied and the device is assigned to the group(s) defined in the matching policies. This device grouping does not overwrite the CMDB Device group assigned during discovery. The grouping defined here is in addition to the discovery defined CMDB group.

1. Go to **ADMIN** > **Settings** > **Discovery** > **CMDB Groups** tab.
2. Click **New**.
3. In the **CMDB Group Definition** dialog box, select or enter the following information:
   - **Organization** - the organization which this rule applies to
   - **Vendor** - the matching device vendor
   - **Model** - the matching device model
   - **Host Name** - matching device host name via regular expression match
   - **IP Range** - matching device access IP - format is single IP, IP range, CIDR
   - **Custom Properties** - see Grouping Devices by Custom Properties
   - **Groups** - specify the groups which the matching devices will be added to
   - **Biz Services**- specify the business services which the matching devices will be added to
4. Click **Save**.
5. Select the new CMDB group from the list and click **Apply**.

Conditions are matched in ANDed manner: Both the actions are taken, that is, if both a Group and a Business Service is specified, then the device will be added to both the specified Group and Business Service.

To apply one or more CMDB Group policies:

1. Select one or more policies and click **Apply** or click **Apply All** to apply all policies.
2. Once a policy is saved, then next discovery will apply these policies. That means, discovered devices will belong to the groups and business services defined in the policies.

Note: For all the above configurations, use the **Edit** button to modify any setting or **Delete** to remove any setting.

Grouping Devices by Custom Properties

FortiSIEM allows you to define device groups based on IP address, host name, or device type. You can also group devices based on custom properties. These steps assume that you have already defined the custom properties you are interested in. See Working with Custom Properties.

To group devices by custom properties:

1. In the **CMDB Group Definition** dialog box, click the edit icon next to **Custom Properties**.
2. Click **+** to add a new group definition based on the custom property.
3. Select a custom property from the **Property** drop-down list.
4. Enter a **Value** for the property. You can add multiple values by clicking the **+** button.
5. Click **Save**, then click **Save** again to return to the **CMDB Group Definition** dialog box.
6. In the **Add To** section of the dialog box, select the group to which the CMDB Group will be added from the **Groups** drop-down list.

Monitoring Settings

The following sections describe the procedures for Monitoring settings:

- Important Processes
- Important Ports
- Important Interfaces
- Excluded Disks
- Windows WMI Filter

Important Processes

This setting allows you to always get process resource utilization reports and UP/DOWN alerts on a set of important processes across all device types.

1. Go to **ADMIN** > **Settings** > **Monitoring** > **Important Processes** tab.
2. Click **Enable**.
   This will stop monitoring all processes.
3. Click **New**.
4. Enter a **Process Name**, **Parameter**, and select an **Organization** from the drop-down.
5. Click **Save**.
6. Select the processes from the table and click **Apply**.

FortiSIEM will start monitoring only the selected processes in this tab.

7. If you want to disable this and return to ALL process monitoring, then click **Disable**.

Important Ports

This setting allows you to get TCP/UDP port UP/DOWN status only for a set of important critical ports. Always reporting UP/DOWN status for every TCP/UDP port on every server can consume a significant amount of resources. A port's UP/DOWN status is reported only if the port belongs to this list defined here.

Matching is exact based on port number and IP protocol.

1. Go to **ADMIN** > **Settings** > **Monitoring** > **Important Ports** tab.
2. Click **New**.
3. Enter the **Port Number** and select the **Port Type** and **Organization** from the drop-down.
4. Click **Save**.
5. Select the new ports from the list and click **Apply**.

Important Interfaces

This setting allows you to always get interface utilization reports on a set of important network interfaces across all device types.

1. Create a list of all Important interfaces.
2. Go to **ADMIN** > **Settings** > **Monitoring** > **Important Interfaces** tab.
3. Click **Enable**.
   This will stop monitoring all interfaces.
4. Click the icon left to search field to select either **Show Device Table** or **Show Interface only**.
5. Click **Select** to add the selected interface to the list. The **Critical** and **Monitor** columns will be automatically checked.
6. Check the WAN box if applicable. If checked, the interface utilization events will have the `isWAN = "yes"` attribute.
   You can use this to run a report for all WAN interfaces.
7. Select the interfaces from the table and click **Apply**.
   FortiSIEM will start monitoring only the selected interfaces in this tab.
8. If you want to disable this and return to ALL process monitoring, click **Disable**.

By default, this feature is disabled regardless of whether it is upgraded or newly installed. If this feature is disabled, FortiSIEM monitors all interface util and up/down events. The `isHostIntfCritical` attribute will be set to false for all interfaces. Only non-critical interface staying down rule may trigger. Critical interface staying down rule will have no chance to trigger. If this feature is enabled, there are two check boxes - monitor and critical. If critical is checked, monitor will be checked automatically. Monitor controls whether we must generate interface util event. We monitor interface utils events for interface whose monitor check box is selected. Critical controls whether we must generate interface up/down events. FortiSIEM monitors interface up/down events for an interface whose critical check box is selected. If one interface is marked as critical, we set the attribute of `isHostIntfCritical` to true in the generated interface util and up/down events. The Rule “critical interface staying down” will trigger on interfaces whose `isHostIntfCritical` is true. Non-critical interface staying down rule will have no chance to trigger.

Excluded Disks

This setting allows you to exclude disks from disk capacity utilization monitoring. Disk capacity utilization events will not be generated for devices matching device name, access IP and disk name. Incidents will not trigger for these events, and the disks will not show up in summary dashboards. Use this list to exclude read only disk volumes or partitions that do not grow in size and are close to full.

1. Go to **ADMIN** > **Settings** > **Monitoring** > **Excluded Disks** tab.
2. Click **New**.
3. From the **Choose Disk** dialog box, select the device from the device group.
4. Click **Select**.
5. Select the device from the table and click **Apply**.

Windows WMI Filter

Windows can produce a very high number of system, application, and security logs. The system provides a default filter, **Get All Logs**, which returns all of the Windows logs detected. By defining a filter, you can obtain only the logs you need.

Step 1: Create the Windows WMI Filter

1. Go to **ADMIN** > **Settings** > **Monitoring** > **Windows WMI Filter** tab.
2. Click **New**.
3. Enter a name and an optional description for the filter in the New WMI Filter dialog box.
4. Click **New** to define a filter for the template:
   a. From the **Type** drop-down list, select **Application**, **Security**, or **System**.
   b. In the **Include** and **Exclude** fields, enter a comma-separated list of the event codes which should be included or excluded from the filter.
   c. Click **Save**.
5. Click **Save** again to save the Windows WMI filter.

Step 2: Apply the Filter in a Credential

1. Go to **ADMIN > Setup > Credentials**.
2. Click **New** in **Step 1: Enter Credentials**.
   a. In the Access Method Definition dialog box, select one of the Microsoft devices from the **Device Type** drop-down list.
   b. From the **Access Protocol** drop-down list, select **WMI**.
   c. From the **WMI Filter** drop-down list, select the filter created in Step 1: Create the Windows WMI Filter.
   d. Enter any other required information for the credential. For more information, see Setting Credentials.
   e. Click **Save**.
3. Click **New** in **Step 2: Enter the IP Range for Credential**.
   a. In the Device Credential Mapping Definition dialog box, enter an IP or IP range.
   b. From the **Credentials** drop-down list, select the filter created in Step 1: Create the Windows WMI Filter.
      For more information, see Associating a credential to IP ranges or hosts.
   c. Click **Save**.

Step 3: Discover Using the WMI Credential in Step 2

Any Windows Server discovery that uses that a WMI credential will only pull the logs specified in the Filter in Step 1.

Event Handling Settings

This section provides the procedures to configure Event Handling.

- Event Dropping
- Event Forwarding
- Event Organization Mapping
- Multiline Syslog

Event Dropping

Some devices and applications generate a significant number of logs, which may be very verbose, contain little valuable information, and consume storage resources. You can configure Event Dropping rules that will drop events just after they have been received by FortiSIEM, preventing these event logs from being collected and processed. Implementing these rules may require some thought to accurately set the event type, reporting device, and event regular expression match, for example. However, dropped events do not count towards licensed Events per Second (EPS), and are not stored in the Event database. Dropped events also do not appear in reports, and do not trigger rules. You can also specify that events should be dropped but stored, so event information will be available for searches and reports, but will not trigger rules. An example of an event type that you might want to store but not have trigger any rules would be an IPS event that is a false positive.

1. Go to **ADMIN** > **Settings** > **Event Handling** > **Dropping** tab.
2. Click **New**.
3. Deselect **All** and click the drop-down next to **Reporting Device** and browse the folders to select the device group or individual devices for which you must create a rule.
4. Click **Save**.
5. Deselect **All** and click the drop-down next to **Event Type** and browse the folders to find the group of event types, or a specific event type for which you must create a rule.
6. Click **Save**.
7. Enter **Source IP** or **Destination IP** that you want to filter. The value can be IP range.
8. Select the **Action** that should be taken when the event dropping rule is triggered from the available options.
   - Drop event - Event is dropped and not counted towards licensed EPS.
   - Store event - Event is stored and counted towards licensed EPS
     - Do not trigger rules - this means that FortiSIEM will store events, but will not trigger rules. Events are available for reporting.
     - Drop attributes - to select the attributes to drop, click the edit icon. In the **Event Dropping Rule > Drop Attribute** window, from the left pane, select the attribute(s) you want dropped and click the **>** icon. Dropped attributes appear in the **Selected Attributes** column. When done, click **Save**. Only attributes in the left pane are stored. Stored event attributes are available for reporting.
       Note: You can move dropped attributes so they are stored attributes by selecting them from the **Selected Attributes** column and clicking the **<** icon. When done, click **Save**.
9. For **Regex Filter**, enter any regular expressions you want to use to filter the log files.
   If any matches are made against your regular expression, then the event will be dropped.

10. Enter any **Description** for the rule.
11. Click **Save**.

Notes:

- All matching rules are implemented by FortiSIEM, and inter-rule order is not important. If you create a duplicate of an event dropping rule, the first rule is in effect.
- If you leave a rule definition field blank, then that field is not evaluated. For example, leaving **Event Type** blank is the same as selecting **All Event Types**.
- FortiSIEM drops the event at the first entry point. If your deployment uses Collectors, events are dropped by the Collectors. If your deployment doesn't use Collectors, then the event will be dropped by the Worker or Supervisor where the event is received.
- You can use the report System Event Processing Statistics to view the statistics for dropped events. When you run the report, select AVG(Policy Dropped Event Rate (/sec) as one of the dimensions for Chart to see events that have been dropped to this policy.

Event Forwarding

In systems management, many servers may need access to forward logs, traps and Netflows from network devices and servers, but it is often resource intensive for network devices and servers to forward logs, traps and Netflows to multiple destinations. For example, most Cisco routers can forward Netflow to two locations at most. However, FortiSIEM can forward/relay specific logs, traps and Netflows to one or more destinations. A Super, Worker or Collector can forward events - the one which receives and parses the event forwards it. If you want to send a log to multiple destinations, you can send it to FortiSIEM, which will use an event forwarding rule to send it to the desired locations. If you only want the workers (or super) to forward events, after this configuration, see Event Forwarding by Worker.

1. Go to **ADMIN** > **Settings** > **Event Handling** > **Forwarding** tab.
2. Click **New**.
3. Select the **Organization** for which the rule will apply.
4. Click the drop-down next to **Reporting Device** and browse the folders to find the group of devices, or a specific device for which you must create a rule.
5. Click the drop-down next to **Event Type** and browse the folders to find the group of event types, or a specific event type for which you must create a rule.
6. Click **Save**.
7. Select the **Traffic Type** to which the rule should apply.
8. For **Source IP**, enter the IP address of the device that will be sending the logs.
9. For **Destination IP**, enter the IP address of the device to which the logs are sent.
10. For **Severity**, select an operator and enter a severity level that must match for the log to be forwarded.
11. For **Regex Filter**, enter any regular expressions you want to use to filter the log files.
    If any matches are made against your regular expression, then the event will be forwarded.
12. Select the forwarding **Protocol** from the drop-down.
    - **UDP** - If you use this protocol, events may be lost.
    - **TCP** - This method ensures reliability.
    - **TCP over SSL** - This method ensures reliability and security. See Note 3 below.

13. Based on your selection of **Traffic Type**, enter the following information:
    1. Enter the **IP** address in **Forward to** > **IP**.
    2. Select the **Port** number in **Forward to** > **Port** field.
    3. Select a **Forward to** > **Protocol** from the drop-down list.
    4. Select the **Forward to** > **Format**:
       - **Incoming** - outgoing format is same as incoming.
       - **CEF** - outgoing events are CEF formatted. See here for details on CEF formatted logs.
14. Click **Save**.

Notes:

1. If you want the same sender IP to forward events to multiple destinations, create a rule for each destination.
2. FortiSIEM will implement all rules that you create and enable, so if you create a duplicate of an event forwarding rule, two copies of the same log will be sent to the destination IP.
3. If you want to use public CA certificates for TCP over SSL communication, then note the following:
   - FortiSIEM's SSL library can validate an external system’s certificate if it is signed by a public CA.
   - If the external system wants to verify the FortiSIEM node's certificate, then you need to add the following certificate and key to the `phoenix_config.txt` file of the FortiSIEM nodes forwarding the event.

     ```
     [BEGIN phEventForwarder]
     tls_certificate_file= #/opt/phoenix/bin/.ssh/my_cert.crt
     …
     tls_key_file= #/opt/phoenix/bin/.ssh/my_cert.key
     [END]
     ```

Event Forwarding by Worker

There may be situations where you may not want to forward events from collectors to your target device. Fortinet allows you to forward events when workers (or super) receives collector event information. To configure this, go to **ADMIN** > **Settings** > **Event Handling** > **Forwarding** tab, and add a checkmark to the **Forward From Worker** checkbox. If there is more than one collector per org, this feature will forward events by workers for all collectors.

Event Organization Mapping

FortiSIEM can handle multi-tenant reporting devices that already have Organization names in the events they send, for example, VDOM attribute in FortiGate. This section shows how to map Organization names in external events to those in FortiSIEM. FortiSIEM will create a separate reporting device in each Organization and associate the events to the reporting device in the corresponding FortiSIEM Organization.

This feature requires that:

- One or more (multi-tenant) Collectors are created under Super-Local Organization.
- Multi-tenant devices send logs to the multi-tenant Collectors under Super-Local Organization.

Follow the steps below:

1. Go to **ADMIN** > **Settings** > **Event Handling** > **Event Org Mapping** tab.
2. Click **New**.
3. Select or search the **Device Type** of the sender from the drop-down.
   This has to be a device that FortiSIEM understands and able to parse events.

4. Select or search the **Event Attribute** that contains the external organization name from the drop-down. FortiSIEM will map the value in this field to the FortiSIEM Organization.
5. Select or search the multi-tenant **Collectors** under Super-Local Organization that will receive the events from the drop-down.
   To include all Collectors, select **All Collectors**.
6. Specify the **IP/IP Range** of the multi-tenant devices that are sending events.
   Only a single IP or an IP Range is allowed, for example, 10.1.1.1 or 10.1.1.1-10.1.1.2. Comma-separated values, such as 10.1.1.1,10.1.1.2, are not allowed.
7. Click the edit icon next to **Org Mapping** to map an organization to an event.
   - Click on any **Event Organization** cell in the **Event Organization Mapping** dialog box to edit. Click **Save**.
8. Click **Save**.

Note: Do not define overlapping rules - make sure there are no overlaps in (Collector, Reporting IP/Range, Event Attribute) between multiple rules.

Multiline Syslog

Often applications generate a single syslog in multiple lines. For analysis purposes, the multiple lines must be put together into a single log. This feature enables you to do that. User can write multiple multiline syslog combining rules based on reporting IP and begin and ending patterns. All matching syslog within the begin and ending pattern are combined into a single log.

1. Go to **ADMIN** > **Settings** > **Event Handling** > **Multiline Syslog** tab.
2. Click **New**.
3. Enter or select the following information:
   a. **Organization** - syslog from devices belonging to this Organization will be combined to one line.
   b. **Sender IP** - the source of the syslog. Format is a single IP, IP range, CIDR and a combination of the above separated by comma.
   c. **Protocol** - TCP or UDP since syslog can come via either of these protocols.
   d. **Begin Pattern** - combining syslog starts when the regular expression specified here is encountered.
   e. **End Pattern** - combining syslog stops when the regular expression specified here is encountered.
4. Click **Save**.

Note: For all the above configurations, use the **Edit** button to modify any setting or **Delete** to remove any setting.

The current conception is only for UDP, which is different from TCP. If a single event is sent by multiple UDP packets, you need a multiline rule to combine them. Otherwise, FortiSIEM treats them as multiple events. If a continuous TCP stream contains multiple events, you need a multiline rule to separate them. Otherwise, FortiSIEM treats LF (new line character \n) as the separator.

Database Settings

The following sections provide more information about the Database settings:

Creating Retention Policy

The life cycle of an event in FortiSIEM begins in the *Online* event database, before moving to the *Archive* data store. Online event data resides on faster, but expensive storage. Archive data resides on relatively slower, cheaper and higher capacity storage. You can set up retention policies to specify which events are retained, and for how long, in the online and archive event databases.

- ClickHouse Event Retention
  - How ClickHouse Event Retention Works
  - Creating ClickHouse Event Retention Policy
  - Creating ClickHouse Archive Event Retention Policy for EventDB on NFS
- FortiSIEM EventDB Event Retention
  - How EventDB Event Retention Works
  - Creating EventDB Online Event Retention Policy
  - Creating EventDB Archive Event Retention Policy
- Elasticsearch Event Retention
  - How Elasticsearch Event Retention Works
  - Configuring Elasticsearch Retention Threshold
  - Configuring HDFS Archive Threshold
  - Creating Elasticsearch Archive Event Retention Policy

ClickHouse Event Retention

This section covers how events retention is managed for ClickHouse based deployments. The deployment possibilities are provided in the following table.

FortiSIEM Deployment	Online Storage	Archive Storage
Non-AWS	Hot and Warm and Cold tiers	Real time archive on NFS. Note that Cold tier with large disks may suffice for Archive.
AWS	Hot and Warm and Cold tiers	AWS S3

How ClickHouse Event Retention Works

Case 1: Regular non-AWS Deployments

An example is on-premise ClickHouse deployment, where online data is stored in ClickHouse Hot/Warm/Cold tiers, with multiple disks in each tier. In many cases, Cold tier can serve for archiving old events. If this is not sufficient, then you can add an Archive storage on NFS where events are stored in EventDB format. For NFS based Archive storage, events are copied from FortiSIEM to NFS in real time, as events arrive.

Online Storage Management

Online storage includes events stored in ClickHouse Hot/Warm/Cold tiers. For Online storage, event retention is managed using two mechanisms: Space based Retention and Time based Retention.

- **Space based Retention**:
  - If free Hot tier disk utilization is less than 10%:
    - If Warm tier is defined, then events are moved from Hot tier to the Warm tier until free Hot tier disk utilization is more than 20%.
    - If Warm tier is not defined, then those events are purged.
  - If free Warm tier disk utilization is less than 10%:
    - If Cold tier is defined, then events are moved from the Warm tier to the Cold tier until free Warm tier disk utilization is more than 20%.
    - If Cold tier is not defined, then those events are purged.

  When events are moved or purged, FortiSIEM goes through each ClickHouse event retention bucket (90 days, 180 days, ...) and moves or deletes the *oldest* events within each bucket in a *round robin manner*. All retention buckets are treated uniformly. An example of event movement/purging is as follows.

  Suppose in Hot tier, there are two retention buckets containing events for the following days: Day D1 is the earliest while Day D6 is the latest.

  90 day bucket - days D1, D2, D3, D4, D5, D6

  180 day bucket - days D3, D4, D5, D6

  If the free Hot tier disk utilization goes below 10% on Day D6, then the events (to move or purge) are chosen in the following order, until free Hot tier disk utilization reaches 20%:

  1. 90 day bucket day D1
  2. 180 day bucket day D3
  3. 90 day bucket day D2
  4. 180 day bucket day D4
  5. 90 day bucket day D3
  6. 180 day bucket day D5 ...
- **Time based Retention**: You can specify Online event retention policies to specify the duration for which certain events need to be retained. The policies can take event attributes such as Organization, Reporting Device and Event Type as input. See Creating Online Event Retention Policy. During the retention period, the events can be in Hot or Warm storage depending on the Space based retention, e.g., if Hot tier becomes full, then the event may move to Warm tier, etc... After the retention period expires, these events are purged from Online storage. If you do not have sufficient disk space for the event retention policies, then Space based retention policies kick in and may purge the data, to make room for FortiSIEM to store new events.
  Note: When adding a new retention policy, ensure that there is sufficient disk space to meet the retention policy requirements, or else data may be purged before retention time.

Archive Storage Management

If you define Archive storage, then events are copied in real-time to Archive storage and stored in FortiSIEM EventDB format. This storage is not maintained by ClickHouse. Events can stay in both Online and Archive storage, and their retention is managed independently.

- **Space based Retention**: If free Archive disk utilization is less than 10GB, then *oldest* events are purged until free Archive disk utilization is more than 20GB. These parameters are defined in the `phoenix_config.txt` file.
- **Organization based Retention**: You can write Archive retention policies to specify the duration for which events for each Organization need to be retained. See Creating Archive Event Retention Policy.

Case 2: AWS Deployments

For AWS deployments, you can define S3 as the Archive storage. ClickHouse manages both the Online Hot/Warm/Cold disks and Archive S3 storage.

- **Space based Retention**:
  - If free Hot tier disk utilization is less than 10%:
    - If Warm tier is defined, then events are moved from Hot tier to the Warm tier until free Hot tier disk utilization is more than 20%.
    - If Warm tier is not defined, but S3 Archive is defined, then those events are moved from Hot tier to S3 Archive until free Hot tier disk utilization is more than 20%.
    - If neither Warm tier nor S3 Archive is defined, then those events are purged.
  - If free Warm tier disk utilization is less than 10%:
    - If Cold tier is defined, then events are moved from Warm tier to Cold tier until free Warm tier disk utilization is more than 20%.
    - If Cold tier is not defined, but S3 Archive is defined, then those events are moved from Warm tier to S3 Archive until free Warm tier disk utilization is more than 20%.
    - If neither Cold tier nor S3 Archive is defined, then those events are purged.

  When events are moved or purged, FortiSIEM goes through each retention bucket (90 days, 180 days, ...) and moves/removes the *oldest* events within each bucket in a *round robin manner*. All retention buckets are treated uniformly. An example of event movement/purging is as follows.

  Suppose in Hot tier, there are two retention buckets containing events for the following days where Day D1 is earliest and day D6 is the latest.

  90 day bucket - days D1, D2, D3, D4, D5, D6

  180 day bucket - days D3, D4, D5, D6

  If the free Hot tier disk utilization is less than 10%, then the events to move or purge, are chosen in the following order, until free Hot tier disk utilization reaches 20%:

  1. 90 day bucket day D1
  2. 180 day bucket day D3
  3. 90 day bucket day D2
  4. 180 day bucket day D4
  5. 90 day bucket day D3
  6. 180 day bucket day D5 ...
- **Time based Retention**: You can specify Online event retention policies to specify the duration for which certain events need to be retained. The policies can take event attributes such as Organization, reporting Device and Event Type as input. See Creating Online Event Retention Policy. During the retention period, the events can be in Hot or Warm or Archive storage depending on the Space based retention, e.g., if Hot tier becomes full, then the event may move to Warm tier, etc... After the retention period expires, these events are purged from ClickHouse Online storage and S3 Archive.
  Note: When adding a new retention policy, ensure that there is sufficient disk space to meet the retention policy requirements, or else data may be purged before retention time.

Creating ClickHouse Event Retention Policy

Online event retention policies specify which events are retained, and for how long, in the online event database. Take the following steps to create an Online Event retention policy for ClickHouse.

1. Go to **ADMIN > Settings > Database > Retention Policy**.
2. Under **Online Retention Policy**, click **New**.
3. Select **Enabled** if the policy has to be enforced immediately.
4. Choose the **Organizations** for which the policy must be applied (for service provider installations). Select **All** if it should apply to all organizations.
5. Choose the **Reporting Devices** to apply this policy using the edit icon and click **Save**.
6. Choose the **Event Type** or event type groups to apply this policy and click **Save**.
7. Select the **Retention Period** from the drop-down list (3 Months, 6 Months, 1 Year, 3 Years, 5 Years, 10 Years, Forever (50 Years). Each month is 30 days.
8. Enter any **Description** related to the policy.
9. Click **Save**.
10. When done, click **Apply**.

Implementation Notes:

1. Any time the retention policy on ClickHouse environment is changed, you must click **Apply** to push the retention policy.
2. Retention policies are evaluated based on Rank. A lower rank policy is evaluated first and first match is applied.
3. All events matching a retention policy are retained for the duration specified by the **Retention Period** specified in the policy.
4. For the events that do not match with any existing retention policy, the default value for Retention Days is 18, 250 (50 years)

Creating ClickHouse Archive Event Retention Policy for EventDB on NFS

These policies specify which events are retained, and for how long, when EventDB on NFS is used to archive.

1. Go to **ADMIN > Settings > Database > Retention Policy**.
2. Under **Offline Retention Policy**, click **New** to create a new policy.
3. Select the **Organization** this policy applies to.
4. Enter the **Time Period** in days for archive retention.
5. Click **Save**.

Implementation Notes:

1. Policies are enforced only at the end of the day.
2. FortiSIEM will attempt to retain the events in the archive according to the policies. However, if the low storage threshold is hit (10GB, by default), then the events which occurred earliest in the day are purged.

FortiSIEM EventDB Event Retention

This section covers how events retention is managed for EventDB based deployments.

How EventDB Event Retention Works

For Online storage, event retention is managed using two mechanisms:

- **Space based retention**: If free online disk utilization is less than 10GB, then oldest events are moved to the Archive until free online disk utilization is more than 20GB. If Archive is not defined, then those events are purged.

- **Policy based retention**: You can specify Online event retention policies to specify the duration for which certain events need to be retained in online storage. The policies can take event attributes such as Organization, Reporting Device and Event Type as input. See Creating Online Event Retention Policy. If an event has remained in the online EventDB for the time period in the event retention policy, then the event is moved to the Archive at the end of the day.

For Archive storage, event retention is managed using two mechanisms:

- **Space based retention**: If free archive disk utilization is less than 10GB, then oldest events are purged until free online disk utilization is more than 20GB.
- **Policy based retention**: You can specify Archive event retention policies to specify the duration for specific Organizations. See Creating Archive Event Retention Policy. If an event has remained in the archive EventDB for the time period in the event retention policy, then the event is purged at the end of the day.

Creating EventDB Online Event Retention Policy

1. Go to **ADMIN > Settings > Database > Retention Policy**.
2. Under **Online Retention Policy**, click **New**.
3. Select **Enabled** if the policy needs to be applied.
4. Choose the **Organizations** for which the policy must be applied (for service provider installations). Select **All** if it should apply to all organizations.
5. Choose the **Reporting Devices** to apply this policy using the edit icon and click **Save**. If all reporting devices should be applied, check the **All** checkbox.
6. Choose the **Event Type** or event type groups to apply this policy and click **Save**. If all event types should be applied, check the **All** checkbox.
7. Enter or select the **Time Period** in days that the event data specified by the conditions (Organizations, Reporting Devices and Event Type) should be held in the online storage before it is moved to archive or purged.
8. Enter any **Description** related to the policy.
9. Click **Save**.

Implementation Notes:

- If an event has remained in the online event database for the time period in the event retention policy, then the event is moved to the archive at the end of the day.
- If an event does not match any online event retention policy, then it remains in the online event database until the low storage threshold (10GB, by default) is reached. The event is then moved to the archive.
- If the archive mount point is defined, then ALL events are moved from online to archive. Nothing is purged.
- If the archive is not reachable after multiple retries, then FortiSIEM is forced to purge the event because there is nowhere to store the event.
- FortiSIEM will attempt to retain the events in the online event database according to the policies. However, if the low storage threshold is hit (10GB, by default), then the events from the earliest day are moved to archive.
- Implementing an online event policy requires selectively deleting specific events from the database and then re-indexing the database for the affected days. This is expensive in terms of time and performance. Therefore, do not define excessively fine-grained retention policies, because this will affect database performance.
- Policies are enforced only at the end of day – this means that events are deleted and re-indexed only at the end of the day. This minimizes the impact on database performance because the database usage should be low at that time.

- Policies are enforced by FortiSIEM only from the date just before the retention period. For example, if the retention period for a policy is 10 days, and today is 12/19/2022, then FortiSIEM will automatically enforce the policy for events with event receive time starting from 12/18/2022. For processing older dates, Fortinet recommends customers to use the `EnforceRetentionPolicy` tool as follows:
  - `EnforceRetentionPolicy <`*`DATES`*`>`, where *DATES* is a comma-separated list of dates or date-range on which to enforce the policy. *DATES* is specified as the number of days since the UNIX epoch began: 1970-01-01. A date-range can specified by two dates inclusively separated by "-".
    For example, run the command `EnforceRetentionPolicy 16230,16233-16235` to enforce retention policies on these dates: 6/8/2014 and from 6/11/2014 to 6/13/2014.
  - Run the tool as admin user.

Creating EventDB Archive Event Retention Policy

These policies specify which events are retained, and for how long, in the archive.

1. Go to **ADMIN > Settings > Database > Retention Policy**.
2. Under **Offline Retention Policy**, click **New** to create a new policy.
3. Select the **Organization** this policy applies to.
4. Enter the **Time Period** in days for archive retention.
5. Click **Save**.

Implementation Notes:

1. Policies are enforced only at the end of the day.
2. If an event has remained in the archive for the duration specified in the event retention policy, then the event is purged at the end of the day.

Elasticsearch Event Retention

This section covers how events retention is managed for Elasticsearch based deployments. The deployment possibilities are:

FortiSIEM Deployment	Online Storage	Archive Storage
On-premises Elasticsearch – Option 1	Hot and Warm tiers	HDFS archive from Elasticsearch
On-premises Elasticsearch – Option 2	Hot and Warm tiers	Real-time HDFS archive from FortiSIEM
On-premises Elasticsearch – Option 3	Hot and Warm tiers	Real-time Archive to NFS
Elastic Cloud and AWS Elasticsearch	Hot and Warm tiers	Not available

How Elasticsearch Event Retention Works

Elasticsearch online events storage is managed by the following thresholds:

- **Hot Node**
  - **Free Space Threshold**: When the Hot node cluster disk free space falls below **Low Threshold**, then events are moved to Warm nodes until the Hot node cluster disk free space reaches **High Threshold**. If Warm node is not defined, then events are Archived. If Archive is not defined or real time archive option is chosen, then events are purged.

  - **Age Limit**: Maximum number of days after which events are moved to Warm nodes. If Warm node is not defined, then events are Archived. If Archive is not defined or real time archive option is chosen, then events are purged.
- **Warm Node**
  - **Free Space Threshold**: When the Warm node cluster disk free space falls below **Low Threshold**, then events are Archived. If Archive is not defined or real time archive option is chosen, then events are purged.
  - **Age Limit**: Maximum number of days after which events are moved to Archive. If Archive is not defined or real time archive option is chosen, then events are purged.

These thresholds are defined in Configuring Elasticsearch Retention Threshold.

For archive you can choose either HDFS or EventDB on NFS.

- **HDFS archive from Elasticsearch**: In this option, FortiSIEM `HDFSMgr` process creates Spark jobs to directly pull events from Elasticsearch and store in HDFS. This option may result in extra load on Elasticsearch as events have to read and then deleted from Elasticsearch while events are getting inserted. In this option, archive disk is managed by threshold, that is when low threshold is reached, then events are purged until the high threshold is reached – see Configuring HDFS Archive Threshold.
- **Real-time HDFS archive from FortiSIEM**: In this option, FortiSIEM `HDFSMgr` process creates Spark jobs to pull events from FortiSIEM Supervisor and Worker nodes. This happens while events are getting inserted into Elasticsearch. This approach has no impact in Elasticsearch performance, but events are stored in both Elasticsearch and HDFS and managed independently. Note that HDFS has better event storage compression properties. In this option, archive disk is managed by threshold, that is when low threshold is reached, then events are purged until the high threshold is reached – see Configuring HDFS Archive Threshold.
- **Real time archive to NFS**: In this option, FortiSIEM Supervisor and Worker nodes store events in NFS managed by FortiSIEM EventDB. This happens while events are getting inserted into Elasticsearch. This approach has no impact in Elasticsearch performance, but events are stored in both Elasticsearch and EventDB and managed independently. Note that EventDB has better event storage compression properties. In this option, archive disk is managed by policies– see Creating Archive Event Retention Policy.

Configuring Elasticsearch Retention Threshold

Complete these steps to configure Native Elasticsearch free space and age retention threshold:

1. Go to **ADMIN > Settings > Database > Online Settings**.
2. Select the low percentage threshold, high percentage threshold, and age under:
   a. Hot Node - Free Space Threshold - Events are moved to Warm nodes based on the first occurrence of one of the following:
      - When the Hot node cluster disk free space falls below Low value, then events are moved to Warm nodes until the Hot node cluster disk free space reaches High value.
      - If the time duration limit set under Hot Age (the Warm age phase) is met, all events under this limit are moved to Warm nodes.

   b. Warm Node - Free Space Threshold - Events are moved to Warm nodes based on the first occurrence of one of the following:
      - When the Warm node cluster disk free space falls below Low value, then events are moved to Cold nodes until the Warm node cluster disk free space reaches High value.
      - If the time duration limit set under Warm Age (the Cold age phase) is met, all events under this limit are moved to Cold nodes.
        Note: In the fsiem_ilm_policy, the cold age phase is reflected as a sum of the warm age phase and cold age phase UI values.

Configuring HDFS Archive Threshold

Complete these steps to configure the HDFS retention threshold:

1. Go to **ADMIN > Settings > Database > Archive Data**.
2. Select the low and high percentage thresholds under **Archive Threshold**. If HDFS disk utilization falls below **Low value**, then events are purged until disk utilization reaches **High value**.

Creating Elasticsearch Archive Event Retention Policy

These policies specify which events are retained, and for how long, in the archive.

1. Go to **ADMIN > Settings > Database > Retention Policy**.
2. Under **Offline Retention Policy**, click **New** to create a new policy.
3. Select the **Organization** this policy applies to.
4. Enter the **Time Period** in days for archive retention.
5. Click **Save**.

Implementation Notes:

1. Policies are enforced only at the end of the day.
2. If an event has remained in the archive for the duration specified in the event retention policy, then the event is purged at the end of the day.

Viewing Online Event Data Usage

Online Event Data Usage enables you to see a summarized view of online event data usage. This view enable you to manage storage more effectively by writing appropriate event dropping policies or online event retention policies.

The Online Event Data Usage is displayed in tree view under **ADMIN** > **Settings** > **Database** > **Online Data** grouped by the year and dates for NFS/Local storage. For Elasticsearch-based deployments, if the storage is set per Organization, the usage is displayed specific to each Organization grouped by year and dates. For Elasticsearch and ClickHouse deployments, you can drill-down from the year to view the usage for any specific date. You can also click on the **Expand All** checkbox to view all the available storage information.

Viewing Archive Event Data

The event database archived data is displayed in tree view grouped by Organization and archive dates.

Note: Events for CustomerId 0 correspond to FortiSIEM internal system events. On the Archive Event Data page, these events are shown under Super/Local.

Complete these steps to view archived data:

1. Go to **ADMIN** > **Settings** > **Database** > **Archive Data**.
2. Search the **Archived Data** by Organization in the search box and drill-down to find the specific data by specific dates from the tree view.

Event Log Integrity

Validating Event Log Integrity for EventDB

Security auditors can validate that archived event data has not been tampered using the **Event Integrity** function of event database management.

Note: This setting is not available for Elasticsearch

Viewing EventDB Event Log Integrity Status

1. Go to **ADMIN** > **Settings** > **Database** > **Event Integrity**.
2. Use the following filters to view the event log integrity:
   a. For a specific time using the **From** and **To** fields.
   b. Based on the status of event integrity using the **Status** drop-down:
      - Not Validated - the event integrity has not been validated yet.
      - Successful - the event integrity has been validated and the return was success. This means that the logs in this file were not altered.
      - Failed - the event integrity has been validated and the return was failed. This means that the logs in this file were altered.
      - Archived - the events in this file were archived to offline storage.
      - Purged - the log event is removed from the log.
      - Restored - the event is restored to the log file.

   The event log integrity table is automatically updated with the applied filters.

Columns	Description
Start Time	The earliest time of the messages in this file. The file does not contain messages that were received by FortiSIEM before this time.
End Time	The latest time of the messages in this file. The file does not contain messages that were received by FortiSIEM after this time.
Category	• **Internal**: these messages were generated by FortiSIEM for its own use.

Columns	Description
	This includes FortiSIEM system logs and monitoring events such as the ones that begin with `PH_DEV_MON`. • **External**: these messages were received by FortiSIEM from an external system. • **Incident**: these corresponds to incidents generated by FortiSIEM.
File Name	Name of the log file.
Events	Number of events in the file.
Algorithm	Checksum algorithm used for computing message integrity.
Checksum	Value of the checksum.
Status	Event log integrity validation status.
Location	File location: • **Local**: Local to Supervisor node. • **External**: means external to Supervisor node, for example, on NFS storage.

Validating EventDB Event Log Integrity

1. Go to **ADMIN** > **Settings** > **Database** > **Event Integrity**.
2. To validate the event log integrity of:
   a. Single event log - select the event log and click **Validate**.
   b. Multiple event logs - use **Ctrl**/**Command** keys to select the event logs and click **Validate**.
   c. All logs at a time - click **Validate All**.

The validation **Status** of the event log(s) will be updated in the list. The Validation History of any selected event log can be viewed under **Action** > **Validation History**.

Exporting EventDB Event Log Integrity Status

1. Go to **ADMIN** > **Settings** > **Database** > **Event Integrity**.
2. To generate and download the file in PDF or CSV format, select the event log from the list and click **Export**. Use **Ctrl**/**Command** keys to select multiple event logs.

Validating Event Log Integrity for ClickHouse

Security auditors can validate that archived event data has not been tampered using the **Event Integrity** function of event database management.

Note: This setting is not available for Elasticsearch

Viewing ClickHouse Event Log Integrity Status

1. Go to **ADMIN** > **Settings** > **Database** > **Event Integrity**.
2. Use the following filters to view the event log integrity:
   a. For a specific time using the **From** and **To** fields.
   b. Based on the status of event integrity using the **Show** drop-down:
      - All - All events are shown.
      - Not Validated - the event integrity has not been validated yet.
      - Success - the event integrity has been validated and the return was success. This means that the logs in this file were not altered.
      - Failure - the event integrity has been validated and the return was failed. This means that the logs in this file were altered.
      - Not Found - the log event has been removed or detached.

   The event log integrity table is automatically updated with the applied filters.

Columns	Description
Start Time	The earliest time of the messages in this file. The file does not contain messages that were received by FortiSIEM before this time.
End Time	The latest time of the messages in this file. The file does not contain messages that were received by FortiSIEM after this time.
Shard	The ID of the shard.
Partition ID	The partition ID of the shard.
Partition Name	The partition or "directory" name for ClickHouse logs. Hover the cursor over the name to display the full directory path and name. **Note**: If ClickHouse is unable to consolidate the event data, such as if there is not enough storage space, the **Partition Name** and **Validation Status** will appear blank.
Validation Status	Event log integrity validation status. The following messages may appear: Success - checksum match verified. Failure - checksum match failure.

Columns	Description
	Not Found - partition issue occurred. System Error - shell command or parsing error.
Checksum	Value of the checksum.

Validating ClickHouse Event Log Integrity

1. Go to **ADMIN** > **Settings** > **Database** > **Event Integrity**.
2. To validate the event log integrity of:
   a. Single event log - select the event log and click **Validate**.
   b. Multiple event logs - use **Ctrl**/**Command** keys to select the event logs and click **Validate**.
   c. All logs at a time - click **Validate All**.

The **Validation Status** of the event log(s) will be updated in the list.

Automating ClickHouse Log Integrity

1. Go to **ADMIN** > **Settings** > **Database** > **Event Integrity**.
2. From the **Event Integrity** drop-down list select **On** or **Off**.

When **Event Integrity** is **On**, a ClickHouse log integrity check occurs at the time it consolidates its data. As this is resource intensive, it is off by default.

ClickHouse Configuration

This section covers how to configure a ClickHouse topology of Keeper and Data/Query nodes.

Before beginning, make sure that:

1. You have gone through ClickHouse Operation Overview and the ClickHouse Sizing Guide, located in the FortiSIEM Documentation Library.
2. You have identified the FortiSIEM nodes that are going to be ClickHouse Keeper nodes and ClickHouse Data nodes.
3. You have configured appropriate disks on the FortiSIEM nodes appropriate for their role.

Take the following steps.

1. Navigate to **ADMIN > Settings > Database > ClickHouse Config**.
2. Configure **ClickHouse Keeper Cluster**.
   a. Click on **+** and add a Worker.
   b. Click on **-** to remove a Worker.
   c. An operation for a ClickHouse Keeper Cluster node, such as adding or removing a node, MUST be done individually, meaning that after an operation is done, a test and deploy action must be performed. For example, if you add a ClickHouse Keeper Cluster node, you must then perform a test and deploy before doing any other operation for another ClickHouse Keeper Cluster node, such as adding another ClickHouse Keeper Cluster node, or removing a ClickHouse Keeper Cluster node. Do NOT perform

more than one operation, such as adding or removing a ClickHouse Keeper Cluster node without testing and deploying it, as doing so may cause stability issues.

3. Configure **ClickHouse Server Cluster**. You need to know the number of shards.
   a. Click on **+** and add a shard.
   b. Add Workers to the shard.
      i. Check **Data** if this Worker is a ClickHouse Data Node. A Data node receives events, processes them and writes to ClickHouse database.
      ii. Check **Query** if this Worker is a ClickHouse Query Node. A Query node stores events replicated from data nodes and participates in Queries. However, it does not process events and triggers incidents.
      iii. Check both **Data** and **Query** if this Worker is both a ClickHouse Data and Query Node. This is the most common setup.
4. Once the shards have been created and workers have been added to the shard, then click **Test**.
5. If **Test** succeeds, then click **Deploy** to push the changes to ClickHouse.

Notes:

1. If you made changes to the ClickHouse Keeper Cluster, then after Deploy succeeds, `phClickHouseMonitor`, `ClickHouseKeeper` and `ClickHouseServer` processes will restart.
2. If you made changes to the ClickHouse Cluster, then after Deploy succeeds, `phClickHouseMonitor`, and `ClickHouseServer` processes will restart.

For Advanced Configuration Operations, see Advanced Operations in the Appendix.

Role Settings

FortiSIEM provides performance, availability, and environmental alerts, as well as change and security monitoring for network devices, servers and applications. It is difficult for one admin to monitor across the entire spectrum of available information. In addition, devices may be in widely distributed geographical and administratively disjointed locations. Role-based access control provides a way to partition the FortiSIEM administrative responsibilities across multiple admins.

A role defines two aspects of a user's interaction with the FortiSIEM platform:

- Which user interface elements a user can see and the ability to use the associated Read/Write/Execute permissions. As an example, the built-in Executive role can see only the dashboard, while the Server Admin role cannot see network devices. Role permissions can be defined to the attribute level in which, for example, a Tier1 Network Admin role can see network devices but not their configurations.
- What data can the user see. For example, consider a Windows Admin role and a Unix Admin role. They both can run the same reports, but the Windows admins sees only logs from Windows devices. This definition can also be fine-grained, for example one Windows admin sub-role can be defined to see Windows performance metrics, while another Windows admin sub-role can see Windows authentication logs. The roles described in the following table are default roles.

Role	Permissions
DB Admin	Full access to the database servers part of the GUI and full access to logs from those devices.

Role	Permissions
Executive	View access to the Business Service dashboard and personalized My Dashboard tabs, but reports can be populated by logs from any device.
Full Admin	Full access to the GUI and full access to the data. Only this role can define roles, create users and map users to roles.
Help Desk	Access to the Admin, CMDB, and Dashboard tabs, with view and run permissions for the Analytics and Incidents tabs.
Network Admin	Full access to the network device portion of the GUI and full access to logs from network devices.
Read Only Admin	View access to all tabs and permission to run reports.
Security Admin	Full access to Security aspects of all devices.
Server Admin	Full access to the Server part of the GUI and full access to logs from those devices.
Storage Admin	Full access to the Storage device part of the GUI and full access to logs from those devices.
System Admin	Full access to the Server/Workstation/Storage part of the GUI and full access to logs from those devices.
Unix Server Admin	Full access to the Unix Server part of the GUI and full access to logs from those devices.
Windows Server Admin	Full access to the Windows Server part of the GUI and full access to logs from those devices.

The following sections describe the procedures to create custom roles and privileges:

- Adding a New Role
- Modifying a Role
- Example Role Setup
- Viewing User Roles for AD Group Mappings

Adding a New Role

You can create a new role or use an existing role by selecting an existing role and clicking the **Clone** button.

1. Go to **ADMIN > Settings > Role > Role Management**.
2. Click **New**.
3. Enter a **Role Name** and **Description**.
4. Enter the **Data Conditions** for this role.
   This restricts access to the event/log data that is available to the user, and will be appended to any query that is submitted by users with this role. This applies to both Real-Time and Historical searches, as well as Report and Dashboard information.
5. Enter the **CMDB Report Conditions** for this role. Choose a type from the drop-down list.
   This restricts access to the reports for devices, users, monitors, rule, report, task, identity, incident, audit that are available to the user with this role.
6. Select the appropriate **Approver** capability:
   - Select **De-Obfuscation** if this role can approve De-Obfuscation requests.
   - Select **Report Schedule** if this role can approve Report Schedule Activation requests.
   - Select **Rule Activation/Deactivation** if this role can approve Rule Activation/Deactivation requests.
   - Select **Remediation** if this role can approve Remediation requests. FortiSIEM recommends creating at least two user accounts with the Remediation approver role. See Adding Users for more information on creating a user account.
7. Select the appropriate **Activation** capability:
   - Select **Report Schedule** if this role does NOT require approval for Report Schedule Activation.
   - Select **Rule Activation/Deactivation** if this role does NOT require approval for Rule Activation/Deactivation.
   - Select **Remediation** if this role does NOT require approval for Remediation Activation.
8. Select the **Data Obfuscation** options for this role:
   - **System Event/CMDB Attribtues** to anonymize IP, User and Email, or Host Name in the events.
   - **Custom Event Attributes** to anonymize custom event attributes. Search or click **+** to include multiple attributes. To create a custom event attribute, see Adding an Event Attribute.

   Note: If Data Obfuscation is turned on for a FortiSIEM user:
   - - The value for that object marked for data obfuscation is obfuscated. For example, if IP is marked for data obfuscation, the IP address is obfuscated. In earlier versions of FortiSIEM, raw events were completely obfuscated.
   - CSV Export feature is disabled.

   Note: If Remediation is turned on, the requestor and approver users must have a valid email address, configured in the **Email** field in Contacts, in order for the requestor and approver to receive requests and approval information.
9. Select the **UI Access** conditions for this role.
   This defines the user interface elements that can be accessed by users with this role. By default, the child nodes in the tree inherit the permissions of their immediate parent, however you can override those default permissions by explicitly editing the permission of the child node. The options for these settings are in the **All Nodes** drop-down list:
   - **Full** - No access restrictions.
   - **Edit** - The role can make changes to the UI element.

- **Run** - The role can execute processes for the UI element.
- **View** - The role can only view the UI element.
- **Hide** - The UI element is hidden from the role.

10. Click **Save**.

Hiding Network Segments

If a **Network Segment** is marked as hidden for a user role, users with that role will not be able to see any of the devices whose IP addresses fall within that network segment, even if the CMDB folder(s) containing those devices have not been hidden.

Modifying a Role

Complete these steps to modify a cloned or user defined role. (You cannot directly modify a system defined role):

1. Select the role from the table.
2. Click the required option:
   a. **Edit** to modify any role setting.
   b. **Delete** to remove a role.
   c. **Clone** to duplicate a role.
3. Click **Save**.

Example Role Setup

- Setting Up an Incident Remediation Workflow Example

Setting Up an Incident Remediation Workflow Example

You will need at least one user as an incident remediation approver, and one user as a requester that requires approval for incident remediation. This example assumes you have incident remediation configured.

From here, take the following steps as an admin:

1. Create a role for an incident remediation approver by taking the steps in Add a New Role and ensuring in step 6 that the role can approve incident remediation, which we'll call Approver.
2. Create a user with the Approver role by taking the steps in Adding Users, and ensuring that step 3m is configured correctly, and that a valid email address is provided in step 3n.
   Note: A requester can select multiple approvers when making a request. For real world scenarios, Fortinet recommends creating a minimum of two approvers, in case an approver is unavailable.
3. Create a requester user by taking the steps in Adding Users, and ensuring the following:
   - A non-admin role is assigned in step 3kii.
     Note: By default, a non-admin role requires approval for incident remediation. If you want to create/edit a non-admin role where a user does NOT need to get approval for incident remediation, you would add a checkmark to **Remediation** at **Activation** in step 7 in Add a New Role.
   - A valid email address is provided in step 3n.
4. Log out of FortiSIEM, and log in as the requester user.
5. Navigate to **INCIDENTS > List by Time >** and select an incident.
6. Click on **Actions**, and select **Remediate Incident**.

7. From the **Remediation** drop-down list, select a remediation script and select **Run**. A **Create New Request** window will appear with the message "No permission to run Remediation. Send a permission request."
8. From the **Approver** drop-down list, select the user with the Approver role that you created.
   Note: The user may select multiple approvers in his/her request, not just one.
9. In the **Justification** field, enter any comments and click **Submit**. This request will appear as "pending" in **TASKS**.
10. Log out of FortiSIEM, and log in as the user with the Approver role. As the "Approver" user, you will see a message stating "You have pending requests. Please check Task > Approval.
11. Navigate to **TASKS** and select **Approval** in the left panel.
12. Select the **Request ID** of the request, and review it. You have the choice to "Approve" or "Reject" the request in the drop-down list, next to the **Status** column. In this situation, select "Approve".
    Note: See Approving a de-anonymization request for more information, including how FortiSIEM handles requests when multiple approvers are involved.
13. An **Approve Request** windows appears, prompting for the expiry timeframe. If we want to make the approval window available for two days, you would select **For**, and input "2" for Days, then click **OK**. The **Status** column is updated with this information.
14. Log out of FortiSIEM, and log in as the requester user.
15. The requester user should have received an email from the user with the approver role, with the title "Remediation Request is approved".
16. Navigate to **TASKS**. In the left panel, select **Request**. In the **Status** column, you will see that the request has been approved.
17. Navigate to **INCIDENTS > List by Time >** and select the incident that was approved for remediation.
18. Click on **Actions**, and select **Remediate Incident**.
19. From the **Remediation** drop-down list, select a remediation script and select **Run**. The remediation script now runs.

Viewing User Roles for AD Group Mappings

To see the AD groups that the user is a member of, go to **CMDB > Users > Member Of**.

The User Roles are explicitly shown in **CMDB > Users > Access Control**.

Mapping AD Groups to Roles

FortiSIEM provides the ability to map Microsoft Active Directory (AD) Groups to Roles. A user mapped to more than one Role has permissions for all roles following the Least Restrictive Role principle described below.

Follow these steps to map an AD Group to a Role:

Step 1: Setup or Edit an Authentication Profile

1. Log in to the FortiSIEM system.
2. Follow the instructions in Adding External Authentication Settings to setup a new profile or edit an existing profile. Currently, only LDAPS and LDAPTLS are supported for mapping AD Groups. The new or edited entry appears in the list of authenticated organizations.

Step 2: Create a Role to be Mapped to the AD Group

Follow the instructions in Adding a New Role to add a role that is to be mapped to an AD Group.

Step 3: Assign an AD Group

1. Click **ADMIN > Settings > Role > AD Group Role**.
2. Click **New** to create a new AD Group mapping or select a row and click **Edit** to edit an existing mapping.
3. Provide the following information in the Add AD Group Role popup:
   - **Organization** - Set to System (all organizations can use the information), Super/Local (only Super/Local can use the information).
   - **AD Group DN** - The AD Group domain name. Currently, the server must be either LDAPS or LDAPTLS.
   - **Mapped Role** - Scroll down the list for the role you want to map to. You can find descriptions of the pre-defined roles in Role Settings.
   - **Comment** - Enter an optional comment describing the mapping.

Step 4: Test Your Mappings

Test your mappings by logging out of the FortiSIEM session then logging back in as the LDAPS/LDAPTLS user.

You can use either the CN or the SamAccountName as the Username in FortiSIEM.

The following example account illustrates the options:

```
PS C:\Users\Administrator> Get-ADUser -Identity jdoe

DistinguishedName : CN=J Doe,OU=department1,DC=fortisiem,DC=lab
Enabled : True
GivenName : J
Name : J Doe
ObjectClass : user
ObjectGUID : 2386c3e6-d2c0-47b8-85d0-334585e959f
SamAccountName : jdoe
SID : S-1-5-21-87403157-1919951427-186658781-1620
Surname : Doe
UserPrincipalName : jdoe@fortisiem.lab
```

- Using the CN as the Username, for example:
  ```
  User: J Doe
  Password: ********
  Domain: local
  ```
- Using the SamAccountName as the Username, for example:
  ```
  User: fortisiem\jdoe
  Password: ********
  Domain: local
  ```

Principle of Least Restrictive Role

If a user belongs to two FortiSIEM Roles, then the user will have the rights of BOTH Roles.

- Case 1 - A node is explicitly defined in both role definitions. Then a user belonging to BOTH roles have the union of all permissions for that node. Explicit definitions mean that the node appears in the bottom **Restrictions** area when you view the Role in **Settings > Role > Role Management**. Some examples:
  One Role has READ permission on the **RESOURCES** tab, while the other Role has WRITE and EXECUTE permissions on **RESOURCES** tab. Then, a user belonging to BOTH roles has READ, WRITE, EXECUTE on **RESOURCES** tab.

One Role has READ permission on the **RESOURCES** tab, while the **RESOURCES** tab is hidden in the other Role. Then, a user belonging to BOTH roles has READ permission on the **RESOURCES** tab.

- Case 2 - A node is not explicitly defined in one Role but explicitly defined in the other role. Then the user belonging to BOTH roles have the explicit permission defined in the second role. For example, a Full Admin role has nothing explicitly defined, because it has full permission on ALL nodes. If the user belongs to both Full Admin role and another role that can only READ the CMDB tab, then the user has only READ permission on the CMDB tab.
- Case 3 - A node is not explicitly defined in two Roles. Then the user belonging to BOTH roles has full permission on that node.

Compliance Settings

The following sections provide more information about the Compliance settings:

PCI Compliance Policy

This screen allows you to view, create, edit, or delete payment card industry (PCI) logging policies.

- Viewing PCI Policies
- Adding a PCI Logging Policy
- Editing a PCI Logging Policy
- Deleting a PCI Logging Policy

Viewing PCI Policies

The PCI table shows the following PCI attribute information.

PCI Logging Attribute	Description
Device Group Name	The name of the device group with a PCI logging policy.
Authentication	Provides information on last authentication event, if enabled.
FIM	Provides information on last file integrity monitoring (FIM) event, if enabled.
Change	Provides information on when the last change occurred, if enabled.

Adding a PCI Logging Policy

You can create a new PCI logging policy by taking the following steps:

1. From **ADMIN > Settings > Compliance > PCI**, click **New**.
2. From the **Device Group Name** drop-down list, select a device group.
3. Enable your preferred options by checking the appropriate checkboxes. When an option is selected, from the drop-down list, select the report you want the information to be generated from.
   a. Need Authentication
   b. Need FIM
   c. Need Change
4. Click **Save** when done.

Editing a PCI Logging Policy

You can edit a PCI logging policy by taking the following steps:

1. From **ADMIN > Settings > Compliance > PCI**, select an existing policy and click **Edit**.
2. Make any changes to your existing PCI logging policy, and click **Save** when done.

Deleting a PCI Logging Policy

You can delete a PCI logging policy by taking the following steps:

1. From **ADMIN > Settings > Compliance > PCI**, select an existing policy and click **Delete**.
2. Click **Yes** to confirm.

General Settings

- External Authentication Settings
- Incident Notification Settings
- External System Integration Settings
- Escalation Settings
- Mapping AD Groups to Roles
- Configuring SSL Socket Certificates
- Cloud Machine Learning

External Authentication Settings

The following section specifies how to configure external authentication for users in FortiSIEM CMDB.

- Configure Users for External Authentication
- Configure Users for Generic SAML Authentication
- Configure Users for SAML Authentication with Azure AD
- Authenticating Users Against FortiAuthenticator (FAC)
- Add 2-Factor Authentication Option for FortiSIEM Users
- Appendix

Configure Users for External Authentication

- Step 1: Create External Authentication Profile
- Step 2: Configure User for External Authentication

Step 1: Create External Authentication Profile

An external authentication profile can be created for the following protocols:

- LDAP/LDAPS/LDAPTLS External Authentication Profile
- RADIUS External Authentication Profile
- Okta External Authentication Profile
- Duo External Authentication Profile
- SAML External Authentication Profile

LDAP/LDAPS/LDAPTLS External Authentication Profile

Add LDAP, LDAPS, and LDAPTLS authentication profile as follows:

1. Go to **ADMIN** > **Settings** > **General** > **External Authentication**.
2. Click **New**.
3. Enter **Name**.
4. Select **Organization**.
5. Set **Protocol** as LDAP or LDAPS or LDAPTLS.
6. Set IP/Host of LDAP server.
7. Change the port if it is different than default port.
8. Check **Set Base DN** if needed by filling in the DN Pattern field.
   Setting the DN pattern manually is not necessary if the user is discovered via LDAP. However, this feature allows you to manually override the discovered pattern, or enter it for a user that is being manually created. Enter `%s` to represent the user's name (`CN/uid`), for example:
   `CN=%s,CN=Users,DC=accelops,DC=com`
9. Click **Save**.

RADIUS External Authentication Profile

Add RADIUS authentication profile as follows:

1. Go to **ADMIN** > **Settings** > **General** > **External Authentication**.
2. Click **New**.
3. Enter **Name**.
4. Select **Organization**.
5. Set **Protocol** as RADIUS.
6. Set IP/Host of RADIUS server.
7. Change and set **Authen Port** if the port is different from default.
8. Enter **Shared Secret**.
9. Click on **CHAP** if Radius server uses Challenge Handshake Authentication Protocol.
10. Click **Save**.

Okta External Authentication Profile

Add Okta authentication profile as follows:

1. Go to **ADMIN** > **Settings** > **General** > **External Authentication**.
2. Click **New**.
3. Enter **Name**.
4. Select **Organization**
5. Set **Protocol** as "Okta".
6. Copy and paste the certificate you downloaded during Okta Authentication. (Example: Configuring Okta Authentication - step 6 to **Certificate**).
7. Click **Save**.

Duo External Authentication Profile

Add a duo (2-factor) external authentication profile as follows:

1. Go to **ADMIN** > **Settings** > **General** > **External Authentication**.
2. Click **New**.
3. Enter **Name**.
4. Select **Organization**
5. Set **Protocol** as "Duo".
6. In the **IP/Host** field, enter the IP address/host name from the API hostname.
7. In the **Integration Key** field, enter/paste the Integration Key.
8. In the **Secret Key** field, enter/paste the Secret Key.
9. In the Application Key field, enter/paste the Application Key.
10. Click **Save**.

SAML External Authentication Profile

Add a SAML external authentication profile as follows:

1. Go to **ADMIN** > **Settings** > **General** > **External Authentication**.
2. Click **New**.
3. Enter **Name**.
4. Select **Organization**
5. Set **Protocol** as "SAML".
6. In the **Certificate** field, paste your SAML certificate.
7. For the **User**, **Org**, and **Role** selection, choose the appropriate attribute.
8. Click **Save**.

Step 2: Configure User for External Authentication

- LDAP/LDAPS/LDAPTLS, RADIUS, Okta, SAML User Configuration
- Duo User Configuration

LDAP/LDAPS/LDAPTLS, RADIUS, Okta, SAML User Configuration

To configure a user for all protocols excluding Duo, take the following steps:

1. Log on to FortiSIEM as Admin.
2. Go to **CMDB > Users**.
3. Click **New** to create a new user.
   Note: You may need to navigate to **CMDB > Users > Ungrouped**.
4. Click **System Admin**.
5. From the **Mode** drop-down list, select **External**.
6. From the **Authentication Profiles** drop-down list, select your user profile.
7. Set the user's Role.
8. When done, click **Save**.

Duo User Configuration

To configure a user for Duo protocol, take the following steps:

1. Log on to FortiSIEM as Admin.
2. Go to **CMDB > Users**.
3. Click **New** to create a new user.
   Note: You may need to navigate to **CMDB > Users > Ungrouped**.
4. Click **System Admin**.
5. In the **Password** and **Confirm Password** fields, enter the user's password.
6. Select the **Second Factor** checkbox, and select your Duo (2 Factor authentication) profile.
7. Select a **Default Role** from the drop-down list.
8. When done, click **Save**.

Configure Users for Generic SAML Authentication

- Step 0: Overview
- Step 1 - Preparation
- Step 2 - Create External Authentication Profile in FortiSIEM
- Step 3 - Create SAML Role Mappings in FortiSIEM
- Step 4 - Create the User in CMDB

Step 0: Overview

In SAML authentication, there are 3 entities:

- Identity Provider (IDP) - this is where user authentication happens. There are many examples, OKTA, Entrust, etc...
- IDP Portal - this is where you define users and credentials for your IDP and Service Providers.
- Service Provider (SP) - this is where the user logs on after authentication succeeds, e.g. FortiSIEM in this case.

After configuration, the flow is as follows:

1. The user authenticates on to the IDP Portal.
2. The user clicks a FortiSIEM icon on the IDP Portal.
3. IDP sends a SAML response to FortiSIEM containing the User, Org, and Role. User and Org are required, while Role is optional.
4. FortiSIEM trusts the IDP and logs in the User with the right Org and Role (if applicable).

To ensure SAML works correctly, the following must be done.

1. Define URLs and credentials in IDP Portal and FortiSIEM so that they can securely communicate with each other.
2. Map the User, Org, and Role in the IDP Portal to the User, Org, and Role in FortiSIEM. The User must be an exact match, including case-sensitivity. For Org and Role, you can define mappings in FortiSIEM for IDP Org to FortiSIEM Org and IDP Role to FortiSIEM Role.

The following is a detailed example showing the steps required for configuration. This example assumes a FortiSIEM user has already been created in an IDP Portal.

Step 1 - Preparation

A. Configure your IDP for the specific User, Organization, and Role. Collect IDP Portal endpoint and certificate.

B. Study the SAML Response from your IDP and determine where to find the User, Org, and Role. Typically, the User is in the NameIdentifier element of the Subject statement. Org is in the Audience element of AudienceRestriction.

This step is different for every IDP vendor. See the representative examples below for Okta.com and samltest.idp website. In OKTA.com, there is no Role information. However, the samltest.idp website allows you to define a role.

Step 2 - Create External Authentication Profile in FortiSIEM

A. Log on to FortiSIEM as Admin.

B. Go to **ADMIN > Settings > General > External Authentication**.

C. Click **New** to create an External Authentication profile.
   - i. (Service Provider Case) Set **Organization** to **System** if any User from any Org can use this profile. Otherwise, set it to the specific Org.
   - ii. In the **Protocol** drop-down list, select **SAML**.
   - iii. Fill in the **Issuer** and **Certificate** (credentials) fields using the information collected in Step 1A.
   - iv. Set **User** to the specific field in the SAML Response containing the User information. (note - match is exact and case-sensitive). This information was gathered in Step 1B. If the User is not in the NameIdentifier element of the Subject Statement, then select **Custom Attribute** and enter the field containing the User information.
   - v. Set **Org** to the specific field in the SAML Response containing the Org information. This information was gathered in Step 1B. If Org is not in the Audience element of AudienceRestriction, then select **Custom Attribute** and enter the field containing the Org information. Matching is determined by the Role mapping rules in Step 3.
   - vi. If Role is present in the SAML Response from the IDP, then select **Custom Attribute** and enter the field containing the Role information. Otherwise, select **None**. In the later case, you must create the User in CMDB for the specific Org, and assign the right Role. Step 3 is not needed.

Step 3 - Create SAML Role Mappings in FortiSIEM

This step is only needed if Role is present in the SAML Response as in Step 2Cvi. For example, OKTA does not have Role, so this step is not needed.

A. Log on to FortiSIEM as Admin.

B. Go to **ADMIN > Settings > Role > SAML Role**.

C. Click **New**.

D. In the Add SAML Role, enter the following information.
   - i. From the **SAML Auth profile**, select the user.
   - ii. In the **SAML Role** field, enter the SAML Role.
   - iii. In the **SAML Organization** field, enter the SAML Organization.
   - iv. From the **Mapped Role** drop-down list, select an existing role.
   - v. From the **Mapped Organization** drop-down list, select an organization.
   - vi. (Optional) In the **Comments** field, enter any information you may wish to reference at a future date.
   - vii. Click **Save**.

Step 4 - Create the User in CMDB

This step is only needed if Role is not present in the SAML Response, as in Step 2Cvi. For example, OKTA does not have Role, so this step is needed.

A. Log on to FortiSIEM as Admin.
B. Go to **CMDB > Users**.
C. If the SAML user is not present, then click **New** to create a new user.
Note: You may need to navigate to **CMDB > Users > Ungrouped**.
D. In the **User Name** field, enter the name exactly as that used in Step 2Civ. The name must match exactly, including case-sensitivity.
E. Click **System Admin** and set the Role.
F. When done, click **Save**.

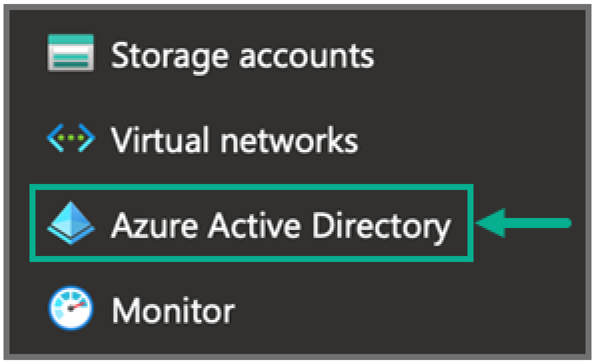
This procedure is described in more details in https://help.fortinet.com/fsiem/7-0-2/Online-Help/HTML5_Help/Adding_users.htm.

Configure Users for SAML Authentication with Azure AD

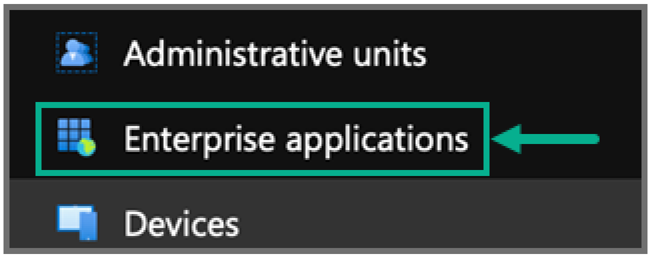
- Step 1: Setup Azure
- Step 2: Setup FortiSIEM
- Step 3: Setup SAML Role Mapping

Step 1: Setup Azure

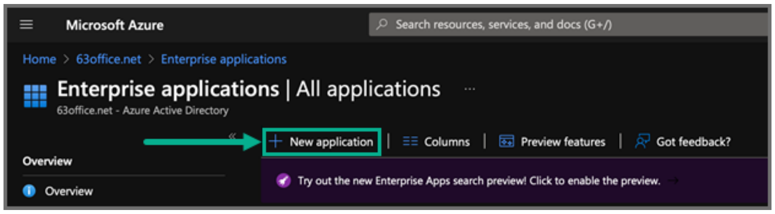
1. In Azure, navigate to **Azure Active Directory**.



2. Navigate to **Enterprise applications**.

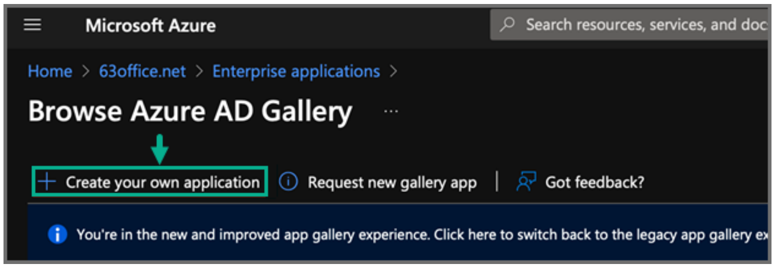


3. Select **New application**.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > 63office.net > Enterprise applications
Enterprise applications | All applications
63office.net - Azure Active Directory
New application
Columns
Preview features
Got feedback?
Overview
Overview

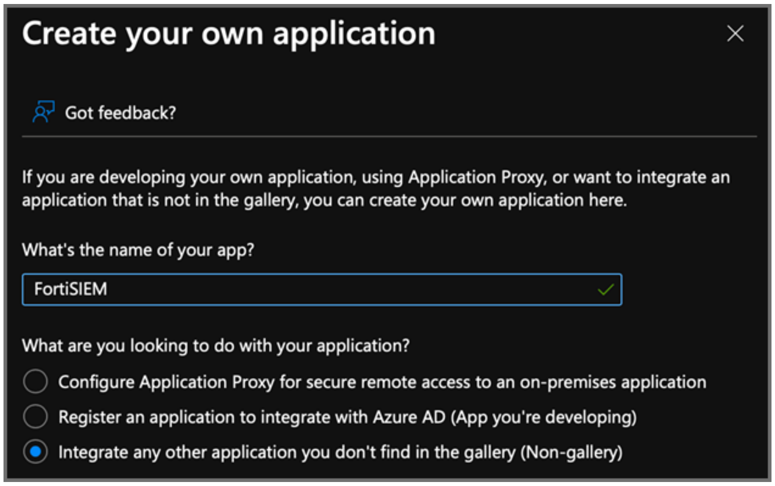
Try out the new Enterprise Apps search preview! Click to enable the preview.

4. Select **Create your own application**.


Microsoft Azure
Search resources, services, and doc
Home > 63office.net > Enterprise applications >
Browse Azure AD Gallery
Create your own application
Request new gallery app
Got feedback?

You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery ex

5. For "What's the name of your app?", enter a name, such as FortiSIEM.
6. For "What are you looking to do with your application?", select **Integrate any other application you don't find in the gallery (Non-gallery)**.



If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

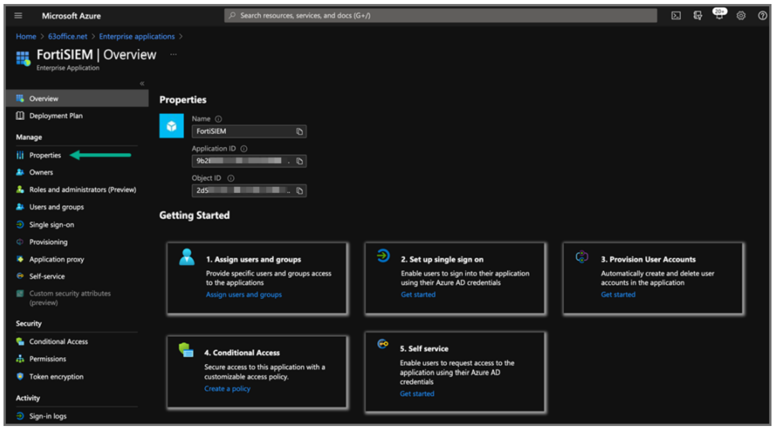
FortiSIEM

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application
○ Register an application to integrate with Azure AD (App you're developing)
● Integrate any other application you don't find in the gallery (Non-gallery)

After the application has been created, take the following steps:

1. From the **Azure Active Directory**, select your new application.
2. Display the **Properties**.



Name: FortiSIEM
Application ID: 9b2[redacted]
Object ID: 2d5[redacted]

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

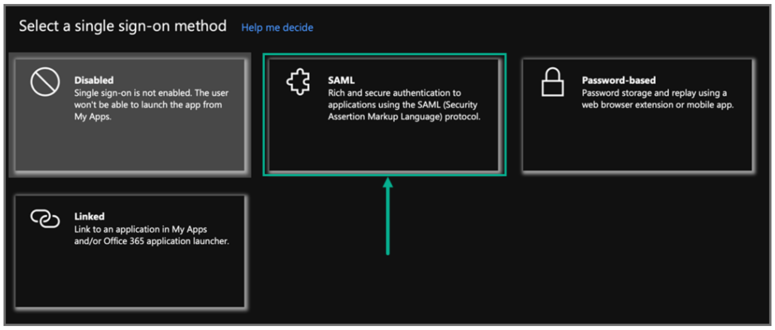
2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

3. Under **Getting Started**, under options **1. Assign users and groups**, select the **Assign users and groups** link and ensure you have some users and groups defined who will be able to access the new application.
4. Under option 2. Set up single sign on, click the **Get started** link, and select **SAML**.



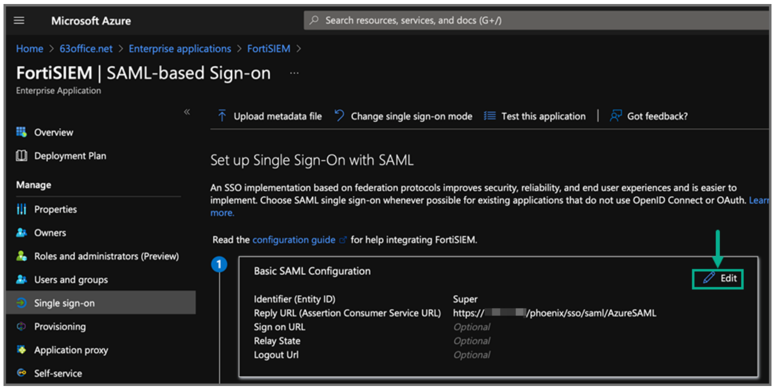
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

5. Under the **Set up Single Sign-On with SAML** options, click **Edit** for **Step One: Basic SAML Configuration**.



Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating FortiSIEM.

Basic SAML Configuration

Identifier (Entity ID) Super
Reply URL (Assertion Consumer Service URL) https://[redacted]/phoenix/sso/saml/AzureSAML
Sign on URL Optional
Relay State Optional
Logout Url Optional

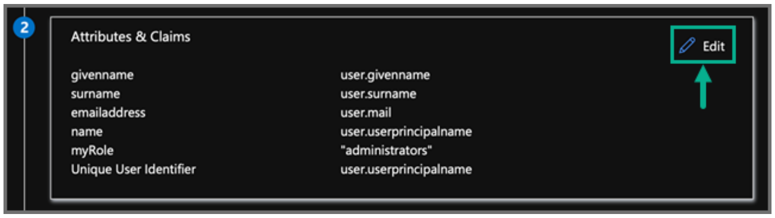
6. For **Identifier (Entity ID)** and **Reply URL**, enter the following information whether you plan to use Option 1 or Option 2.
Note: The difference between the two options suggested is that for the Option 2 FortiSIEM interface, you need to specify which SAML schema attribute will determine the Organization at login.

Option 1 - Using the Default Org Mapping in FortiSIEM	
Identifier (Entity ID)	*<FortiSIEM Org Name>* For example, enter **Super** for Enterprise installations or the name of your new Organization created in a Multi-Tenant installation.
Reply URL	`https://<fsm ip or fqdn>/phoenix/sso/saml/<external authentication profile name>`

In the FortiSIEM Authentication Profile, the default value of “AudienceRestriction” will be used.

Option 2 - Using a Custom Attribute to Define the Org Mapping in FortiSIEM	
Identifier (Entity ID)	Anything you like.
Reply URL	`https://<fsm ip or fqdn>/phoenix/sso/saml/<external authentication profile name>`

7. Under **Step Two: Attributes & Claims**, click **Edit**.

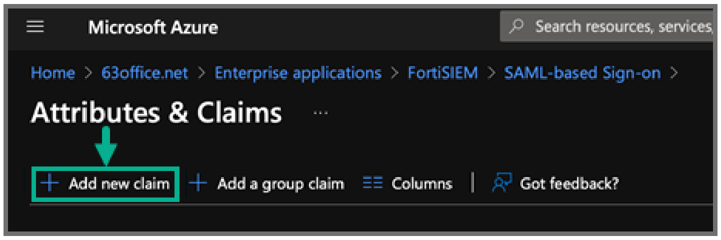


givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
myRole	"administrators"
Unique User Identifier	user.userprincipalname

Here is where the SAML response can be manipulated to add extra attributes which can be used to tell FortiSIEM the Org to use at login (If Option 2 is used above), and also a Role name to be assigned at Login, if the user does not exist already in the FortiSIEM CMDB.

Take the following steps to add an attribute for Organization, if Option 2 is being used above.

a. Click **Add new claim**.

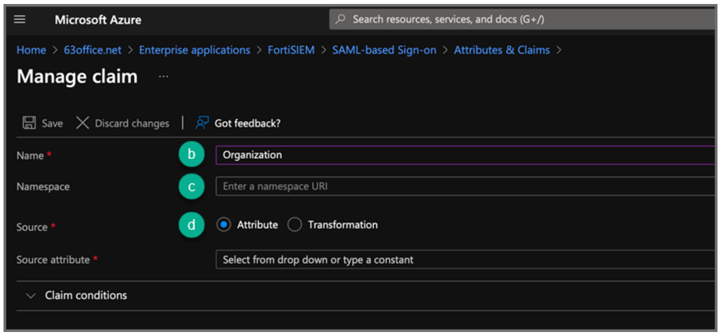

Microsoft Azure
Search resources, services
Home > 63office.net > Enterprise applications > FortiSIEM > SAML-based Sign-on >
Attributes & Claims ...
+ Add new claim
+ Add a group claim
Columns
Got feedback?

b. In the **Name** field, enter the Custom Attribute to use, for example: Organization.

c. For **Namespace**, leave the field blank.

d. For **Source**, make sure “Attribute” is selected and then under Source attribute select the drop-down and then type a value such as the Organization name or an Identifier you will use in FortiSIEM to map to the correct Org.
Note: Alternatively, one of the predefined Azure Values can be used such as `user.companyname` if those values are populated in the directory. (Just make sure the Name of the attribute does not contain

any characters other than letters, underscore or dash.)



Microsoft Azure

Search resources, services, and docs (G+/)

Home > 63office.net > Enterprise applications > FortiSIEM > SAML-based Sign-on > Attributes & Claims >

Manage claim

Save | Discard changes | Got feedback?

Name * (b): Organization

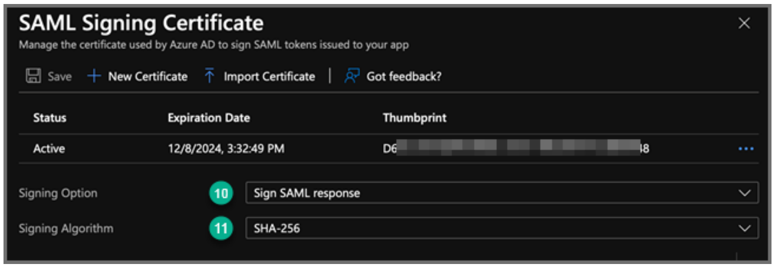
Namespace (c): Enter a namespace URI

Source * (d): ● Attribute ○ Transformation

Source attribute *: Select from drop down or type a constant

Claim conditions

8. Take the following steps to add an attribute for Role.
    a. Click **Add new claim**.
    b. In the **Name** field, enter the Custom Attribute to use, for example: **myRole**.
    c. For **Namespace**, leave the field blank.
    d. For **Source Attribute**, set it to be a value for the Role.
9. Under **Step Three: SAML Signing Certificate**, click **Edit**.
10. For the **Signing Option**, select **Sign SAML Response**.
11. For the **Signing Algorithm**, select **SHA-256**.



SAML Signing Certificate

Manage the certificate used by Azure AD to sign SAML tokens issued to your app

Save | New Certificate | Import Certificate | Got feedback?

Status	Expiration Date	Thumbprint
Active	12/8/2024, 3:32:49 PM	D6[redacted]8

Signing Option (10): Sign SAML response

Signing Algorithm (11): SHA-256

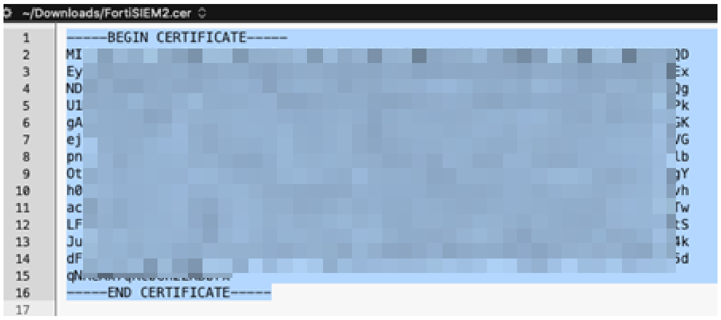
12. Click **Save**.
13. Exit back to the configuration by clicking the **X** in the top right corner, and then **Download the Certificate in Base64** encoded format. (This will be needed in step 3e. under Step 1: Setup FortiSIEM.)
14. Under **Step Four: Set up FortiSIEM**, copy the **Azure AD Identifier** string. (This will also be needed below to be input into FortiSIEM)

Step 2: Setup FortiSIEM

In FortiSIEM, take the following steps:

1. Navigate to **ADMIN > Settings > General > External Authentication**.
2. Click **New**.
3. In the External Authentication Profile window, take the following steps:
    a. In the **Name** field, enter a name, for example, AzureSAML.
    b. In the **Organization** drop-down list, select your Organization.
    c. In the **Protocol** drop-down list, select **SAML**.
    d. In the **Issuer** field, paste the **Azure AD Identifier**.

e. In the **Certificate** field, paste the certificate information.



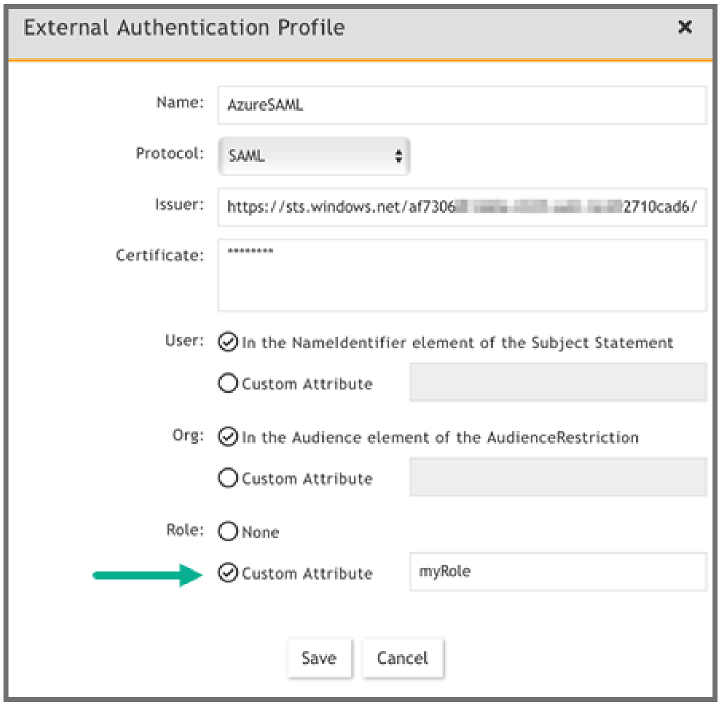
~/Downloads/FortiSIEM2.cer

```
-----BEGIN CERTIFICATE-----
[redacted]
-----END CERTIFICATE-----
```

f. In the **User** section, leave the default option "In the NameIdentifier element of the Subject Statement" selected.

g. In the **Org** section, take the following steps:
   i. If Option 1 was used at step (6) in Azure setup, then leave the default option of "In the Audience element of the AudienceRestriction" selected.
   ii. If Option 2 was used, then select **Custom Attribute** and enter the name of the Attribute created at step (7b) in the Azure set up above.

h. In the **Role** section, select **Custom Attribute** and enter the name of the Attribute created at step (8d) in the Azure set up above.



External Authentication Profile ✕

Name:	AzureSAML
Protocol:	SAML
Issuer:	https://sts.windows.net/af7306[redacted]2710cad6/
Certificate:	********
User:	☑ In the NameIdentifier element of the Subject Statement
	○ Custom Attribute
Org:	☑ In the Audience element of the AudienceRestriction
	○ Custom Attribute
Role:	○ None
	☑ Custom Attribute myRole

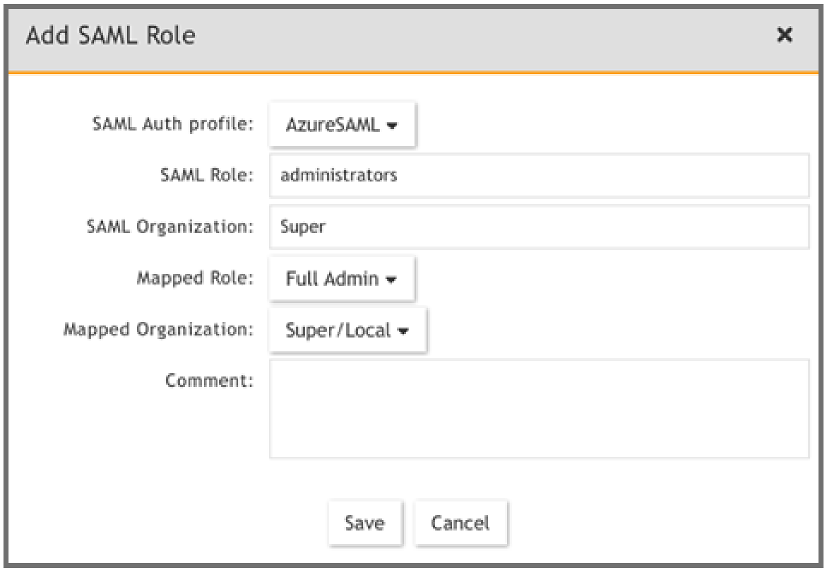
i. Click **Save** when done.

Step 3: Setup SAML Role Mapping

1. Log into the FortiSIEM GUI as a user with Admin rights and navigate to **ADMIN > Settings > Role > SAML Role**.
2. Click **New**.

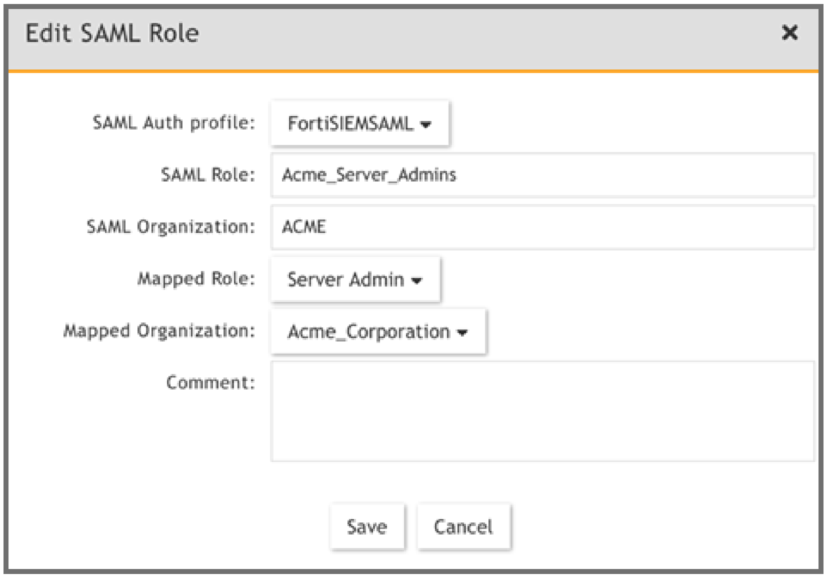
3. From the Add SAML Role window, take the following steps.
   a. From the **SAML Auth profile** drop-down list, select the External SAML Authentication Profile created above.
   b. For the **SAML Role** field, enter the value being output in the SAML response which should be the Source Attribute value entered at Azure set up step (8d).
   c. For the **SAML Organization** field, enter the value being output in the SAML response which should be the Identifier (Entity ID) at Azure set up step (6) if Option 1 was used, or the Source Attribute value entered at Azure set up step (7c) if Option 2 was used.
   d. For the **Mapped Role** drop-down list, select the FortiSIEM Role to assign based upon a matching value.
   e. For the **Mapped Organization** drop-down list, select the FortiSIEM Organization to assign based upon a matching value.
   f. Click **Save**.

Here is an example of an Enterprise mapping. The SAML Organization for an Enterprise mapping is **Super**.



SAML Auth profile: AzureSAML
SAML Role: administrators
SAML Organization: Super
Mapped Role: Full Admin
Mapped Organization: Super/Local
Comment:

Here is an example of a Multi-Tenant mapping.



Edit SAML Role

SAML Auth profile: FortiSIEMSAML

SAML Role: Acme_Server_Admins

SAML Organization: ACME

Mapped Role: Server Admin

Mapped Organization: Acme_Corporation

Comment:

Authenticating Users Against FortiAuthenticator (FAC)

- Step 1: Configure AD Users
- Step 2: Configure FortiAauthenticator
- Step 3: Configure FortiSIEM

Step 1: Configure AD Users

1. Install AD Domain Services following the steps here.
2. Configure the test domain users:
   a. **Server Manager** > **Tools** > **Active Directory Users and Computers**.
   b. Expand the Domain, right-click **Users**, select **New** > **User**.

Step 2: Configure FortiAauthenticator

1. Perform the basic FAC setup following the steps in the *FortiAuthenticator Administration Guide: Section: FortiAuthenticator-VM image installation and initial setup* here.
   a. Use the default credentials:
      - user name: `admin`
      - password: <blank>
   b. At the CLI prompt enter the following commands:
      - `set port1-ip 192.168.1.99/24`
      - `set default-gw 192.168.1.2`

      Note that the CLI syntax has changed in FAC 5.x. Refer to a 6.x FortiAuthenticator Administration Guide for details.
   c. Log in to the FAC GUI (default credentials user name / password: `admin` / `<blank>`).
   d. Set the time zone under **System** > **Dashboard** > **Status** > **System Information** > **System Time**.
   e. Change the GUI idle timeout for ease of use during configuration, if desired: **System Administration** > **GUI Access** > **Idle Timeout**.

2. Configure the DC as a remote LDAP server under **Authentication** > **Remote Authentication Servers** > **LDAP**.
   Follow the Fortinet Single Sign-On instructions in the appropriate FortiAuthenticator Administration Guide. Note that the user must have appropriate privileges. The Domain Admin account can be used for testing in a lab environment. The 'Remote LDAP Users' section will be blank at this stage, users are imported later.
3. Configure an external Realm to reference the LDAP store:
   a. Select **Authentication** > **User Management** > **Realms** > **Create New**.
   b. Choose the LDAP source from the drop-down and click **OK**.
4. Configure the FortiSIEM as a RADIUS Client:
   a. Select **Authentication** > **RADIUS Service** > **Clients** > **Create New**.
   b. Enter the IP address of FortiSIEM and a shared secret.
   c. Choose the realms as required.
   d. Click 'add a realm' to include multiple realms.
      Note the FAC evaluation license only supports 2 realms.
   e. Click **Save**.
5. Import users from LDAP to FortiSIEM to allow FortiToken to be used:
   a. Select **Authentication** > **User Management** > **Remote Users**.
   b. Select the **Import** button.
   c. Choose and import the test users configured in AD. Note that the FAC Evaluation license is limited to 5 users.
6. (Optional) Configure local users in the FAC database for local authentication under **Authentication** > **User Management** > **Local Users**.
7. Provision the FortiToken:
   a. Select and edit the user in **Authentication** > **User Management** > **Remote Users** (or Local Users as appropriate).
   b. Select the **Token Based Authentication** check box, and assign an available FortiToken Mobile.
      FAC evaluation includes 2 demo FortiTokens.
   c. Choose **Email** delivery method and enter an email address in user information.
      The email address doesn't have to be valid for basic testing, the provisioning code is visible in the FAC logs.
   d. Click **OK**.
8. Configure the FortiToken iPhone app:
   a. Install the FortiToken app from the app store.
   b. Open the app and select the **+** icon in the top right corner.
   c. Choose **enter manually** from the bottom of the screen.
   d. Select and edit the user in **Authentication** > **User Management** > **Remote Users** (or Local Users as appropriate).
   e. Select the **Token Based Authentication** check box, and assign an avaialble FortiToken Mobile. FAC eval includes 2 demo FortiTokens.
   f. Choose **Email** delivery method and enter an email address in user information. The email address doesn't have to be valid for basic testing, the provisioning code is visible in the FAC logs.
   g. Click **OK**.

Step 3: Configure FortiSIEM

Step A: Configure an External Authentication Source

1. Go to **ADMIN** > **Settings** > **General** > **External Authentication**.
2. Click **New**.
3. Enter the following settings:
   - **Organization** - System
   - **Protocol** - RADIUS
   - **IP/Host** - IP of FortiAuthenticator
   - **Shared Secret** - Secret configured when setting RADIUS Client in FAC
4. Click **Save**.
5. Click **Test** to test the authentication settings.

Step B: Configure Users in FortiSIEM Database

1. Go to **CMDB** > **Users** and click **New**.
2. Enter the user name to match the user configured in FSM/AD. (Use the format: user@domain.com)
3. Select the **System Admin** checkbox.
4. Select the **Mode** as **External**.
5. Select the RADIUS profile previously configured from **Authentication Profiles**.
6. Select the **Default Role** from the list.
7. Click **Save**.

Logging In

The **User Name** must be entered in the format `user@domain.xyz`. For 2-factor authentication, the password and FortiToken value must be concatenated and entered directly into the **Password** field.

For example:

- Username: `user123@testdomain.local`
- Password : `testpass123456`; where `123456` is the current FortiToken value

Note: FortiAuthenticator logs are accessible by opening the **Logging** tab. Select a log entry to see more details.

Add 2-Factor Authentication Option for FortiSIEM Users

- Step 0: Obtain Keys for FortiSIEM to Communicate with Duo Security
- Step 1: Create and Manage FortiSIEM users in Duo Security
- Step 2: Add 2-Factor Authentication Option for FortiSIEM Users
- Step 3: Log in to FortiSIEM Using 2-Factor Authentication

Step 0: Obtain Keys for FortiSIEM to Communicate with Duo Security

1. Sign up for a Duo Security account: signup.
   This will be admin account for Duo Security.
2. Log in to Duo Security Admin Panel and navigate to **Applications**.
3. Click **Protect an Application.** Locate **Web SDK** in the applications.

4. Get **API Host Name**, **Integration key**, **Secret key** from the page.
   You will need it when you configure FortiSIEM.
5. Generate **Application key** as a long string.
   This is a password that Duo Security will not know. You can choose any 40 character long string or generate it as follows using python

   ```
   import os, hashlib

   print hashlib.sha1(os.urandom(32)).hexdigest()
   ```

Step 1: Create and Manage FortiSIEM users in Duo Security

This determines how the 2-factor authentication response page will look like in FortiSIEM and how the user will respond to the second-factor authentication challenge:

1. Log in to Duo Security as admin user.
2. Choose the **Logo** which will be shown to users as they log on.
3. Choose the super set of 2-factor **Authentication Methods**.
4. **Optional** - you can create the specific users that will logon via FortiSIEM. If the users are not pre-created here, then user accounts will be created automatically when they attempt 2-factor authentication for the first time.

Step 2: Add 2-Factor Authentication Option for FortiSIEM Users

1. Create a 2-factor authentication profile:
   a. Go to **ADMIN** > **Settings** > **General** > **External Authentication**.
   b. Click **New**.
      a. Enter **Name**.
      b. Select the organization from the **Organization** drop-down.
      c. Set the **Protocol** as 'Duo'.
      d. Set the **IP/Host** from API hostname in Step 4 above.
      e. Set the **Integration key**, **Secret key**from Step 4 above.
      f. Set the **Application key** from Step 5 above.
      g. Click **Save**.
2. Add the 2-factor authentication profile to a user:
   a. Go to **CMDB** > **Users** > **Ungrouped**.
   b. Click **New** to create a new use or **Edit** to modify a selected user.
   c. Select **System Admin** checkbox and click the edit icon.
   d. In the **Edit User** dialog box, enter and confirm a password for a new user.
   e. Select the **Second Factor** check-box.
   f. Select the 2-factor authentication profile created earlier in Step 2: Add 2-Factor Authentication Option for FortiSIEM Users.
   g. Select a **Default Role** from the drop-down list.
   h. Click **Save**.

Step 3: Log in to FortiSIEM Using 2-Factor Authentication

1. Log on to FortiSIEM normally (first factor) using the credential defined in FortiSIEM - local or external in LDAP.
2. If the 2-factor authentication is enabled, the user will now be redirected to the 2-factor step.
   a. If the user is not created in the Duo system (by the Duo admin), a setup wizard will let you set some basic information like phone number and ask you to download the Duo app.
   b. If the user already exists in FortiSIEM, then follow the authentication method and click **Log in**.

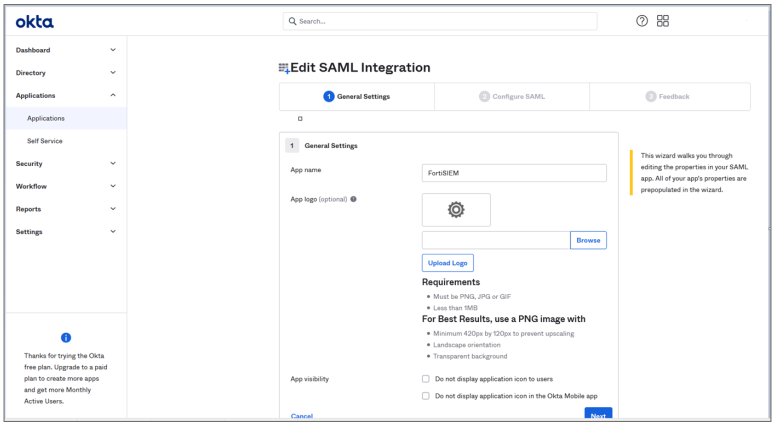
   The user will be able to log in to FortiSIEM.

Appendix

- Example 1: Setup OKTA for SAML Authentication
- Example 2: Setup SAMLTEST.ID for SAML Authentication
- Troubleshooting SAML Configuration

Example 1: Setup OKTA for SAML Authentication

1. Using an admin account, log into Okta (https://okta.com/)
2. Click on the **Admin** button.
3. Enter the Okta Verify code.
4. At the **Use single sign on** option, click the **Add App** button.
5. Click on **Create New App**.
6. Select SAML 2.0 and click **Create**.
   In **General Settings**, provide the following:
   - App name - FortiSIEM
   - App logo (optional)
7. Click **Next**.



Edit SAML Integration

1 General Settings

App name: FortiSIEM

App logo (optional)

Requirements
- Must be PNG, JPG or GIF
- Less than 1MB

For Best Results, use a PNG image with
- Minimum 420px by 120px to prevent upscaling
- Landscape orientation
- Transparent background

App visibility
☐ Do not display application icon to users
☐ Do not display application icon in the Okta Mobile app

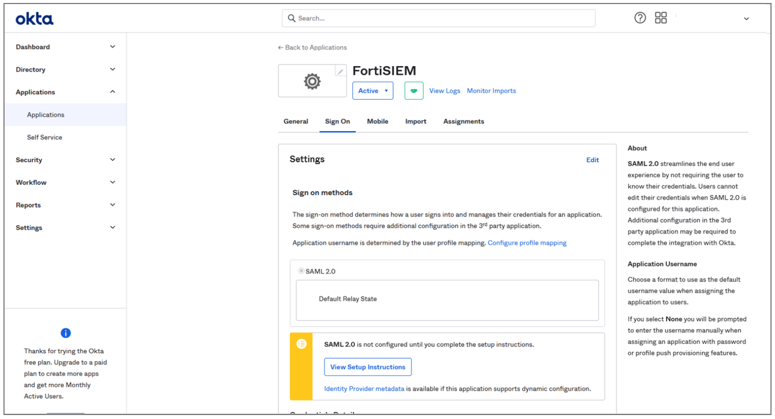
This wizard walks you through editing the properties in your SAML app. All of your app's properties are prepopulated in the wizard.

Thanks for trying the Okta free plan. Upgrade to a paid plan to create more apps and get more Monthly Active Users.

8. In **Configure SAML**, provide the following:

- In Single sign on URL, enter https://*super_ip*/phoenix/sso/saml/*ExternalAuthenticationProfileName*
  super_ip represents the FortiSIEM IP address you want to log into, and ExternalAuthenticationProfileName will need to be configured in FortiSIEM by a full Admin creating an SAML External Authentication Profile via **ADMIN > Settings > General > External Authentication**.
- In the **Audience URI (SP Entity ID)**, enter your organization name, for example "Super".

9. Click **Next**, then **Finish**. The FortiSIEM app is now being created.
10. On the Okta Application page, under Sign On Settings, SAML 2.0, click **View Setup Instructions**.



Settings

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

○ SAML 2.0

Default Relay State

SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

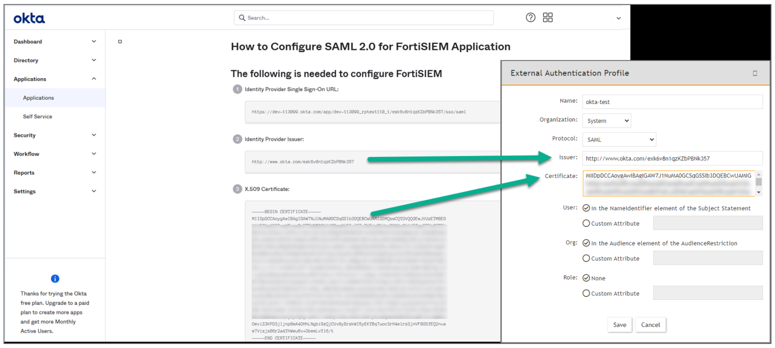
Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

Thanks for trying the Okta free plan. Upgrade to a paid plan to create more apps and get more Monthly Active Users.

11. Copy the **Identify Provider Issuer** and **Certificate** information. When you create your External Authentication Profile in FortiSIEM, the Identify Provider Issuer will go into the **Issuer** field, and the Certificate information will go into the **Certificate** field.



[redacted]

How to Configure SAML 2.0 for FortiSIEM Application

The following is needed to configure FortiSIEM

1. Identity Provider Single Sign-On URL:

```
https://dev-113099.okta.com/app/dev-113099_rptest110_1/exk6v8n1qzKZbPBNk357/sso/saml
```

2. Identity Provider Issuer:

```
http://www.okta.com/exk6v8n1qzKZbPBNk357
```

3. X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDpDCCAoygAwIBAgIGAW7NJ1NuMA0GCSqGSIb3DQEBCwUAMIGSMQswCQYDVQQGEwJVUzETMBEG
OeviZ3KPD3j1jnp8mA4OHhLNgbi9zQjCUv8yXrxkWI5yEKYBq7uoc3rH4elrx3jnVF8GSfEQ2n+a
e7Vixjz06r2a4YhWwu6v+ObeeLvYI6/t
-----END CERTIFICATE-----
```

External Authentication Profile

Name: okta-test

Organization: System

Protocol: SAML

Issuer: http://www.okta.com/exk6v8n1qzKZbPBNk357

Certificate: MIIDpDCCAoygAwIBAgIGAW7J1NuMA0GCSqGSIb3DQEBCwUAMIG

User: ☑ In the NameIdentifier element of the Subject Statement

○ Custom Attribute

Org: ☑ In the Audience element of the AudienceRestriction

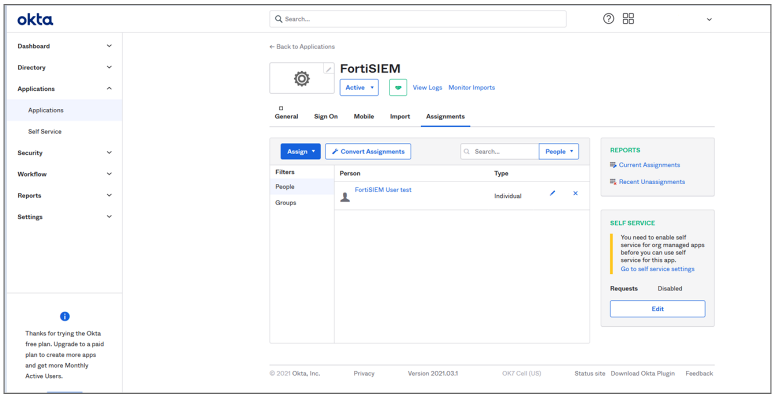
○ Custom Attribute

Role: ☑ None

○ Custom Attribute

Thanks for trying the Okta free plan. Upgrade to a paid plan to create more apps and get more Monthly Active Users.

12. Assign the OKTA user(s) for FortiSIEM.



Person	Type
FortiSIEM User test	Individual

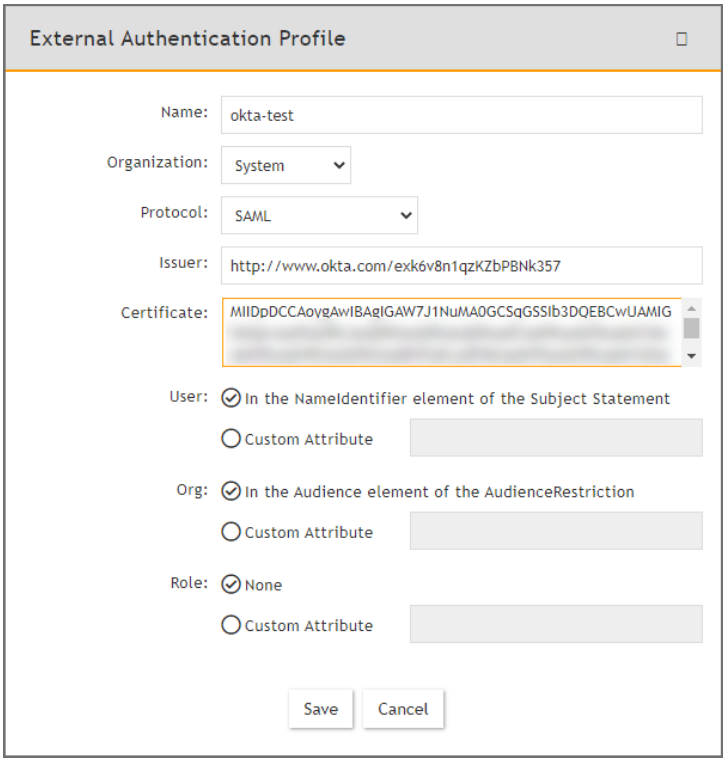
You need to enable self service for org managed apps before you can use self service for this app.

Requests Disabled

Thanks for trying the Okta free plan. Upgrade to a paid plan to create more apps and get more Monthly Active Users.

13. Log on to FortiSIEM as a full Admin.
14. Go to **ADMIN > Settings > General > External Authentication**.
15. Click **New** to create an External Authentication Profile.
16. From External Authentication Profile, take the following steps:

a. In the **Name** field, enter your ExternalAuthenticationProfileName.
b. From the **Organization** drop-down list, select the org.
c. From the **Protocol** drop-down list, select **SAML**.
d. In the **Issuer** field, enter the Identify Provider Issuer from Okta.
e. In the **Certificate** field, enter/paste the certificate information from Okta.
f. Configure User, and Org according to your IDP.
g. Click **Save**.



External Authentication Profile

Name: okta-test

Organization: System

Protocol: SAML

Issuer: http://www.okta.com/exk6v8n1qzKZbPBNk357

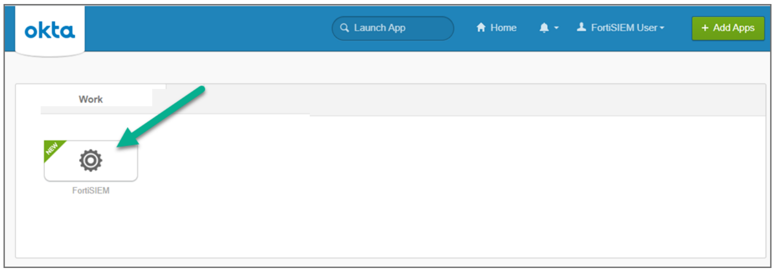
Certificate: MIIDpDCCAoygAwIBAgIGAW7J1NuMA0GCSqGSSIb3DQEBCwUAMIG [redacted]

User: ☑ In the NameIdentifier element of the Subject Statement
○ Custom Attribute

Org: ☑ In the Audience element of the AudienceRestriction
○ Custom Attribute

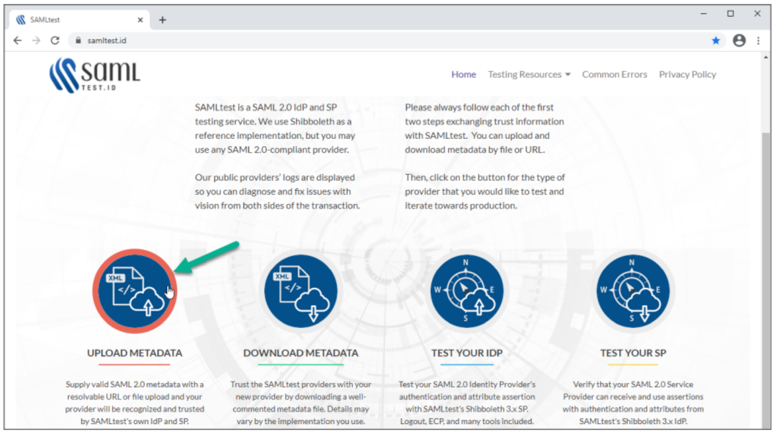
Role: ☑ None
○ Custom Attribute

17. Go to **CMDB > Users > Ungrouped**.
18. Click **New** to add the Okta user.
19. In the **User Name** field, enter the user's Okta assigned username.
    Note: You can enter the name by using an email address depending on how the user was configured in Okta.
20. Click the **System Admin** field to open the **New User** window.
21. From the **Mode** drop-down list, select **External**.
22. From the **Authentication Profiles** drop-down list, select your Okta authentication profile that you created under your External Authentication profile.
23. From the **Default Role** drop-down list, select the appropriate user role and check the appropriate organization checkboxes the user is enabled for.
24. Click **Back**.
25. Click **Save**.
26. Log on to Okta as an assigned user for FortiSIEM. The assigned Okta user is now able to log on to FortiSIEM by clicking the FortiSIEM icon/application.



Example 2: Setup SAMLTEST.ID for SAML Authentication

1. Prepare a SAML.XML file.
2. Go to https://samltest.id/.
3. Click **UPLOAD METADATA**.



SAMLtest is a SAML 2.0 IdP and SP testing service. We use Shibboleth as a reference implementation, but you may use any SAML 2.0-compliant provider.

Our public providers' logs are displayed so you can diagnose and fix issues with vision from both sides of the transaction.

Please always follow each of the first two steps exchanging trust information with SAMLtest. You can upload and download metadata by file or URL.

Then, click on the button for the type of provider that you would like to test and iterate towards production.

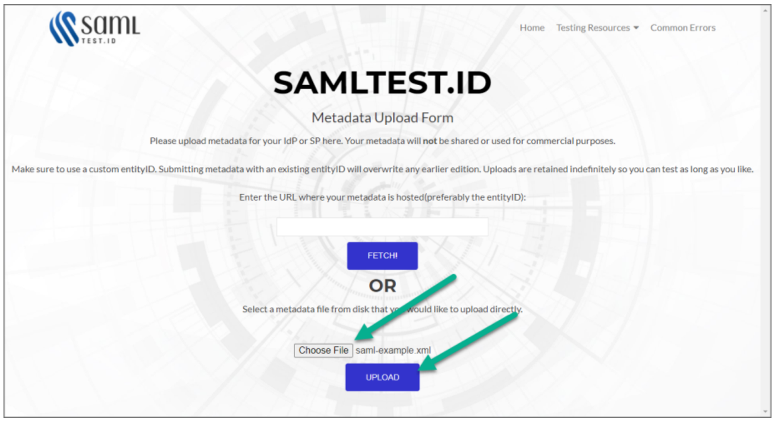
UPLOAD METADATA: Supply valid SAML 2.0 metadata with a resolvable URL or file upload and your provider will be recognized and trusted by SAMLtest's own IdP and SP.

DOWNLOAD METADATA: Trust the SAMLtest providers with your new provider by downloading a well-commented metadata file. Details may vary by the implementation you use.

TEST YOUR IDP: Test your SAML 2.0 Identity Provider's authentication and attribute assertion with SAMLtest's Shibboleth 3.x SP. Logout, ECP, and many tools included.

TEST YOUR SP: Verify that your SAML 2.0 Service Provider can receive and use assertions with authentication and attributes from SAMLtest's Shibboleth 3.x IdP.

4. Click **Choose File**, select your SAML.XML file, and click **UPLOAD**. When SAMLTEST.ID reports success, proceed to the next step, otherwise check your XML file and re-upload.



SAMLTEST.ID

Metadata Upload Form

Please upload metadata for your IdP or SP here. Your metadata will **not** be shared or used for commercial purposes.

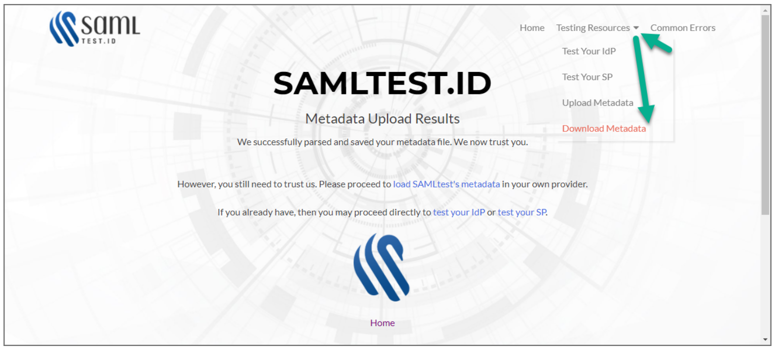
Make sure to use a custom entityID. Submitting metadata with an existing entityID will overwrite any earlier edition. Uploads are retained indefinitely so you can test as long as you like.

Enter the URL where your metadata is hosted(preferably the entityID):

Select a metadata file from disk that you would like to upload directly.

saml-example.xml

5. Click on **Testing Resources**, and select **Download Metadata**.



SAMLTEST.ID

Metadata Upload Results

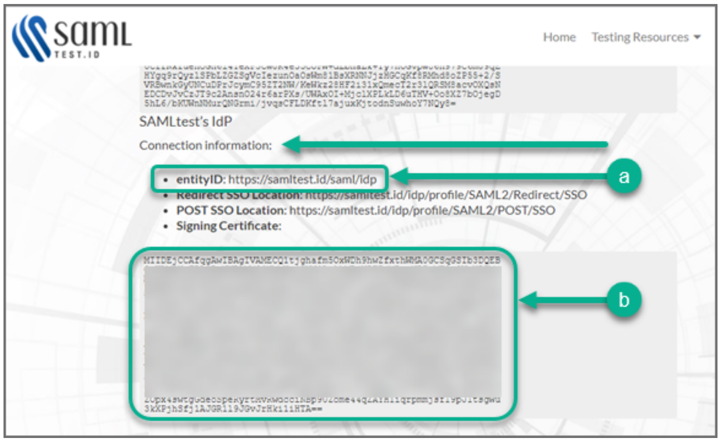
We successfully parsed and saved your metadata file. We now trust you.

However, you still need to trust us. Please proceed to load SAMLtest's metadata in your own provider.

If you already have, then you may proceed directly to test your IdP or test your SP.

Home

6. Scroll down until you see SAMLtest's IdP " Connection information".
   a. Copy the **entityID** information. This will go into the **Issuer** field in the External Authentication Profile for the SAML IDP configuration.
   b. Copy the **Signing Certificate** information. This will go into the **Certificate** field in the External Authentication Profile for the SAML IDP configuration.



```
HYgq9rQyz1SPbLZGZSgVcIezunOaOsWm81BsXRNNJjzMGCqKf8RMhd8oZP55+2/S
VRBwnkGyUNCuDPrJcymC95ZT2NW/KeWkz28HF2i31xQmecT2r31QRSM8acvOXQeN
EDCDvJvCzJT9c2Ansn024r6arPXs/UWAxOI+MjclXPLkLD6uTHV+Oo8XZ7bOjegD
5hL6/bKUWnNMurQNGrmi/jvqsCFLDKft17ajuxKjtodnSuwhoY7NQy8=
```

SAMLtest's IdP

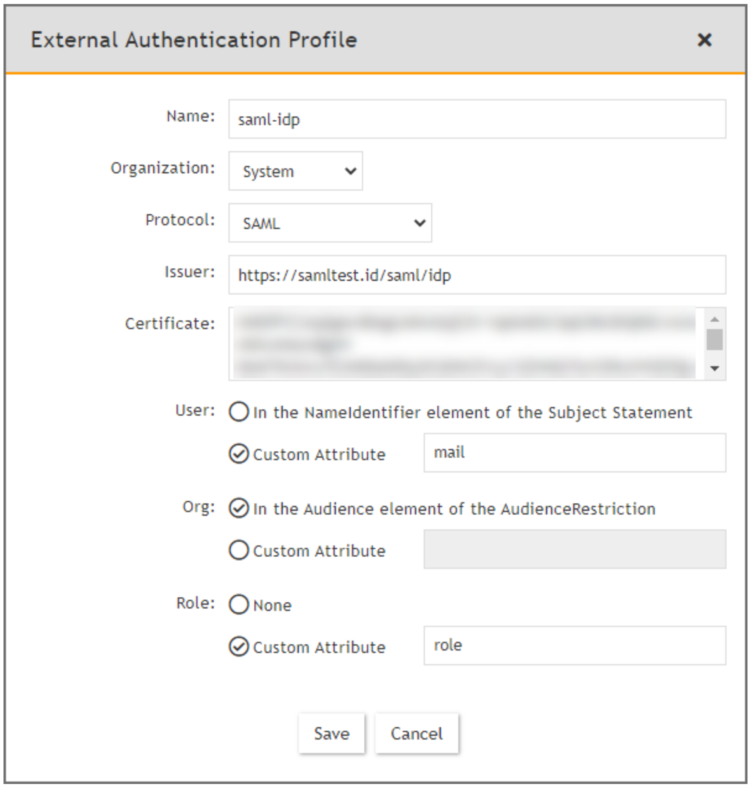
Connection information:

- **entityID:** https://samltest.id/saml/idp
- **Redirect SSO Location:** https://samltest.id/idp/profile/SAML2/Redirect/SSO
- **POST SSO Location:** https://samltest.id/idp/profile/SAML2/POST/SSO
- **Signing Certificate:**

```
MIIDEjCCAfqgAwIBAgIVAMECQ1tjghafm5OxWDh9hwZfxthWMA0GCSqGSIb3DQEB
[redacted]
ZOpx4swtgGdeospeKyrtmVxWdccINspyoZome44qZAIh1iqrpmmjsI19pJ1tsgwu
3kXPjhSfj1AJGRl19JGvJrHki1iHTA==
```

7. Log on to FortiSIEM with an Admin account, and navigate to **ADMIN > Settings > General > External Authentication**.
8. Click **New**.
9. Following the steps for SAML configuration in Step 1: Create External Authentication Profile, fill out the required information and click **Save**. Mandatory settings include
   - In the **Protocol** drop-down list, select **SAML**.
   - In the **Issuer** field, provide the entityID from step 6a.
   - In the **Certificate** field, paste/enter the signing certificate content from step 6b.

- Configure the User, Org, and Role appropriately, based on your elements.



External Authentication Profile

Name: saml-idp

Organization: System

Protocol: SAML

Issuer: https://samltest.id/saml/idp

Certificate:

User: ○ In the NameIdentifier element of the Subject Statement

● Custom Attribute mail

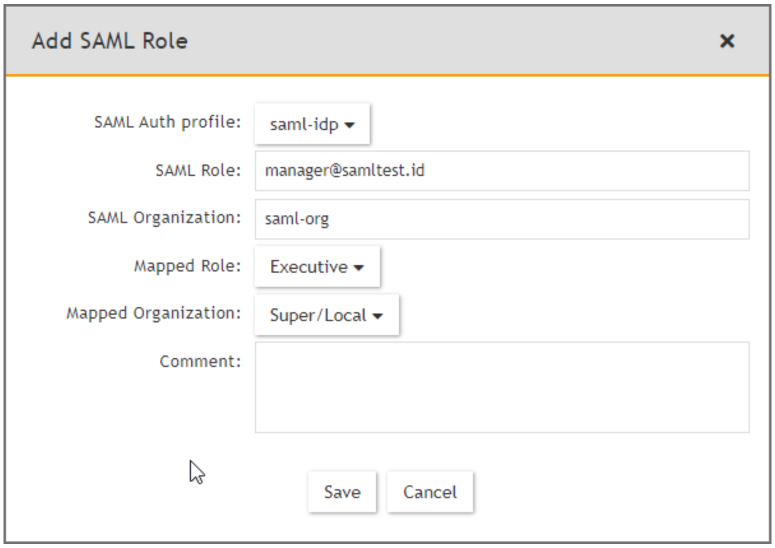
Org: ● In the Audience element of the AudienceRestriction

○ Custom Attribute

Role: ○ None

● Custom Attribute role

10. Go to **ADMIN > Settings > Role > SAML Role**, click **New**, fill out the information and click **Save**. The SAML user will be added automatically in **CMDB > Users** once the user logs on to FortiSIEM.



Add SAML Role

SAML Auth profile: saml-idp

SAML Role: manager@samltest.id

SAML Organization: saml-org

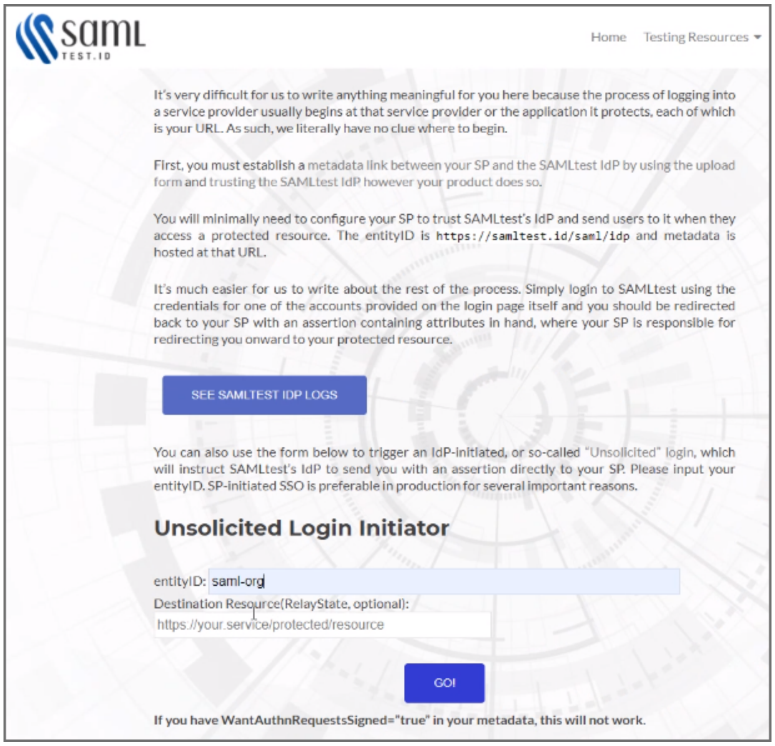
Mapped Role: Executive

Mapped Organization: Super/Local

Comment:

11. Go to https://samltest.id/ and navigate to **Testing Resources > Test Your SP**.

12. On the Test Your SP page, in the **entityID** field, enter your entityID, and click **GO!**.



It's very difficult for us to write anything meaningful for you here because the process of logging into a service provider usually begins at that service provider or the application it protects, each of which is your URL. As such, we literally have no clue where to begin.

First, you must establish a metadata link between your SP and the SAMLtest IdP by using the upload form and trusting the SAMLtest IdP however your product does so.

You will minimally need to configure your SP to trust SAMLtest's IdP and send users to it when they access a protected resource. The entityID is `https://samltest.id/saml/idp` and metadata is hosted at that URL.

It's much easier for us to write about the rest of the process. Simply login to SAMLtest using the credentials for one of the accounts provided on the login page itself and you should be redirected back to your SP with an assertion containing attributes in hand, where your SP is responsible for redirecting you onward to your protected resource.

SEE SAMLTEST IDP LOGS

You can also use the form below to trigger an IdP-initiated, or so-called "Unsolicited" login, which will instruct SAMLtest's IdP to send you with an assertion directly to your SP. Please input your entityID. SP-initiated SSO is preferable in production for several important reasons.

Unsolicited Login Initiator

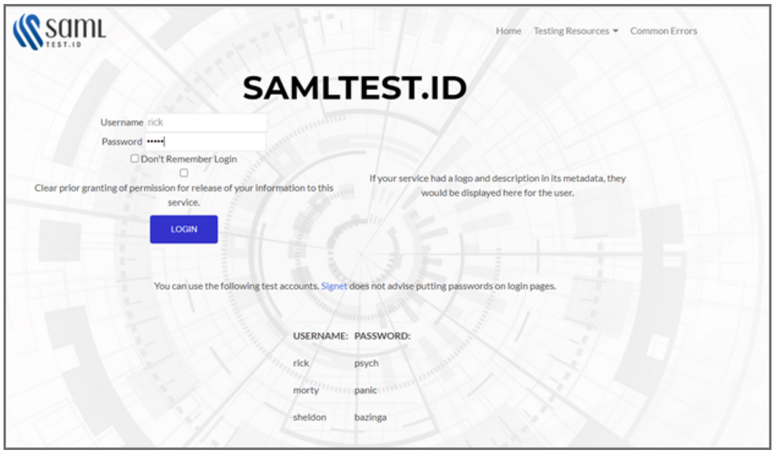
entityID: saml-org

Destination Resource(RelayState, optional): https://your.service/protected/resource

GO!

If you have WantAuthnRequestsSigned="true" in your metadata, this will not work.

13. In the **Username** and **Password** fields, enter your user name and password respectively, and click **LOGIN**.



SAMLTEST.ID

Username rick

Password •••••

□ Don't Remember Login

□ Clear prior granting of permission for release of your information to this service.

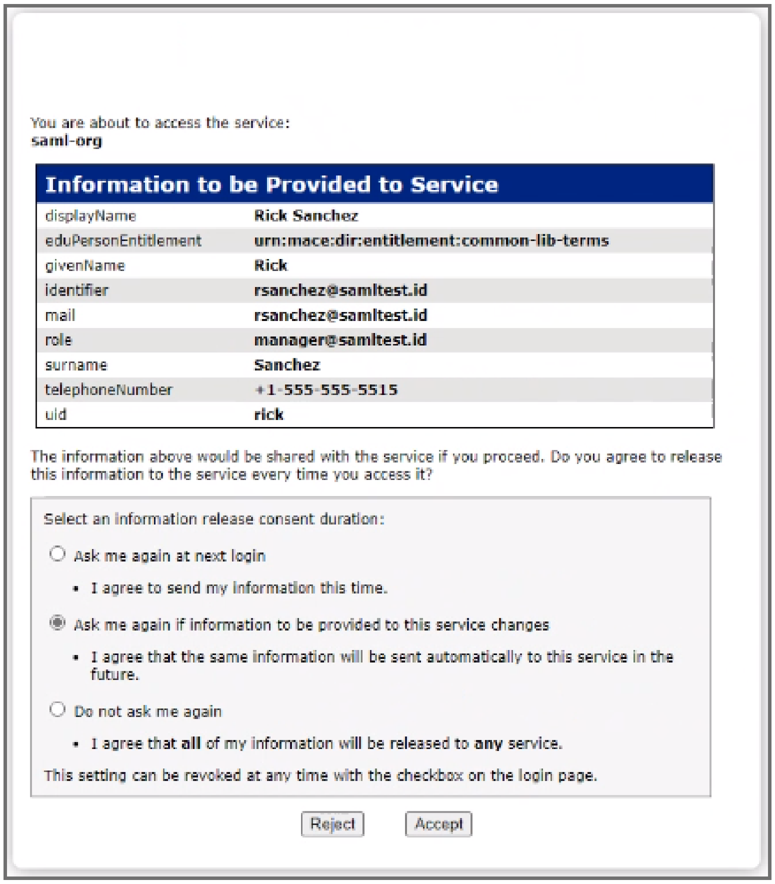
LOGIN

If your service had a logo and description in its metadata, they would be displayed here for the user.

You can use the following test accounts. Signet does not advise putting passwords on login pages.

USERNAME:	PASSWORD:
rick	psych
morty	panic
sheldon	bazinga

14. SAMLTEST.ID will prompt with choices for logging in. Select your choice, and click **Accept** to login to FortiSIEM.



You are about to access the service:
saml-org

Information to be Provided to Service	
displayName	**Rick Sanchez**
eduPersonEntitlement	**urn:mace:dir:entitlement:common-lib-terms**
givenName	**Rick**
identifier	**rsanchez@samltest.id**
mail	**rsanchez@samltest.id**
role	**manager@samltest.id**
surname	**Sanchez**
telephoneNumber	**+1-555-555-5515**
uid	**rick**

The information above would be shared with the service if you proceed. Do you agree to release this information to the service every time you access it?

Select an information release consent duration:

○ Ask me again at next login

- I agree to send my information this time.

● Ask me again if information to be provided to this service changes

- I agree that the same information will be sent automatically to this service in the future.

○ Do not ask me again

- I agree that **all** of my information will be released to **any** service.

This setting can be revoked at any time with the checkbox on the login page.

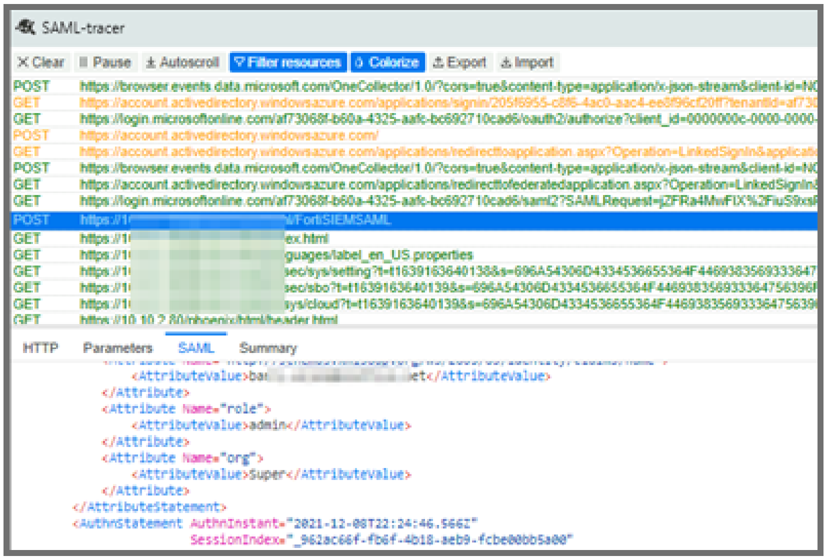
Troubleshooting SAML Configuration

- Plugin Tool
- Issues after Successful Authentication
- Common Configuration Errors
- SAML Login Error Codes

Plugin Tool

One way to troubleshoot a SAML response is to install the SAML-tracer Google Chrome plugin.

It will display the complete SAML response, with the actual attributes being returned. You can then check what the `AudienceRestriction` or expected Custom Attributes are and whether you have mapped them correctly.

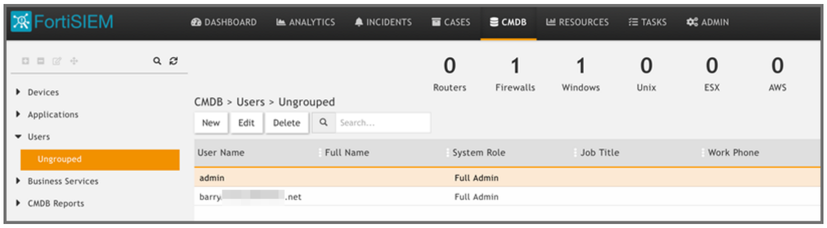


```
POST   https://browser.events.data.microsoft.com/OneCollector/1.0/?cors=true&content-type=application/x-json-stream&client-id=NO
GET    https://account.activedirectory.windowsazure.com/applications/signin/205f6955-c8f6-4ac0-aac4-ee8f96cf20ff?tenantId=af730
GET    https://login.microsoftonline.com/af73068f-b60a-4325-aafc-bc692710cad6/oauth2/authorize?client_id=0000000c-0000-0000-
POST   https://account.activedirectory.windowsazure.com/
GET    https://account.activedirectory.windowsazure.com/applications/redirecttoapplication.aspx?Operation=LinkedSignIn&applicati
POST   https://browser.events.data.microsoft.com/OneCollector/1.0/?cors=true&content-type=application/x-json-stream&client-id=NO
GET    https://account.activedirectory.windowsazure.com/applications/redirecttofederatedapplication.aspx?Operation=LinkedSignIn&
GET    https://login.microsoftonline.com/af73068f-b60a-4325-aafc-bc692710cad6/saml2?SAMLRequest=jZFRa4MwFIX%2FiuS9xsP
POST   https://1[redacted]/FortiSIEMSAML
GET    https://1[redacted]ex.html
GET    https://1[redacted]guages/label_en_US.properties
GET    https://1[redacted]sec/sys/setting?t=t1639163640138&s=696A54306D4334536655364F446938356933364
GET    https://1[redacted]sec/sbo?t=t1639163640139&s=696A54306D4334536655364F4469383569333647563961
GET    https://1[redacted]sys/cloud?t=t1639163640139&s=696A54306D4334536655364F446938356933364756396
GET    https://10.10.2.80/phoenix/html/header.html
```

```
        <AttributeValue>ba[redacted]et</AttributeValue>
    </Attribute>
    <Attribute Name="role">
        <AttributeValue>admin</AttributeValue>
    </Attribute>
    <Attribute Name="org">
        <AttributeValue>Super</AttributeValue>
    </Attribute>
</AttributeStatement>
<AuthnStatement AuthnInstant="2021-12-08T22:24:46.566Z"
                SessionIndex="_962ac66f-fb6f-4b18-aeb9-fcbe00bb5a00"
```

Issues after Successful Authentication

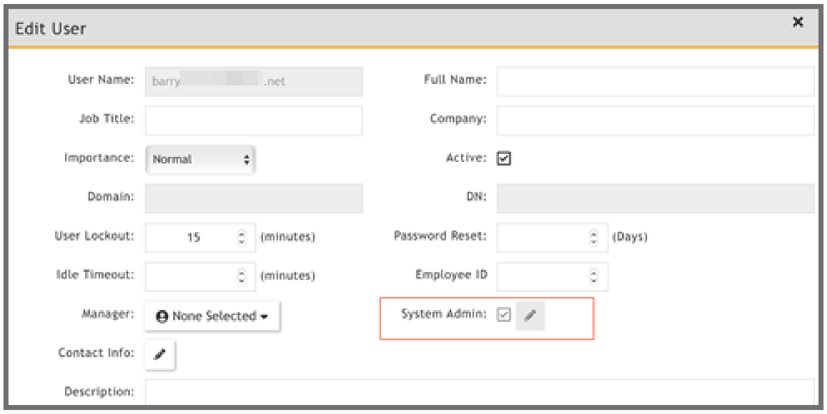
When the logged in user is automatically added to the CMDB.



CMDB > Users > Ungrouped

User Name	Full Name	System Role	Job Title	Work Phone
admin		Full Admin		
barry[redacted].net		Full Admin		

Some fields are Read Only, for example the System Admin flag.



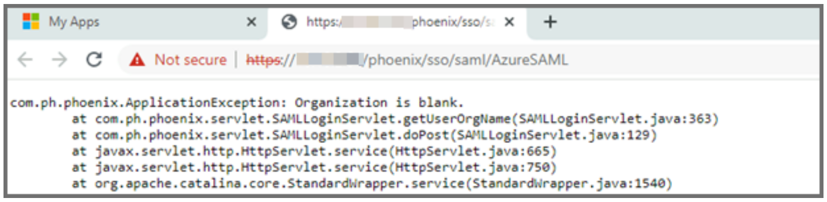
Edit User

User Name:	barry[redacted].net	Full Name:	
Job Title:		Company:	
Importance:	Normal	Active:	☑
Domain:		DN:	
User Lockout:	15 (minutes)	Password Reset:	(Days)
Idle Timeout:	(minutes)	Employee ID	
Manager:	None Selected	System Admin:	☑
Contact Info:			
Description:			

Common Configuration Errors

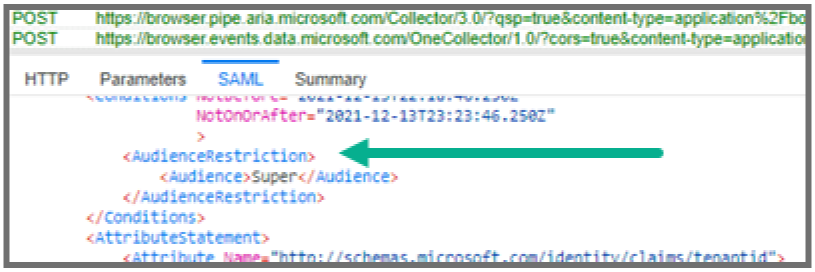
Organization is Blank

If you get a message saying "Organization is blank", check that the Org definition in the FortiSIEM External Authentication Profile is correct and mapped to the output from the SAML response.


My Apps
https:/[redacted]phoenix/sso/s
Not secure
https://[redacted]/phoenix/sso/saml/AzureSAML

```
com.ph.phoenix.ApplicationException: Organization is blank.
        at com.ph.phoenix.servlet.SAMLLoginServlet.getUserOrgName(SAMLLoginServlet.java:363)
        at com.ph.phoenix.servlet.SAMLLoginServlet.doPost(SAMLLoginServlet.java:129)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:665)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:750)
        at org.apache.catalina.core.StandardWrapper.service(StandardWrapper.java:1540)
```

I.e. either `AudienceRestriction` or your Custom Attribute definition:

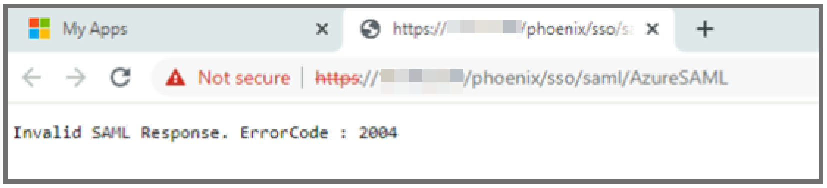


```
POST     https://browser.pipe.aria.microsoft.com/Collector/3.0/?qsp=true&content-type=application%2Fbo
POST     https://browser.events.data.microsoft.com/OneCollector/1.0/?cors=true&content-type=applicatio
```

```
                    NotOnOrAfter="2021-12-13T23:23:46.250Z"
                    >
            <AudienceRestriction>
                <Audience>Super</Audience>
            </AudienceRestriction>
        </Conditions>
        <AttributeStatement>
            <Attribute Name="http://schemas.microsoft.com/identity/claims/tenantid">
```

ErrorCode 2004

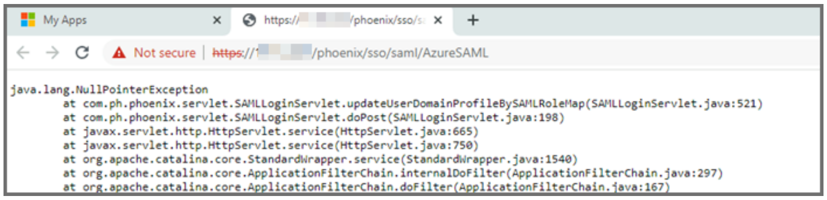
If you get the message "Invalid SAML Response. ErrorCode : 2004", check that the certificate definition in the FortiSIEM External Authentication Profile is correct.


My Apps
https://[redacted]/phoenix/sso/s
Not secure
https://[redacted]/phoenix/sso/saml/AzureSAML

```
Invalid SAML Response. ErrorCode : 2004
```

UpdateUserDomainProfileBySAMLRoleMap Issue

If you run into the following issue, check that the Role definition in the FortiSIEM External Authentication Profile is correct.


My Apps
https://[redacted]/phoenix/sso/s
Not secure
https://1[redacted]/phoenix/sso/saml/AzureSAML

```
java.lang.NullPointerException
        at com.ph.phoenix.servlet.SAMLLoginServlet.updateUserDomainProfileBySAMLRoleMap(SAMLLoginServlet.java:521)
        at com.ph.phoenix.servlet.SAMLLoginServlet.doPost(SAMLLoginServlet.java:198)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:665)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:750)
        at org.apache.catalina.core.StandardWrapper.service(StandardWrapper.java:1540)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:297)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:167)
```

SAML Login Error Codes

Error Code 1000-2000: Invalid SAML Configuration

Error Code 2000-3000: Invalid SAML Response

Error Code 3000-4000: Invalid username or password or organization

Incident Notification Settings

Notification Policies handles the sending of notifications when an incident occurs. Instead of setting notifications for each rule, you can create a policy and apply it to multiple rules.

The following section describes the procedures to enable Incident Notification settings:

- Adding Incident Notification Settings
- Modifying Incident Notification Settings
- Enabling Notification Policies

Adding Incident Notification Settings

1. Go to **ADMIN** > **Settings** > **General** > **Notification Policy** tab.
2. Click **New**.
3. Select the **Severity**.
4. For **Rules**, click the drop-down and select the rule or rules you want to trigger this notification from the folders.
5. Set a **Time Range** during which this notification will be in effect.
   Notifications will be sent only if an incident occurs during the time range you set here.
6. For **Affected Items**, click the drop-down and select the devices or applications from the **Select Devices** drop-down list for which this policy should apply.
   Instead of individual devices or groups, you can apply the notification policy to an IP address or range by clicking **Add IP/Range**. You can also select a group, and move to the **(NOT) Selections** column to explicitly exclude that group of applications or devices from the notification policy.
7. For Service Provider deployments, select the **Affected Orgs** to which the notification policy should apply.
   Notifications will be sent only if the triggering incidents affect the selected organization.
8. Select the **Action** to take when the notification is triggered.
   - Send Email/SMS to the target users. See here.
   - Run Remediation/Script. See here.
   - Invoke integration Policy. Click on **Run** to change policy. A drop-down list will appear. Select the policies you wish to invoke. For example, click on **FortiGUARD IOC Lookup** to invoke this integration policy, if it is available for your FortiSIEM environment.
   - Send SNMP message to the destination set in **ADMIN > Settings > Analytics > Incident Notification**.
   - Send XML file over HTTP(S) to the destination set in **ADMIN> Settings > Analytics > Incident Notification**.
   - Open Remedy ticket using the configuration set in **ADMIN > Settings > Analytics > Incident Notification**.
9. Select the **Settings** to enable the exceptions for notification trigger.
   - Do not notify when an incident is cleared automatically.
   - Do not notify when an incident is cleared manually.
   - Do not notify when an incident is cleared by system.
10. Enter any **Comments** about the policy.
11. Click **Save**.

You can also create a duplicate notification by selecting a notification from the table and clicking **Clone**.

Remember to enable your notification policy after creating it. See Enabling Notification Policies.

Modifying Incident Notification Settings

Complete these steps to modify an Incident Notification setting.

1. Go to **ADMIN** > **Settings** > **General** > **Notification Policy** tab.
2. Use the following buttons to modify Incident Notification settings:
   - **Edit** - To edit an Incident Notification setting
   - **Delete** - To delete an Incident Notification setting
3. Click **Save**.

Enabling Notification Policies

Complete these steps to enable or disable a notification policy

1. Go to **ADMIN** > **Settings** > **General** > **Notification Policy** tab.
2. In the **Enabled** column, click on a notification policy's checkbox to enable or disable it.

Configuring External Integrations

This section describes how to configure FortiSIEM to integrate with external CMDB and ticket management systems and threat entity reputation systems. Currently out-of-the-box supported external systems include ticket management systems such as ServiceNow, Connectwise, Salesforce and Jira, and reputation systems, such as VirusTotal, RiskIQ and FortiGuard IOC lookup.

- Configuring Ticketing System Integrations
- Configuring Reputation System Integrations
- Configuring Communication through Proxies
- Modifying an External System Integration

Configuring Ticketing System Integrations

FortiSIEM integration helps to create a two-way linkage between external ticketing/work flow systems like ServiceNow, ConnectWise and Salesforce. The integration can be for Incidents and CMDB.

This involves two steps.

1. Create an integration.
2. Attach the integration to an Incident Notification Policy or run the integration on a schedule.

Four types of integrations are supported:

- **Incident Outbound Integration**: This integration creates a ticket in an external ticketing system from FortiSIEM incidents. When an incident triggers in FortiSIEM, a ticket is opened in the external ticketing system. Currently, this out-of-the-box integration is supported for ServiceNow, ConnectWise, Salesforce and Jira.
- **Incident Inbound Integration**: This integration updates FortiSIEM incident ticket state from external system ticket states. Specifically, when a ticket is closed in the external ticketing system, the incident is cleared in FortiSIEM and the ticket status is marked closed to synchronize with the external ticketing system. Currently, this out-of-the-box integration is supported for ServiceNow, ConnectWise, Salesforce and Jira.
- **CMDB Outbound Integration**: This integration populates an external CMDB from FortiSIEM CMDB. When a device is added or updated in FortiSIEM CMDB, a device can be created in the external ticketing system. Currently, this out-of-the-box integration is supported for ServiceNow, ConnectWise and Salesforce.
- **CMDB Inbound Integration**: This integration populates FortiSIEM CMDB from an external CMDB. It works for any external CMDB.

Integration with other systems can be built using the API.

- ServiceNow Integration
- Jira Integration
- ConnectWise Integration
- Salesforce Integration
- CMDB Inbound Integration

ServiceNow Integration

- ServiceNow SOAP Based Integration
- ServiceNow Security Operations (SecOps) Integration

ServiceNow SOAP Based Integration

- Configuring ServiceNow for FortiSIEM Integration
- FortiSIEM Incident Schema
- Incident Outbound Integration (Default)
- Incident Inbound Integration (Default)
- Incident Outbound Integration (Custom)
- Incident Inbound Integration (Custom)
- CMDB Outbound Integration (Default)
- Example Custom Integration

Configuring ServiceNow for FortiSIEM Integration

1. Log in to ServiceNow.
2. For Service Provider Configurations, create Companies by creating Company Name.
3. For the integrations to work, FortiSIEM needs to modify certain ServiceNow database tables.
    - If you are using default integration, make sure that the FortiSIEM user account has the permissions specified, see Required Permissions for ServiceNow SOAP Integration.
    - if you are using custom integration, then sure that the FortiSIEM user account has the read/write permissions on the specific ServicNow tables and columns.

FortiSIEM Incident Schema

The following FortiSIEM Incident fields are available for integration.

FortiSIEM Incident Field	Type	Description	Required for Custom Integration
Incident ID	64bit Integer	Incident Id in FortiSIEM database.	Optional for outbound
Incident Title	String	Incident Title is a formatted string to capture Incident details and actors .	Optional for outbound
Rule Name	String	The name of the rule that triggered the Incident.	Optional for outbound
Rule Description	String	The description of the rule that triggered the Incident.	Optional for outbound

FortiSIEM Incident Field	Type	Description	Required for Custom Integration
First Seen Time	64bit Integer	The first time an incident triggered in FortiSIEM. Format: Unix epoch timestamp (number of seconds that have elapsed since 00:00:00 UTC on 1 January 1970)	Optional for outbound
Last Seen Time	64bit Integer	The last time an incident triggered in FortiSIEM. Format: Unix epoch timestamp (number of seconds that have elapsed since 00:00:00 UTC on 1 January 1970)	Optional for outbound
Incident Severity	32bit integer – values 1-10	Severity of the Incident. Severities are increasing meaning 1 is lowest and 10 is highest.	Optional for outbound
Incident Severity Category	String – takes 3 values: LOW, MEDIUM, HIGH	Incident severity categorized into 3 levels: LOW, MEDIUM, HIGH	Optional for outbound
Incident Source	String	Incident source attributes in comma separated attribute:Value format. Following attributes are included: srcIpAddr	Optional for outbound
Incident Target	String	Incident destination in comma separated attribute:Value format. Following attributes are included: destIpAddr, destName, hostIpAddr, hostname, user, targetUser	Optional for outbound
Incident Detail	String	Incident details in comma separated attribute:Value format. All attributes not included in Incident Source and Incident target are included in this attribute.	Optional for outbound
Triggering Attributes	String	List of attributes present in the incident.	Optional for outbound
Incident Count	32bit integer	Number of times the incident triggered.	Optional for outbound
Host Name	String	Host Name in incident. This is also present in Incident Target.	Optional for outbound
Incident Comment	String	Comments added by user or by a notification script.	Optional for outbound
Status	32bit integer	Incident Status: 0 means Active, 1 means System Cleared, 2 means User Cleared.	Optional for outbound
Incident Resolution	String	Four values: Open, InProgress, TruePostive and FalsePositive	Optional for outbound
Rule Remediation Note	String		Optional for outbound

FortiSIEM Incident Field	Type	Description	Required for Custom Integration
External Ticket Id	String	ServiceNow Ticket Id	Required for both Inbound and Outbound
External Ticket State	String	ServiceNow Ticket State	Required for Inbound and must have a value mapping for "Closed"
External User	String	User who closed the Ticket in ServiceNow.	Optional for outbound
External Cleared Time	String	Time at which Incident cleared in ServiceNow.	Required for Inbound

There are two main requirements for a successful custom integration.

1. Outbound and Inbound – must have a mapping for External Ticket Id.
2. Inbound - External Ticket State must have value "Closed".
3. Inbound - must have a mapping for External Cleared Time.

Incident Outbound Integration (Default)

In this integration, you can create tickets in ServiceNow when an Incident triggers in FortiSIEM. In the Default integration, FortiSIEM Incidents are written to the ServiceNow **incident** table. FortiSIEM incident attributes are mapped to ServiceNow incident table columns as follows.

FortiSIEM Incident Attribute	ServiceNow Incident Table Column
Incident Status	work_notes
Incident Name	short_description
Incident Comments (generated string containing few Incident attributes – see Step 1.4.k.)	comments
Organization Name	company
Incident Severity	impact
Incident Severity	urgency

Step 1: Create an Integration

1. Log into your Supervisor node with administrator credentials.
2. Navigate to **ADMIN > Settings > General > External Integration**.
3. Click **New**.
4. From the **Integration Policy** window, take the following steps.
   a. From the **Type** drop-down list, select **Incident**.
   b. From the **Direction** drop-down list, select **Outbound**.

c. From the **Vendor** drop-down list, select **ServiceNow**. When you select a vendor, an instance is created, with a unique name for the policy. For example, if you had two ServiceNow installations, each would have different instance names.

d. For **Plugin Type**, select **Ticket**.

e. For **Plugin Name**, a default Plugin Name is populated. Leave it as is. This is the Java code that implements the integration, including connecting to the external help desk systems and synching the CMDB elements.

f. In the **Host/URL** field, enter the login URL, for example, `https://vendor123.service-now.com`.

g. In the **User Name** field, enter the ServiceNow username login credential.

h. In the **Password** field, enter the ServiceNow password login credential.

i. Leave the **ServiceNow Table Name** attribute alone.

j. In the **Description** field, enter a description as to what the integration does. This is for display purposes only.

k. For **Incident Comment**, you can keep the default format shown in Step 1.k.i, or create your own, shown in Step 1.k.ii.

    i. Default format : `[FortiSIEM]Incident Id:<val>;First seen time:<val>;Target IP:<val>;Incident Details:<val>;Mitre TechniqueId:<val>;Mitre Tactics:<val>; Description:<Rule Name>`

    ii. To create your own, click the Edit icon, and form a string by combining your own text and incident attributes by choosing from the Insert Content drop-down list. When done, click **Save**.

l. For **Organization Mapping**, click the Edit icon to create mappings between the Organizations in your FortiSIEM deployment and Company names in ServiceNow (created in Configuring ServiceNow for FortiSIEM Integration, Step 2).

m. For **Run For**, click the Edit icon, and choose the organizations for whom tickets will be created.

n. In the **Max Incidents** field, enter the maximum number of incidents you want to record.

o. Click **Save**.

Step 2: Link Integration to a Notification Policy

You need to link the integration to a notification policy, so that the integration runs when the notification policy triggers.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Notification Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Notification Settings** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

Incident Inbound Integration (Default)

Using this integration, a FortiSIEM Incident can be programmatically cleared when a user closes the corresponding ticket in ServiceNow. In the default integration, the following fields from ServiceNow **incident** table are mapped to FortiSIEM incident fields.

ServiceNow Incident Table Column	FortiSIEM Incident Field
incident_state	Incident Status
Closed_code	Incident Resolution
Closed_by	External User
number	External Ticket Id
incident_state	External Ticket Status

Step 1: Create an Incident Inbound Integration

1. Log into your Supervisor node with administrator credentials.
2. Navigate to **ADMIN > Settings > General > External Integration**.
3. Click **New**.
4. From the **Integration Policy** window, take the following steps.
    a. From the **Type** drop-down list, select **Incident**.
    b. From the **Direction** drop-down list, select **Inbound**.
    c. From the **Vendor** drop-down list, select **ServiceNow**. When you select a vendor, an instance is created, with a unique name for the policy. For example, if you had two ServiceNow installations, each would have different instance names.
    d. For **Plugin Type**, select **Ticket**.
    e. For **Plugin Name**, a default Plugin Name is populated. Leave it as is. This is the Java code that implements the integration, including connecting to the external help desk systems and synching the CMDB elements.
    f. In the **Host/URL** field, enter the login URL, for example, `https://vendor123.service-now.com`.
    g. In the **User Name** field, enter the ServiceNow username login credential.
    h. In the **Password** field, enter the ServiceNow password login credential.
    i. Leave the **ServiceNow Table Name** attribute alone.
    j. In the **Description** field, enter a description as to what the integration does. This is for display purposes only.
    k. For **Content Mapping**, do not make any edits. Keep the system defined one.
    l. In the **Time Window** field, enter/select the number of hours for which incident states will be synched from ServiceNow. For example, if time window is set to 10 hours, then the states of incidents that occurred in the last 10 hours will be synched.
    m. When done, click **Save**.

Step 2: Create an Incident Inbound Integration Schedule

This determines the schedule on which the inbound integration policy defined in **Step 1: Create an Incident Inbound Integration** will be run.

1. Log into your Supervisor node with administrator credentials.
2. Navigate to **ADMIN > Settings > General > External Integration**.
3. Click **Schedule**.

4. Click **+** to open the **Integration Policy Schedules** window.
    a. From the **Integration Policy** column, select your integration policy and move it to the **Selected** column.
    b. Under **Time Range**, configure your schedule by taking the following steps.
        i. In the **Start Time** field, enter the start time of your schedule.
        ii. From the **Local/UTC Time**and **Region** drop-down lists, configure the start time of the schedule.
    c. Under **Recurrence Pattern**, configure the frequency.
        a. Select **Once**, **Minutely**, **Hourly**, **Daily**, **Weekly**, or **Monthly** for the schedule's recurrence pattern. Depending on what is selected, configure the related date/time schedule attributes.
        b. In the **Start From** field, enter the date which the schedule starts.
    d. When done, click **Save**.

Incident Outbound Integration (Custom)

In this integration, you can create tickets in ServiceNow when an Incident triggers in FortiSIEM. You can choose your *own ServiceNow table* to map FortiSIEM Incidents to. Take the following steps to create a custom outbound integration.

Step 1: Create an Integration

1. Log into your Supervisor node with administrator credentials.
2. Navigate to **ADMIN > Settings > General > External Integration**.
3. Click **New**.
4. From the **Integration Policy** window, take the following steps.
    a. From the **Type** drop-down list, select **Incident**.
    b. From the **Direction** drop-down list, select **Outbound**.
    c. From the **Vendor** drop-down list, select **ServiceNow**. When you select a vendor, an instance is created, with a unique name for the policy. For example, if you had two ServiceNow installations, each would have different instance names.
    d. For **Plugin Type**, select **Ticket**.
    e. For **Plugin Name**, a default Plugin Name is populated. Leave it as is. This is the Java code that implements the integration, including connecting to the external help desk systems and synching the CMDB elements. For other vendors, you must create your own plugin and enter the plugin name here.
    f. In the **Host/URL** field, enter the login URL, for example, `https://vendor123.service-now.com`.
    g. In the **User Name** field, enter the ServiceNow username login credential.
    h. In the **Password** field, enter the ServiceNow password login credential.
    i. In the **ServiceNow Table Name** field, enter the custom ServiceNow table
    j. In the **Description** field, enter a description as to what the integration does. This is for display purposes only.
    k. For **Incident Comment**, you can keep the default format shown in Step 1.k.i, or create your own, shown in Step 1.k.ii.
        i. Default format : `[FortiSIEM]Incident Id:<val>;First seen time:<val>;Target IP:<val>;Incident Details:<val>;Mitre TechniqueId:<val>;Mitre Tactics:<val>; Description:<Rule Name>`
        ii. To create your own, click the Edit icon, and form a string by combining your own text and incident attributes by choosing from the Insert Content drop-down list. When done, click **Save**.

l. For **Organization Mapping**, click the Edit icon to create mappings between the Organizations in your FortiSIEM deployment and Company names in ServiceNow (created in Configuring ServiceNow for FortiSIEM Integration, Step 2).
m. For **Run For**, click the Edit icon, and choose the organizations for whom tickets will be created.
n. For **Content Mapping**, click the Edit icon to define mappings between FortiSIEM Incident fields and ServiceNow custom table columns.
    i. Select the **Field Mappings** dialog box and click **+**.
       Note: To delete a Field Mapping, select the entry and click **-**. To edit a Field Mapping, click the Edit icon.
    ii. From the **FortiSIEM Incident Field** drop-down list, select a FortiSIEM Incident field.
    iii. From the **ServiceNow Field** drop-down list, select a mapped ServiceNow field. Note that the menu is populated from the table in step 4.i.
    iv. Select the **Value Mappings** dialog box and click **+** to enter Value Mappings if you want the values for a specific field to be transformed. A standard example is Severity, where FortiSIEM Incident Severity 1-> 4 may be mapped to Low, 5-8 as Medium and 9-10 as High.
    v. From **Field**, select the ServiceNow Field whose values need to be transformed.
    vi. In the **From** field, select the value that FortiSIEM generates.
    vii. In the **To** field, select the value that you want ServiceNow to store.
    viii. When done, click **Save**.
o. In the **Max Incidents** field, enter the maximum number of incidents you want to record.
p. Click **Save**.

Step 2: Link Integration to a Notification Policy

You need to link the integration to a notification policy, so that the integration runs when the notification policy triggers.

Note: In the default Outbound integration, Incident updates are recorded in the comments field. However, in the custom integration, Incident updates are not reflected in ServiceNow.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Notification Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Notification Settings** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

Incident Inbound Integration (Custom)

In this integration, you can clear tickets in FortiSIEM when a user closes the corresponding ServiceNow ticket. You can choose your *own ServiceNow table* to update the following FortiSIEM Incident fields:

- External Ticket Id
- Incident Status
- Incident Resolution

- External User
- External Ticket State

Step 1: Create an Incident Inbound Integration

1. Log into your Supervisor node with administrator credentials.
2. Navigate to **ADMIN > Settings > General > External Integration**.
3. Click **New**.
4. From the **Integration Policy** window, take the following steps.
    a. From the **Type** drop-down list, select **Incident**.
    b. From the **Direction** drop-down list, select **Inbound**.
    c. From the **Vendor** drop-down list, select **ServiceNow**. When you select a vendor, an instance is created, with a unique name for the policy. For example, if you had two ServiceNow installations, each would have different instance names.
    d. For **Plugin Type**, select **Ticket**.
    e. For **Plugin Name**, a default Plugin Name is populated. Leave it as is. This is the Java code that implements the integration, including connecting to the external help desk systems and synching the CMDB elements.
    f. In the **Host/URL** field, enter the login URL, for example, `https://vendor123.service-now.com`.
    g. In the **User Name** field, enter the ServiceNow username login credential.
    h. In the **Password** field, enter the ServiceNow password login credential.
    i. For the **ServiceNow Table Name**, choose your custom ServiceNow table.
    j. In the **Description** field, enter a description as to what the integration does. This is for display purposes only.
    k. For **Content Mapping**, click the Edit icon to define mappings between FortiSIEM Incident fields and ServiceNow custom table columns.
        i. Select the **Field Mappings** dialog box and click **+**.
        Note: To delete a Field Mapping, select the entry and click **-**. To edit a Field Mapping, click the Edit icon.
        ii. From the **FortiSIEM Incident Field** drop-down list, select a FortiSIEM Incident field.
        iii. From the **ServiceNow Field** drop-down list, select a mapped ServiceNow field. Note that the menu is populated from the table in step 4.i.
        iv. Select the **Value Mappings** dialog box and click **+** to enter Value Mappings if you want the values for a specific field to be transformed. For the Incident Inbound Integration to function, we need a mapping to the “Closed” value of FortiSIEM Incident Status field. This allows FortiSIEM to close an Incident.
        v. From **Field**, select the ServiceNow Field whose values need to be transformed.
        vi. In the **From** field, select the value that FortiSIEM generates.
        vii. In the **To** field, select the value that you want ServiceNow to store.
        viii. When done, click **Save**.
    l. In the **Time Window** field, enter/select the number of hours for which incident states will be synched from ServiceNow. For example, if time window is set to 10 hours, then the states of incidents that occurred in the last 10 hours will be synched.
    m. When done, click **Save**.

Step 2: Create an Incident Inbound Integration Schedule

This determines the schedule on which the inbound integration policy defined in **Step 1: Create an Incident Inbound Integration** will be run.

1. Log into your Supervisor node with administrator credentials.
2. Navigate to **ADMIN > Settings > General > External Integration**.
3. Click **Schedule**.
4. Click **+** to open the **Integration Policy Schedules** window.
    a. From the **Integration Policy** column, select your integration policy and move it to the **Selected** column.
    b. Under **Time Range**, configure your schedule by taking the following steps.
        i. In the **Start Time** field, enter the start time of your schedule.
        ii. From the **Local/UTC Time**and **Region** drop-down lists, configure the start time of the schedule.
    c. Under **Recurrence Pattern**, configure the frequency.
        a. Select **Once**, **Minutely**, **Hourly**, **Daily**, **Weekly**, or **Monthly** for the schedule's recurrence pattern. Depending on what is selected, configure the related date/time schedule attributes.
        b. In the **Start From** field, enter the date which the schedule starts.
    d. When done, click **Save**.

CMDB Outbound Integration (Default)

CMDB Outbound Integration populates an external CMDB from FortiSIEM’s own CMDB. Built in integrations are available for ServiceNow.

Step 1: Create a CMDB Outbound integration

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Device**.
5. For **Direction**, select **Outbound**.
6. For **Vendor**, select the vendor of the system you want to connect to. ServiceNow is supported out of the box. When you select the Vendor:
    a. An **Instance** is created - this is the unique name for this policy. For example if you had 2 ServiceNow installations, each would have different Instance names.
    b. A default **Plugin Name** is populated - this is the Java code that implements the integration including connecting to the external help desk systems and synching the CMDB elements. The plugin is automatically populated for ServiceNow. For other vendors, you have to create your own plugin and type in the plugin name here.
7. For **Host/URL**, enter the host name or URL of the external system. For ServiceNow, select the login URL
8. For **User Name** and **Password**, enter a user name and password that the system can use to authenticate with the external system. For ServiceNow, select the login credentials.
9. In **Attribute Mapping**, specify the mapping of attributes to resources.

10. For **Organization Mapping**, click **Edit** to create mappings between the organizations in your FortiSIEM deployment and the names of the organization in the external system. For ServiceNow, select the Company names as in Configuring ServiceNow for FortiSIEM Integration, Step 2.
11. For **Run For**, choose the organizations for whom tickets will be created.
12. For **Groups**, select the FortiSIEM CMDB Groups whose member devices would be synched to external CMDB.
13. Select **Run after Discovery** if you want this export to take place after you have run discovery in your system. This is the only way to push automatic changes from FortiSIEM to the external system.
14. Enter the **Maximum** number of devices to send to the external system.
15. Click **Save**.

Step 2: Create a CMDB Outbound integration schedule

Updating external CMDB automatically after FortiSIEM discovery:

1. Create an integration policy.
2. Make sure **Run after Discovery** is checked.
3. Click **Save**.

Updating external CMDB on a schedule:

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **Schedule** and then click **+**.
   a. Select the integration policies.
   b. Select a schedule.

Updating external CMDB on-demand (one-time):

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Select a specific integration policy and click **Run**.

Example Custom Integration

This section provides a sample integration.

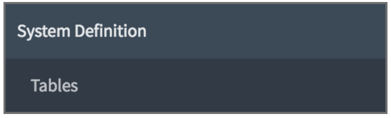
There are a few main requirements for a successful custom integration

1. Outbound and Inbound – must have a mapping for External Ticket Id
2. Inbound - External Ticket State must have value “Closed”
3. Inbound - must have a mapping for External Cleared Time

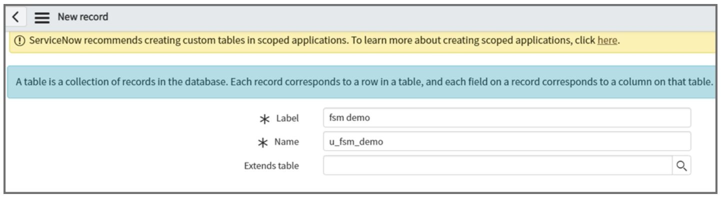
Follow these steps:

Step 1. From ServiceNow, take the following steps to create a ServiceNow Table.

1. Login to ServiceNow.
2. From the left pane, navigate to **System Definitions > Tables**.



3. Next to the heading **Tables**, click **New** to create a table.
   a. In the **Label** field, enter a label. Here, we can use "fsm demo". The **Name** field will be automatically populated. Keep this name recorded, as it will be needed later.



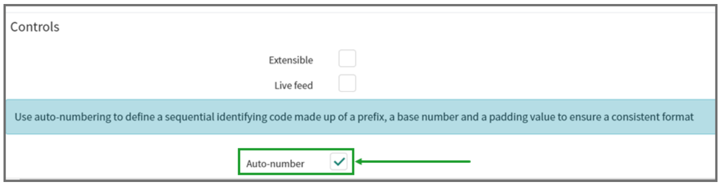
New record

ServiceNow recommends creating custom tables in scoped applications. To learn more about creating scoped applications, click here.

A table is a collection of records in the database. Each record corresponds to a row in a table, and each field on a record corresponds to a column on that table.

* Label: fsm demo
* Name: u_fsm_demo
Extends table:

   b. Under **Controls**, check the **Auto-number** checkbox. This is required to map the External Ticket Id.



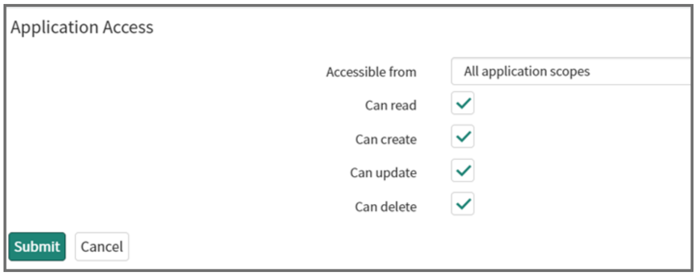
Controls

Extensible □
Live feed □

Use auto-numbering to define a sequential identifying code made up of a prefix, a base number and a padding value to ensure a consistent format

Auto-number ☑

   c. Under **Application Access**, check the following checkboxes.
      - Can read
      - Can create
      - Can update
      - Can delete



Application Access

Accessible from: All application scopes
Can read ☑
Can create ☑
Can update ☑
Can delete ☑

Submit Cancel

   d. Click **Submit**.
   A ServiceNow table has now been created.
4. Next to the heading **Table Columns**, click **New** to create a table column.
   a. Create your column/mappings and ensure that **Type** is set correctly (See FortiSIEM Incident Schema for the correct Types). For this example, we use the following:
   Type: String
   Column label: ticketnumber
   Note: For External Ticket ID
   Max length: 256
   b. **Type**: String
   Column label: externalcleartime

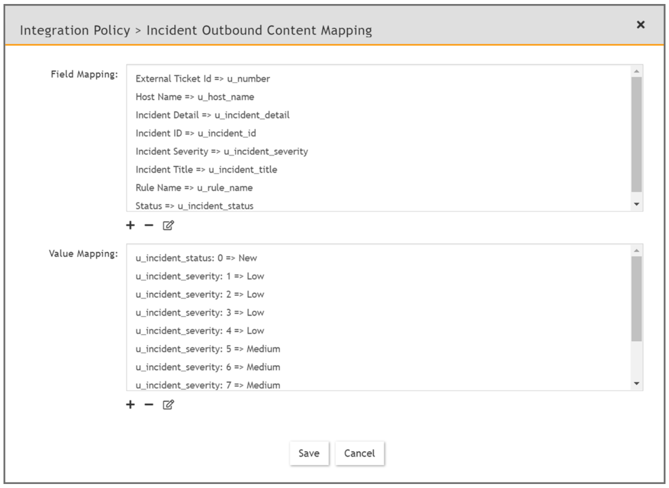
    Note: For External Cleared Time
    Max length: 256

   c. **Type**: String
      Column label: incident_status
      Note: For Ticket Status
      Max length: 256
   d. Configure any additional mappings necessary for your ServiceNow table.
      To create a drop-down list, navigate to **Choice List Specification**, and from the **Choice** drop-down list, make a selection. To configure what will appear in your drop-down list, click the **Advanced view** link, and under **Choices**, click **New** to add items to appear in your drop-down list.

5. When done, click **Submit**.

Step 2. From FortiSIEM, take the following steps to create Incident Outbound Integration Policy.

1. Login to FortiSIEM.
2. Navigate to **ADMIN > Settings > General > External Integration**.
3. Click **New** to create an Integration Policy, and take the following steps.
   a. From the **Type** drop-down list, select **Incident**.
   b. From the **Direction** drop-down list, select **Outbound**.
   c. From the **Vendor** drop-down list, select **ServiceNow**.
   d. In the **Host/URL** field, enter the ServiceNow URL being used.
   e. In the **User Name** field, enter the ServiceNow username credential.
   f. In the **Password** and **Confirm Password** field, enter the password associated with the ServiceNow User Name account.
   g. In the **ServiceNow Table Name** field, enter the name of the ServiceNow table that was set up during the ServiceNow table creation.
   h. In the **Content Mapping** row, click the Edit icon.
   i. In the **Integration Policy > Incident Outbound Content Mapping** window, take the following steps.
      i. From the **FortiSIEM Incident Field** drop-down list, select **External Ticket Id**.
      ii. From the **ServiceNow Field** drop-down list, select the "ticketnumber" mapping.
      iii. From the **FortiSIEM Incident Field** drop-down list, select **External Ticket State**.
      iv. From the **ServiceNow Field** drop-down list, select the "externalcleartime" mapping.
      A more complicated custom mapping is provided in the following screenshot.



Integration Policy > Incident Outbound Content Mapping

Field Mapping:

External Ticket Id => u_number
Host Name => u_host_name
Incident Detail => u_incident_detail
Incident ID => u_incident_id
Incident Severity => u_incident_severity
Incident Title => u_incident_title
Rule Name => u_rule_name
Status => u_incident_status

Value Mapping:

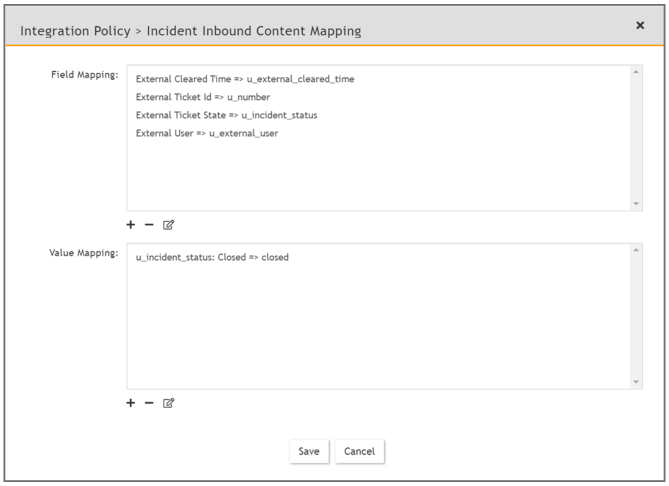
u_incident_status: 0 => New
u_incident_severity: 1 => Low
u_incident_severity: 2 => Low
u_incident_severity: 3 => Low
u_incident_severity: 4 => Low
u_incident_severity: 5 => Medium
u_incident_severity: 6 => Medium
u_incident_severity: 7 => Medium

v. **Click Save**.

j. Click **Save**.
Your Outbound Integration Policy has been created.

Step 3. From FortiSIEM, take the following steps to create Incident Inbound Integration Policy.

1. Click **New** to create an Integration Policy, and take the following steps.
   a. From the **Type** drop-down list, select **Incident**.
   b. From the **Direction** drop-down list, select **Inbound**.
   c. From the **Vendor** drop-down list, select **ServiceNow**.
   d. In the **Host/URL** field, enter the ServiceNow URL being used.
   e. In the **User Name** field, enter the ServiceNow username credential.
   f. In the **Password** and **Confirm Password** field, enter the password associated with the ServiceNow User Name account.
   g. In the **ServiceNow Table Name** field, enter the name of the ServiceNow table that was set up during the ServiceNow table creation.
   h. In the **Content Mapping** row, click the Edit icon.
   i. In the **Integration Policy > Incident Outbound Content Mapping** window, take the following steps.
      i. From the **FortiSIEM Incident Field** drop-down list, select from External Cleared Time, External Ticket Id, External Ticket State, External User, or Incident Resolution.
      Note: External Ticket ID and External Ticket State are required.
      ii. From the **ServiceNow Field** drop-down list, select the corresponding column.
      iii. **Click Save**.
      iv. Repeat i.-iii. for any additional mappings. Proceed to v. when done with incident mapping.
      v. In **Value Mapping**, click **+** .
      vi. In the **Field** drop-down list, select the ServiceNow "external ticket state".
      vii. In the **From** field, enter "Closed".
      The value mapping should appear similar to the following example: `u_incident_status: Closed => closed`



Field Mapping:

External Cleared Time => u_external_cleared_time
External Ticket Id => u_number
External Ticket State => u_incident_status
External User => u_external_user

Value Mapping:

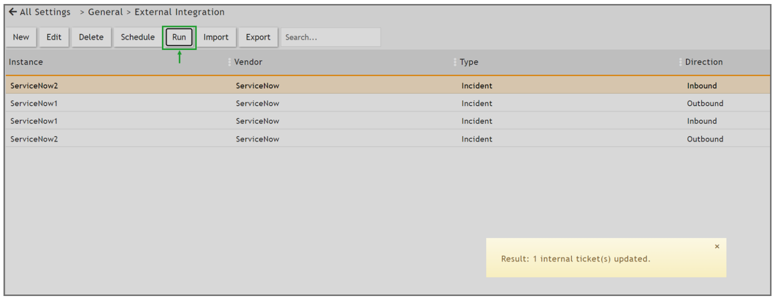
u_incident_status: Closed => closed

viii. Click **Save**.

j. Click **Save**.
Your Inbound Integration Policy has been created. Now, if you close an incident/ticket in ServiceNow, and run the inbound integration in FortiSIEM, the incident/ticket will also be closed.

Step 4. Run Outbound Integration

1. Confirm you are on the External Integration page. (**ADMIN > Settings > General > External Integration**)
2. Select the Outbound Integration you created.
3. Click **Run**.
   Note: The maximum number of incidents can be configured by changing the value of the **Max Incidents** field in your Outbound Integration Notification policy .



Instance	Vendor	Type	Direction
ServiceNow2	ServiceNow	Incident	Inbound
ServiceNow1	ServiceNow	Incident	Outbound
ServiceNow1	ServiceNow	Incident	Inbound
ServiceNow2	ServiceNow	Incident	Outbound

Result: 1 internal ticket(s) updated.

4. Click **Yes** to confirm.

Step 5. Run Inbound Integration

1. Confirm you are on the External Integration page. (**ADMIN > Settings > General > External Integration**)
2. Select the Inbound Integration you created.
3. Click **Run**.
   Note: You can verify the closing of an incident/ticket by checking the **External Ticket State** column.

Jira Integration

- Configuring Jira for FortiSIEM Integration
- Jira Incident Outbound Integration
- Jira Incident Inbound Integration

Configuring Jira for FortiSIEM Integration

Before configuring Jira, you must log in to your Jira account and create an API Key. Follow these steps.

1. Log in to your Jira account.
2. Create an API Key.
3. Use the GUI user name and API Key in FortiSIEM.

Jira Incident Outbound Integration

Jira outbound integration allows a user to map FortiSIEM fields to Jira ticket fields and to create incidents in Jira. When the integration runs, FortiSIEM looks for incidents that match the mappings and creates a ticket in the Jira system.

To create an outbound integration, follow these steps.

Step 1: Create an Integration

1. Go to **Admin > Settings > General > External Integration**.
2. Click **New** to create a new integration or **Edit** to modify an existing integration.
3. In the **Integration Policy** dialog box, provide the following values:
   - **Type**: select **Incident**.
   - **Direction**: select **Outbound**.
   - **Vendor**: select **Jira**.
   - **Instance**: enter an instance name or accept the default.
   - **Plugin Name**: is pre-populated with the name of the Jira integration class: `com.accelops.phoenix.jira.JiraTicketIntegration`.
   - **Host/URL**, enter the URL of the Jira provider, for example, `https://<`*`customer`*`>.atlassian.net`.
   - **Username** and **Password**, enter your Jira user name and password.
4. Click the edit icon next to **Field Mapping**.
5. In the **Field Mapping** dialog box, provide the following values:
   - **Project**: enter a name for the project
   - **Issue Type**: select Event.
   - The **Summary**: field is pre-populated with the **Incident Rule Name (**`$ruleName`**)**.
   - For **Description**: click the edit icon to build the expression for the Jira issue description. The drop-down list contains FortiSIEM fields that can be mapped to.
   - The **Priority**: field is pre-populated with **Incident Severity Category (**`$incident_severityCat`**)**.
6. Create mappings between Jira fields and FortiSIEM fields by clicking **New**.
   Select Jira fields from the upper drop-down list and match them with corresponding FortiSIEM fields in the lower drop-down list.

7. Click **Save** when you are finished mapping fileds. The mappings are reflected in the table in the Field Mapping dialog box.
   Note: Click **Cancel** to dismiss the **Mapping Fields** dialog box.

Step 2: Link Integration to a Notification Policy

You need to link the integration to a notification policy, so that the integration runs when the notification policy triggers.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Notification Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Notification Settings** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

Jira Incident Inbound Integration

Jira inbound integration allows a user to close a ticket in FortiSIEM if the ticket is closed in Jira.

To create an inbound integration, follow these steps.

Step 1: Create an Integration

1. Go to **Admin > Settings > General > External Integration**.
2. Click **New** to create a new integration or **Edit** to modify an existing integration.
3. In the **Integration Policy** dialog box, provide the following values:
   - **Type**: select **Incident**.
   - **Direction**: select **Inbound**.
   - **Vendor**: select **Jira**.
   - **Instance**: enter an instance name or accept the default.
   - **Plugin Name**: is pre-populated with the name of the Jira integration class: `com.accelops.phoenix.jira.JiraTicketIntegration`.
   - **Host/URL**, enter the URL of the Jira provider, for example, `https://<customer>.atlassian.net`.
   - **Username** and **Password**, enter your Jira user name and password.
   - **Description**: enter an optional description of the integration.
   - **Time Window**: enter the number of hours for which incident states will be synched. For example, if time windows is set to 10 hours, the states of incidents that occurred in the last 10 hours will be synched.
4. Click the edit icon next to **Field Mapping**.
5. In the Field Mapping dialog box, provide the following values:
   - **Project**: enter a name for the project.
   - **Issue Type**: select **Event**.
   - The **Summary**: field is pre-populated with the **Incident Rule Name (**`$ruleName`**)**.
   - For **Description**: click the edit icon to build the expression for the Jira issue description. The drop-down list contains FortiSIEM fields that can be mapped to.
   - The **Priority**: field is pre-populated with **Incident Severity Category (**`$incident_severityCat`**)**.

6. Create mappings between Jira fields and FortiSIEM fields by clicking **New**.
   Select Jira fields from the upper drop-down list and match them with corresponding FortiSIEM fields in the lower drop-down list.
7. Click **Save** when you are finished mapping fileds. The mappings are reflected in the table in the Field Mapping dialog box.
   Note: Click **Cancel** to dismiss the **Mapping Fields** dialog box.

Step 2: Create an Incident Inbound Integration Schedule

This determines the schedule on which the inbound integration policy defined in **Step 1: Create an Incident Inbound Integration** will be run.

1. Log into your Supervisor node with administrator credentials.
2. Navigate to **ADMIN > Settings > General > External Integration**.
3. Click **Schedule**.
4. Click **+** to open the **Integration Policy Schedules** window.
   a. From the **Integration Policy** column, select your integration policy and move it to the **Selected** column.
   b. Under **Time Range**, configure your schedule by taking the following steps.
      i. In the **Start Time** field, enter the start time of your schedule.
      ii. From the **Local/UTC Time**and **Region** drop-down lists, configure the start time of the schedule.
   c. Under **Recurrence Pattern**, configure the frequency.
      a. Select **Once**, **Minutely**, **Hourly**, **Daily**, **Weekly**, or **Monthly** for the schedule's recurrence pattern. Depending on what is selected, configure the related date/time schedule attributes.
      b. In the **Start From** field, enter the date which the schedule starts.
   d. When done, click **Save**.

ConnectWise Integration

- Adding a Client ID for ConnectWise Integration
- Configuring ConnectWise for FortiSIEM Integration
- ConnectWise Incident Outbound Integration
- ConnectWise Incident Inbound Integration
- ConnectWise CMDB Outbound Integration

Adding a Client ID for ConnectWise Integration

ConnectWise has recently changed their policy and requires that vendors create a client ID in order to integrate with FortiSIEM. Due to this change and restriction from ConnectWise, Fortinet has published a public client ID in order to allow clients to integrate with ConnectWise. This Client ID is `1a7ed749-47a1-4d3e-94b0-696288a1140f`.

Note: A ConnectWise working account is required before integration can occur.

To add this client ID for ConnectWise, take the following steps.

1. Go to **ADMIN > Settings >General > External Integration**.
2. Click **New** to create a new Integration Policy or select an existing Integration Policy and click **Edit**.
3. From the **Vendor** drop-down list, select **ConnectWise**.

4. In the **Client ID** field, paste the following Client ID:
   `1a7ed749-47a1-4d3e-94b0-696288a1140f`
5. Make any necessary configuration changes.
6. Click **Save**.

Configuring ConnectWise for FortiSIEM Integration

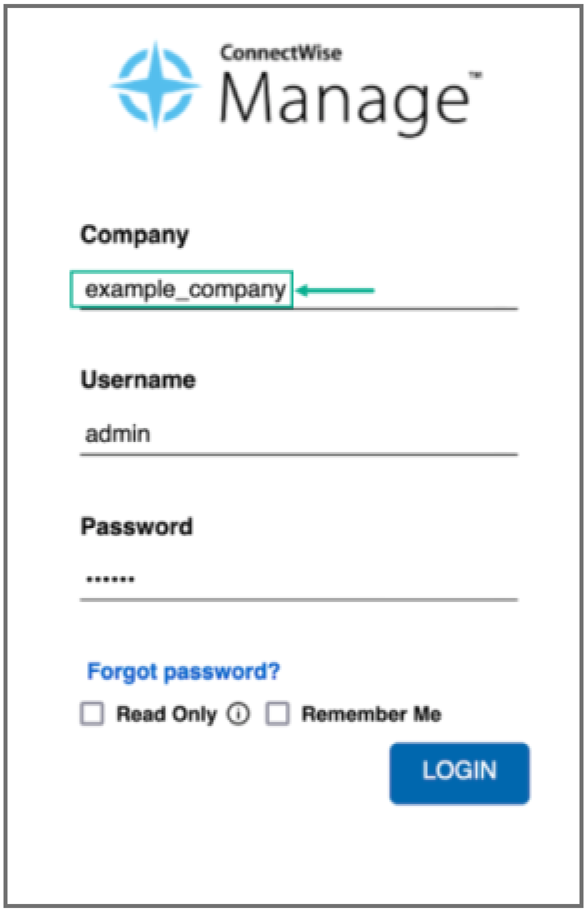
1. Log in to ConnectWise MANAGE.
2. Go to **Setup Tables > Integrator Login** List.
3. Create a new **Integrator Login** for FortiSIEM:
   a. Enter **Username**.
   b. Enter **Password**.
   c. Set **Access Level** to **Records created by integrator**.
   d. Enable **Service Ticket API** for Incident Integration.
   e. Enable **Configure API** for CMDB Integration.
4. For Service Provider Configurations, create Companies by creating:
   a. **Company Name**
   b. **Company ID**

ConnectWise Incident Outbound Integration

Step 1: Create an Integration

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Incident**.
5. For **Direction**, select **Outbound**.
6. For **Vendor**, select the vendor of the system you want to connect to. ConnectWise is supported out of the box. When you select the Vendor:
   a. An **Instance** is created - this is the unique name for this policy. For example if you had two ConnectWise installations, each would have different Instance names.
   b. Choose whether the **Plugin Type** is **SOAP** or **REST**.
   Note: The SOAP method is deprecated, so you should select REST.
   c. A default **Plugin Name** is populated - this is the Java code that implements the integration including connecting to the external help desk systems and synching the CMDB elements. The plugin is automatically populated for ConnectWise. For other vendors, you must create your own plugin and enter the plugin name here.
7. For **Host/URL**, enter the host name or URL of the external system. For ConnectWise, enter the login URL of the ConnectWise instance. Make sure to include the https:// prefix.
   Example: `https://my.login.test`

8. For **Company**, enter the company name that you use when logging in to ConnectWise Manage. Do not use the company name from within ConnectWise.



Company

example_company

Username

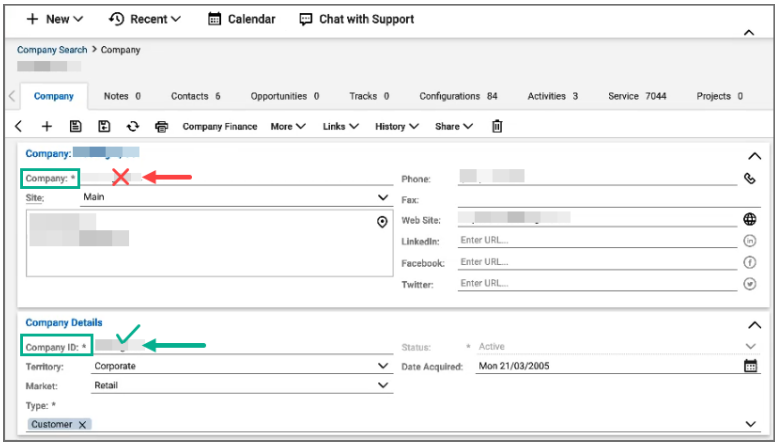
admin

Password

••••••

9. If you chose **SOAP** as **Plugin Type**, enter a **User Name**, **Password**, and **Client ID** that the system can use to authenticate with the external system. For ConnectWise, select the credentials created in Configuring ConnectWise for FortiSIEM Integration, Step 3. If you chose REST, enter the **Public Key** and the **Private Key** and **Client ID**.
   Note: The Client ID is 1a7ed749-47a1-4d3e-94b0-696288a1140f. See Adding a Client ID for ConnectWise Integration for more information.
   To get your **Public Key** and **Private Key** from ConnectWise, login and take the following steps.
   a. In the upper right part of the window, click your account name to open a drop-down list, and select **My Account**.
   b. Click the **API Keys** tab, and create your private and public keys, keeping a record of what they are so you can enter them in the FortiSIEM configuration in the **Private Key** and **Public Key** fields.
10. For **Incidents Comments Template**, specify the formatting using the incident fields.
11. For **Organization Mapping**, click **Edit** to create mappings between the organizations in your FortiSIEM deployment and the names of the organization in the external system. In ConnectWise, locate and use the **Company ID** field under Company Details in ConnectWise for the FortiSIEM Organization Mapping, NOT the

company name.



Company: [redacted]

Company: * [redacted]

Site: Main

Phone: [redacted]

Fax:

Web Site: [redacted]

LinkedIn: Enter URL...

Facebook: Enter URL...

Twitter: Enter URL...

Company ID: * [redacted]

Status: * Active

Territory: Corporate

Date Acquired: Mon 21/03/2005

Market: Retail

Type: * Customer

12. For **Run For**, choose the organizations for whom tickets will be created.
13. Enter the **Max Incidents** to be recorded.
    Note: The default number for **Max Incidents** is 50. When running this the first time with the default number, you may encounter a 502 proxy error due to the initial volume of incidents being requested. In this situation, you can change the **Max Incidents** value to 5 or 10 initially, then change it after running the ConnectWise integration once.
14. Click **Save**.

Step 2: Link Integration to a Notification Policy

You need to link the integration to a notification policy, so that the integration runs when the notification policy triggers.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Notification Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Notification Settings** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

ConnectWise Incident Inbound Integration

This updates the FortiSIEM incident state and clears the incident when the incident is cleared in the external help desk system. Built-in integrations are available for ConnectWise.

The steps are:

1. Create an Incident Inbound integration schedule.
2. Create a schedule for automatically running the Incident Inbound integration.
   This will update the FortiSIEM incident inbound integration schedule and clears the incident when the incident is cleared in the external help desk system.

Step 1: Create an Incident Inbound integration

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Incident**.
5. For **Direction**, select **Inbound**.
6. For **Vendor**, select the vendor of the system you want to connect to. ConnectWise is supported out of the box. When you select the Vendor:
   1. An **Instance** is created - this is the unique name for this policy. For example if you had two ConnectWise installations, each would have different Instance names.
   2. Choose whether the **Plugin Type** is **SOAP** or **REST**.
   3. A default **Plugin Name** is populated. This is the Java code that implements the integration including connecting to the external help desk systems and synching the CMDB elements. The plugin is automatically populated for ConnectWise. For other vendors, you must create your own plugin and enter the plugin name here.
7. For **Host/URL**, enter the host name or URL of the external system (see section Configuring external helpdesk systems). For ConnectWise, select the login URL.
8. If you chose **SOAP** as **Plugin Type**, enter a **User Name**, **Password**, and **Client ID** that the system can use to authenticate with the external system. For ConnectWise, select the credentials created in Configuring ConnectWise for FortiSIEM Integration, Step 3. If you chose REST, enter the **Public Key**, the **Private Key**, and **Client ID**.
9. For **Time Window**, select the number of hours for which incident states will be synched. For example, if time windows is set to 10 hours, the states of incidents that occurred in the last 10 hours will be synched.
10. Click **Save**.

Step 2: Create an Incident Inbound integration schedule

This will update FortiSIEM following incident fields when ticket state is updated in the external ticketing system.

- External Ticket State
- Ticket State
- External Cleared Time
- External Resolve Time

Note: FortiSIEM does not support custom mapping, only "new" and "closed", and the incident resolution is not updated.

Follow these steps.

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **Schedule** and then click **+**.
   1. Select the integration policy.
   2. Select a schedule.

ConnectWise CMDB Outbound Integration

CMDB Outbound Integration populates an external CMDB from FortiSIEM's own CMDB. Built in integrations are available for ServiceNow, ConnectWise and Salesforce.

Step 1: Create a CMDB Outbound integration

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Device**.
5. For **Direction**, select **Outbound**.
6. For **Vendor**, select the vendor of the system you want to connect to. ConnectWise is supported out of the box. When you select the Vendor:
    a. An **Instance** is created - this is the unique name for this policy. For example if you had two ConnectWise installations, each would have different Instance names.
    b. Choose whether the **Plugin Type** is **SOAP** or **REST**.
    c. A default **Plugin Name** is populated - this is the Java code that implements the integration including connecting to the external help desk systems and synching the CMDB elements. The plugin is automatically populated for ConnectWise. For other vendors, you have to create your own plugin and type in the plugin name here.
7. For **Host/URL**, enter the host name or URL of the external system. For ConnectWise, select the login URL.
8. If you chose **SOAP** as **Plugin Type**, enter a **User Name**, **Password**, and **Client ID** that the system can use to authenticate with the external system. For ConnectWise, select the credentials created in Configuring ConnectWise for FortiSIEM Integration, Step 3. If you chose REST, enter the **Public Key** and the **Private Key** in addition to the **User Name**, **Password**, and **Client ID**.
9. For **Organization Mapping**, click **Edit** to create mappings between the organizations in your FortiSIEM deployment and the names of the organization in the external system. For ConnectWise, select the Company name in Configuring ConnectWise for FortiSIEM Integration, Step 4.
10. For **Run For**, choose the organizations for whom tickets will be created.
11. For ConnectWise, it is possible to define a **Content Mapping**.
    a. Enter **Column Mapping** values:
        i. To add a new mapping, click the + button.
        ii. Choose FortiSIEM CMDB attribute as the Source Column.
        iii. Enter external (ConnectWise) attribute as the Destination Column.
        iv. Specify Default Mapped Value as the value assigned to the Destination Column if the Source Column is not found in Data Mapping definitions.
        v. Select Put to a Question is the Destination Column is a custom column in ConnectWise.
    b. Enter **Data Mapping** values:
        i. Choose the (Destination) Column Name.
        ii. Enter From as the value in FortiSIEM.
        iii. Enter To as the value in ConnectWise.
12. For **Groups**, select the FortiSIEM CMDB Groups whose member devices would be synched to external CMDB.
13. Select **Run after Discovery** if you want this export to take place after you have run discovery in your system. This is the only way to push automatic changes from FortiSIEM to the external system.
14. Enter the **Max Devices**: the number of devices to send to the external system.
15. Click **Save**.

Step 2: Create a CMDB Outbound integration schedule

Updating external CMDB automatically after FortiSIEM discovery:

1. Create an integration policy.
2. Make sure Run after Discovery is checked.
3. Click **Save**.

Updating external CMDB on a schedule:

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **Schedule** and then click **+**.
   1. Select the integration policies.
   2. Select a schedule.

Updating external CMDB on-demand (one-time):

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Select a specific integration policy and click **Run**.

Salesforce Integration

- Configuring Salesforce for FortiSIEM Integration
- Salesforce Incident Outbound Integration
- Salesforce Incident Inbound Integration
- Salesforce CMDB Outbound Integration

Configuring Salesforce for FortiSIEM Integration

1. Log in to Salesforce.
2. Create a **custom domain**.
3. For Service Provider Configurations, create **Service App** > **Accounts**.
   FortiSIEM will use the **Account Name**.

Salesforce Incident Outbound Integration

Step 1: Create an Integration

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Incident**.
5. For **Direction**, select **Outbound**.
6. For **Vendor**, select the vendor of the system you want to connect to. Salesforce is supported out of the box.
   When you select the Vendor:
   1. An **Instance** is created - this is the unique name for this policy. For example if you had two Salesforce installations, each would have different Instance names.

    b. A default **Plugin Name** is populated - this is the Java code that implements the integration including connecting to the external help desk systems and synching the CMDB elements. The plugin is automatically populated for Salesforce. For other vendors, you must create your own plugin and enter the plugin name here.

7. For **Host/URL**, enter the host name or URL of the external system. For Salesforce:
    a. Log in to Salesforce.
    b. Go to **Setup** > **Settings**.
    c. Use the **Custom URL** under **My Domain**, typically it is `xyz.my.salesforce.com`
8. For **User Name** and **Password**, enter a user name and password that the system can use to authenticate with the external system.
    a. For Salesforce, enter the login credentials.
9. For **Security Token**, enter the security token from Salesforce. If you do not have your security token information, you can get this by taking the following steps.
    a. Log in to Salesforce.
    b. At <*your name*>, click the drop-down list and navigate to **Setup > Personal Setup > My Personal Information**.
    c. Click **Reset My Security Token** to get Salesforce to email your security token.
10. For **Incidents Comments Template**, specify the formatting of the incident fields.
11. For **Organization Mapping**, click the **Edit** icon to take you to the **Integration Policy > Org Mapping** window. Here, you can create mappings between the organizations in your FortiSIEM deployment and the names of the organization in the external system. For Salesforce, to get your account name, take the following steps in Salesforce:
    a. Go to **Service App** > **Accounts**.
    b. Use **Account Name**.
    c. In FortiSIEM, at the **Integration Policy > Org Mapping** window, enter the **Account Name** in the **Default** field.
    Note: You can choose to provide an organization name from FortiSIEM in the **Default** field.
12. For **Run For**, choose the organizations for whom tickets will be created.
13. In the **Max Incidents** field, enter the maximum number of incidents you want recorded.
14. Click **Save**.
15. Click **Run** to confirm the integration. If you receive an "...unable to find valid certification path to requested target", you need to upload a certificate to FortiSIEM.

Step 2: Link Integration to a Notification Policy

You need to link the integration to a notification policy, so that the integration runs when the notification policy triggers.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Notification Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Notification Settings** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

Salesforce Incident Inbound Integration

This updates the FortiSIEM incident state and clears the incident when the incident is cleared in the external help desk system. Built-in integrations are available for Salesforce.

The steps are:

1. Create an Incident Inbound integration schedule.
2. Create a schedule for automatically running the Incident Inbound integration.

   This will update the FortiSIEM incident inbound integration schedule and clears the incident when the incident is cleared in the external help desk system.

Step 1: Create an Incident Inbound integration

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Incident**.
5. For **Direction**, select **Inbound**.
6. For **Vendor**, select the vendor of the system you want to connect to. Salesforce is supported out of the box. When you select the Vendor:
   1. An **Instance** is created - this is the unique name for this policy. For example if you had two Salesforce installations, each would have different Instance names.
   2. A default **Plugin Name** is populated. This is the Java code that implements the integration including connecting to the external help desk systems and synching the CMDB elements. The plugin is automatically populated for Salesforce. For other vendors, you must create your own plugin and enter the plugin name here.
7. For **Host/URL**, enter the host name or URL of the external system. For Salesforce:
   1. Log in to Salesforce.
   2. Go to **Setup > Settings**.
   3. Use the **custom URL** under **My Domain** – typically it is `xyz.my.salesforce.com`.
8. For **User Name** and **Password**, enter a user name and password that the system can use to authenticate with the external system. For Salesforce, select the login credentials.
9. For **Time Window**, select the number of hours for which incident states will be synched. For example, if time windows is set to 10 hours, the states of incidents that occurred in the last 10 hours will be synched.
10. Click **Save**.

Step 2: Create an Incident Inbound integration schedule

This will update FortiSIEM following incident fields when ticket state is updated in the external ticketing system.

- External Ticket State
- Ticket State
- External Cleared Time
- External Resolve Time

Follow these steps.

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **Schedule** and then click **+**.
   a. Select the integration policy.
   b. Select a schedule.

Salesforce CMDB Outbound Integration

CMDB Outbound Integration populates an external CMDB from FortiSIEM’s own CMDB. Built in integrations are available for Salesforce.

Step 1: Create a CMDB Outbound integration

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Device**.
5. For **Direction**, select **Outbound**.
6. For **Vendor**, select the vendor of the system you want to connect to. Salesforce is supported out of the box. When you select the Vendor:
   a. An **Instance** is created - this is the unique name for this policy. For example if you had 2 Salesforce installations, each would have different Instance names.
   b. A default **Plugin Name** is populated - this is the Java code that implements the integration including connecting to the external help desk systems and synching the CMDB elements. The plugin is automatically populated for Salesforce . For other vendors, you have to create your own plugin and type in the plugin name here.
7. For **Host/URL**, enter the host name or URL of the external system. For Salesforce:
   a. Log in to Salesforce.
   b. Go to **Setup** > **Settings**.
   c. Use the **Custom URL** under **My Domain**, typically it is `xyz.my.salesforce.com`.
8. For **User Name** and **Password**, enter a user name and password that the system can use to authenticate with the external system. For Salesforce, select the login credentials.
9. Enter the **Maximum** number of devices to send to the external system.
10. For **Organization Mapping**, click **Edit** to create mappings between the organizations in your FortiSIEM deployment and the names of the organization in the external system. For Salesforce:
    a. Go to **Service App** > **Accounts**.
    b. Use **Account Name**.
11. For **Run For**, choose the organizations for whom tickets will be created.
12. For **Groups**, select the FortiSIEM CMDB Groups whose member devices would be synched to external CMDB.
13. Select **Run after Discovery** if you want this export to take place after you have run discovery in your system. This is the only way to push automatic changes from FortiSIEM to the external system.
14. Click **Save**.

Step 2: Create a CMDB Outbound integration schedule

Updating external CMDB automatically after FortiSIEM discovery:

1. Create an integration policy.
2. Make sure Run after Discovery is checked.
3. Click **Save**.

Updating external CMDB on a schedule:

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **Schedule** and then click **+**.
   a. Select the integration policies.
   b. Select a schedule.

Updating external CMDB on-demand (one-time):

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Select a specific integration policy and click **Run**.

CMDB Inbound Integration

CMDB Inbound Integration populates FortiSIEM CMDB from an external CMDB.

Step 1: Create a CMDB Inbound integration

You must create a CSV file for mapping the contents of the external database to a location on your FortiSIEM Supervisor, which will be periodically updated based on the schedule you set.

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Device**.
5. For **Direction**, select **Inbound**.
6. Enter the **File Path** to the CSV file.
7. For **Content Mapping**, click the edit icon.
   a. For **Column Mapping**, click **+** and enter the mapping between columns in the **Source** CSV file and the **Destination** CMDB.
      I. Enter Source CSV column Name for **Source Column**
      II. Check **Create Property if it Does not Exist** to create the new attribute in FortiSIEM if it does not exist
         i. Enter a name for the **Destination Column** of the property from the drop-down list.
         ii. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite it's current value.
      III. If the property exists in the CMDB, select FortiSIEM CMDB attribute for **Destination Column**.
      IV. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite its current value.
      V. Click **OK**.
   b. For **Data Mapping**, click **+** and enter the mapping between data values in the external system and the destination CMDB.
      For example, if you wanted to change all instances of **California** in the entries for the **State** attribute in

the external system to **CA** in the destination CMDB, you would select the **State** attribute, enter **California** for **From**. and **CA** for **To**.

8. In **Attribute Mapping**, map attributes to resources.
9. Click **OK**.
10. Click **Save**.

Step 2: Create a CMDB Inbound integration schedule

Updating FortiSIEM CMDB on a schedule:

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **Schedule** and then click **+**.
   a. Select the integration policies.
   b. Select a schedule.

Updating FortiSIEM CMDB on-demand (one-time):

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Select a specific integration policy and click **Run**.

Configuring Reputation System Integrations

- VirusTotal Integration
- FortiGuard IOC Lookup Integration
- RiskIQ Integration

VirusTotal Integration

- Configuring VirusTotal for FortiSIEM Integration
- VirusTotal Incident Outbound Integration

Configuring VirusTotal for FortiSIEM Integration

Register at the VirusTotal website to obtain a user name, password, and the API key. For more information, see https://developers.virustotal.com/reference/overview#getting-started.

VirusTotal Incident Outbound Integration

Step 1: Create an Integration

To create an outbound integration, follow these steps.

1. Go to **Admin > Settings > General > External Integration**.
2. Click **New** to create a new integration or **Edit** to modify an existing integration.

3. In the **Integration Policy** dialog box, provide the following values:
   - **Type**: select **Incident**.
   - **Direction**: select **Outbound**.
   - **Vendor**: select **VirusTotal**.
   - **Instance**: enter an instance name or accept the default.
   - **Plugin Name**: is pre-populated with the name of the integration class: `com.acceloops.service.integration.impl.VirusTotalIntegrationServiceImpl`.
   - **Password**: enter your API key in the password field.
4. Enter an optional **Description** of the integration.
5. Click the edit icon next to the **Incident Comments template**.
   a. In the **Incident Comments Template** dialog box, select content from the **Insert Content** drop-down list.
   b. Click **Save** when you are finished.
6. Click the edit icon next to the **Organization Mapping**.
   a. In the **Org Mapping** dialog box, click beneath **External Company ID** to enter the ID of the company you want to map to organizations.
   b. Click **Save** when you are finished.
7. Click the edit icon next to the **Run for**.
   a. In the **Run for** dialog box, select the organizations for which the integrations will be run.
   b. Click **Save** when you are finished.
8. Enter the maximum number of incidents you want recorded in the **Max Incidents** field.
9. Click **Save**.

Step 2: Link Integration to a Notification Policy

You need to link the integration to a notification policy, so that the integration runs when the notification policy triggers.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Notification Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Notification Settings** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

FortiGuard IOC Lookup Integration

- Configuring FortiGuard for FortiSIEM Integration
- FortiGuard Incident Outbound Integration

Configuring FortiGuard for FortiSIEM Integration

No additional license is required to use the FortiGuard feature. Follow the steps in FortiGuard Incident Outbound Integration and Adding Incident Notification Settings to configure this feature.

FortiGuard Incident Outbound Integration

To create an outbound integration, follow these steps.

Step 1: Create an Integration

1. Go to **ADMIN > Settings > General > External Integration**.
2. Click **New** to create a new integration or **Edit** to modify an existing integration.
3. In the **Integration Policy** dialog box, provide the following values:
   - **Type**: select **Incident**.
   - **Direction**: select **Outbound**.
   - **Vendor**: select **FortiGuard IOC Lookup**.
   - **Instance**: enter an instance name or accept the default.
   - **Plugin Name**: is pre-populated with the name of the integration class: `com.accelops.service.integration.impl.FortiGuardIOCIntegrationServiceImpl`.
4. Enter an optional **Description** of the integration.
5. In the **Max Incidents** field, enter the maximum number of incidents you want recorded.
6. Click **Save**.

Step 2: Link Integration to a Notification Policy

You need to link the integration to a notification policy, so that the integration runs when the notification policy triggers.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Notification Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Notification Settings** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

RiskIQ Integration

- Configuring RiskIQ for FortiSIEM Integration
- RiskIQ Incident Outbound Integration

Configuring RiskIQ for FortiSIEM Integration

Register at the RiskIQ website to obtain a user name, password, and the API keys. For more information, see https://api.riskiq.net/api/concepts.html.

RiskIQ Incident Outbound Integration

Step 1: Create an Integration

To create an outbound integration, follow these steps.

1. Go to **Admin > Settings > General > External Integration**.
2. Click **New** to create a new integration or **Edit** to modify an existing integration.
3. In the **Integration Policy** dialog box, provide the following values:
   - **Type**: select **Incident**.
   - **Direction**: select **Outbound**.

- **Vendor**: select **RiskIQ**.
- **Instance**: enter an instance name or accept the default.
- **Plugin Name**: is pre-populated with the name of the integration class: `com.accelops.phoenix.jira.JiraTicketIntegration`.
- **Username** and **Password**, enter your RiskIQ user name and the API key as the password.

4. Enter an optional **Description** of the integration.
5. Click the edit icon next to **Attribute Mapping**.
   a. In the **Incident Comments Template** dialog box, select content from the **Insert Content** drop-down list.
   b. Click **Save** when you are finished.
6. Click the edit icon next to the **Organization Mapping** to map attributes to resources.
7. Click the edit icon next to the **Run for**.
   a. In the **Run for** dialog box, select the organizations for which the integrations will be run.
   b. Click **Save** when you are finished.
8. Enter the maximum number of incidents you want recorded in the **Max Incidents** field.
9. Click **Save**.

Step 2: Link Integration to a Notification Policy

You need to link the integration to a notification policy, so that the integration runs when the notification policy triggers.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Notification Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Notification Settings** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

Configuring Communication through Proxies

If you want the communication between the FortiSIEM Supervisor and the external system to go through a proxy, then complete the following steps

1. Login to Supervisor as `admin`.
2. Go to the glassfish configuration directory: `/opt/glassfish/domains/domain1/config`.
3. Add proxy server information to the `domain.xml` file:

```
<jvm-options>-Dhttp.proxyHost=172.30.57.100</jvm-options>
<jvm-options>-Dhttp.proxyPort=3128</jvm-options>
<jvm-options>-Dhttp.proxyUser=foo</jvm-options>
<jvm-options>-Dhttp.proxyPassword=password</jvm-options>
```

4. Restart glassfish.

Modifying an External System Integration

Complete these steps to modify an External System Integration.

1. Use the below options to modify an External System Integration setting.

Settings	Guidelines
Edit	To edit an External System Integration setting.
Delete	To delete an External System Integration setting.

2. Click **Save**.

ServiceNow Security Operations (SecOps) Integration

- Scope and Purpose
- XML Assets
- Process Overview
- Process Workflow
- ServiceNow FortiSIEM Integration Usage
- ServiceNow FortiSIEM Integration Deletion
- ServiceNow and FortiSIEM Field Mappings
- Known Limitations

Scope and Purpose

ServiceNow FortiSIEM integration is designed to pull FortiSIEM incidents and triggering events from the remote FortiSIEM server every 30 seconds into the desired ServiceNow instance. FortiSIEM incidents pulled into the ServiceNow instance will be automatically mapped to new security incidents. Upon closing the created security incidents, the corresponding FortiSIEM incidents status on the remote FortiSIEM sever will also be updated.

XML Assets

The required XML files for this integration can be downloaded here.

File: FortiSIEM-ServiceNow-Integration-v1_3_6.zip

SHA256 hash: 945214c2128337dc7d8b03f80ebd51e1a07a8c75c855c3ec49583ca61d43e1f5

MD5 hash: d397ad5bf6ba0c0e15942958b95bad4e

Process Overview

1. The ServiceNow system administrator must request a new Paris release ServiceNow instance or login to an existing one to import the provided ServiceNow FortiSIEM integration XML file to ServiceNow.
2. The ServiceNow system administrator configures the REST Message API endpoints and Basic Auth Profile settings on the ServiceNow instance to make API calls to the remote FortiSIEM server.
3. The ServiceNow instance will begin to fetch FortiSIEM incidents and triggering events every 30 seconds.
4. The ServiceNow system administrator or ServiceNow users with security incident roles can view and update security incidents created from FortiSIEM incidents pulled.

Process and Workflow

The following information contains a detailed explanation on how ServiceNow FortiSIEM integration is set up and its usage.

ServiceNow FortiSIEM Integration Prerequisites

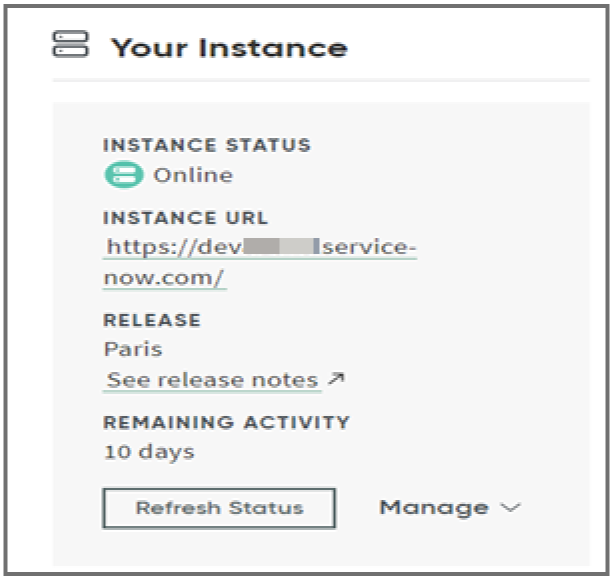
The following is required for ServiceNow FortiSIEM integration.

1. FortiSIEM server.
2. Paris release ServiceNow instance.
3. ServiceNow instance plugin – Security Incident Response Dependencies.
4. ServiceNow instance plugin – Security Incident Response.

ServiceNow FortiSIEM Integration Installation

A ServiceNow system administrator must take the following steps:

1. Request a new Paris release ServiceNow instance or login to an existing one.



Your Instance

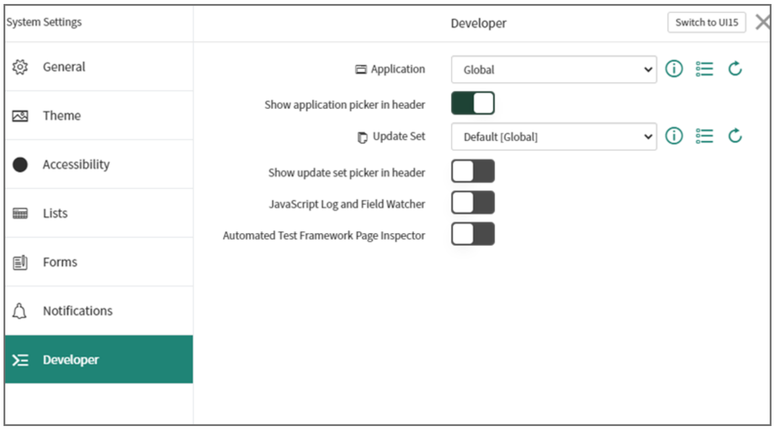
INSTANCE STATUS
Online

INSTANCE URL
https://dev[redacted]service-now.com/

RELEASE
Paris
See release notes ↗

REMAINING ACTIVITY
10 days

2. In the ServiceNow instance, click the **Application** drop-down list and select **Global**.



Application: Global

Show application picker in header

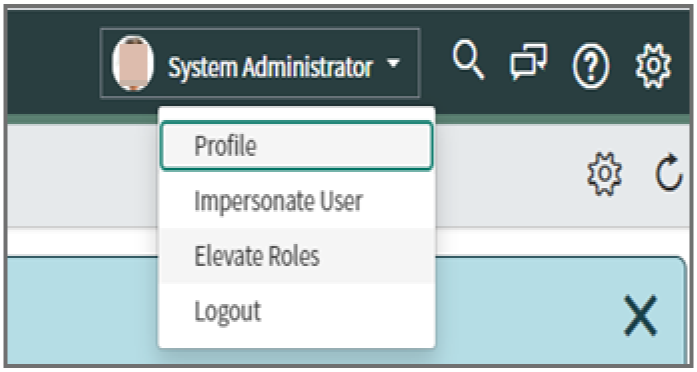
Update Set: Default [Global]

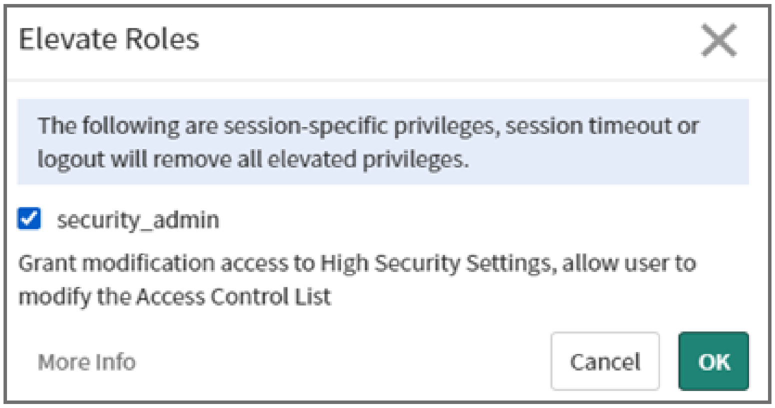
Show update set picker in header

JavaScript Log and Field Watcher

Automated Test Framework Page Inspector

3. Click on the role drop down list and select **Elevate Roles**. Elevate the "System Administrator" role to "Security Admin". This new role ensures the success of the ServiceNow FortiSIEM integration import in the next step.



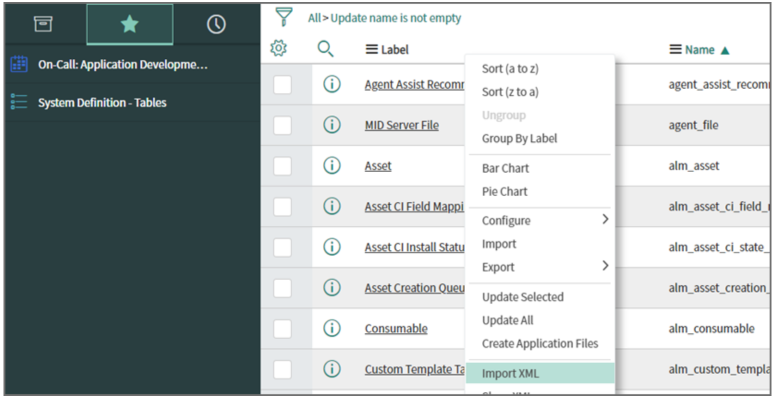


The following are session-specific privileges, session timeout or logout will remove all elevated privileges.

☑ security_admin

Grant modification access to High Security Settings, allow user to modify the Access Control List

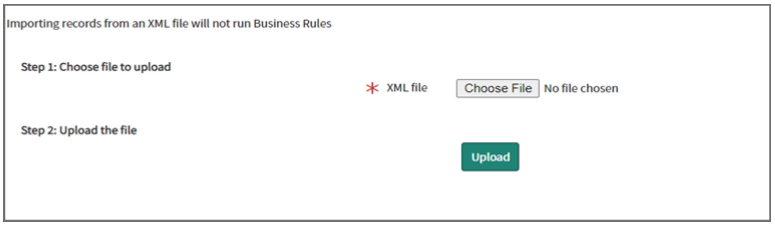
4. Navigate to **System Definition - Tables**, right click on **Table Headers** on the page, and select **Import XML**.



All > Update name is not empty

Label	Name ▲
Agent Assist Recomr	agent_assist_recomi
MID Server File	agent_file
Asset	alm_asset
Asset CI Field Mappi	alm_asset_ci_field_
Asset CI Install Statu	alm_asset_ci_state_
Asset Creation Queu	alm_asset_creation_
Consumable	alm_consumable
Custom Template Ta	alm_custom_templa

In "Import XML", select the provided `FSMSNIntegrationImportData` file (See XML Assets) and click **Upload**.



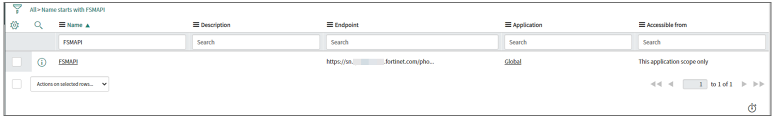
Importing records from an XML file will not run Business Rules

Step 1: Choose file to upload

* XML file Choose File No file chosen

Step 2: Upload the file

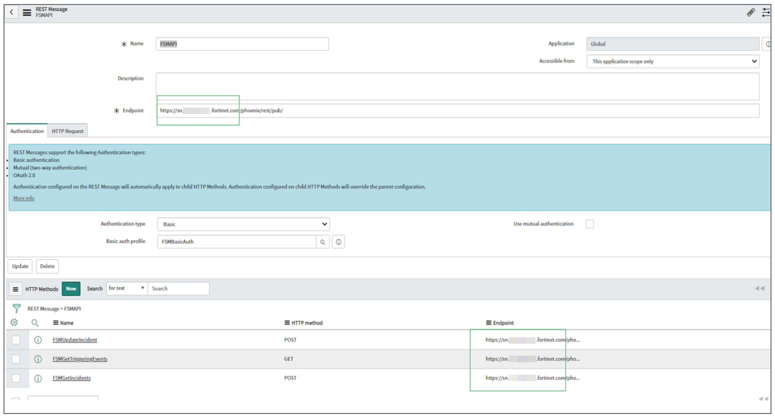
5. After the upload is complete, navigate to **System Web Services/Rest Message**, and click on **FSMAPI** (This was imported in step 5) to change the FortiSIEM remote server API endpoint and basic auth profile.



All > Name starts with FSMAPI

Name ▲	Description	Endpoint	Application	Accessible from
FSMAPI	Search	Search	Search	Search
FSMAPI		https://sn.[redacted].fortinet.com/pho...	Global	This application scope only

6. In **REST Message/FSMAPI**, if the remote FortiSIEM server host name is different than the ones displayed, please manually change the hostname in “FSMAPI” and all the endpoints in **HTTP Methods**, as shown here. For **HTTP Methods**, please manually click on each record, and change the hostname.
Note: Only change the host name.(I.E. `https://myNewHostName.com`). The slashes or symbols after the host name must be retained.



REST Message
FSMAPI

* Name: FSMAPI
Application: Global
Accessible from: This application scope only
Description:
* Endpoint: https://sn.[redacted].fortinet.com/phoenix/rest/pub/

REST Messages support the following Authentication types:
- Basic authentication
- Mutual (two-way authentication)
- OAuth 2.0

Authentication configured on the REST Message will automatically apply to child HTTP Methods. Authentication configured on child HTTP Methods will override the parent configuration.

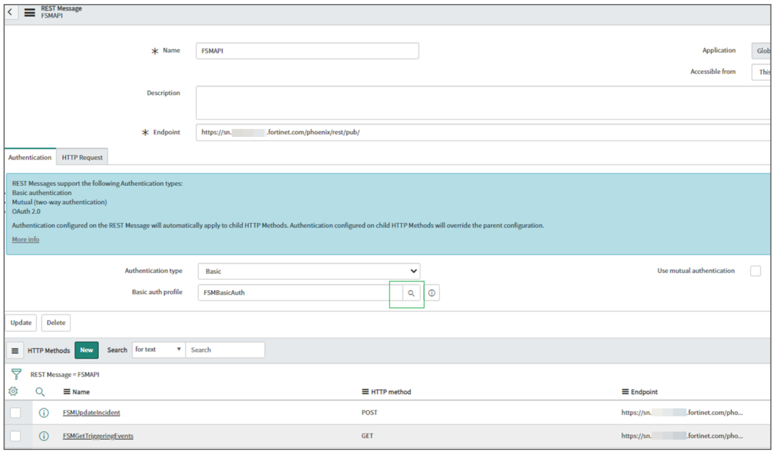
More info

Authentication type: Basic
Use mutual authentication: □
Basic auth profile: FSMBasicAuth

REST Message = FSMAPI

Name	HTTP method	Endpoint
FSMUpdateIncident	POST	https://sn.[redacted].fortinet.com/pho...
FSMGetTriggeringEvents	GET	https://sn.[redacted].fortinet.com/pho...
FSMGetIncidents	POST	https://sn.[redacted].fortinet.com/pho...

7. In “REST Message/FSM API”, to change the basic auth profile, first click the search icon.



REST Message
FSMAPI

* Name: FSMAPI

Application: Glob

Accessible from: This

Description:

* Endpoint: https://sn.[redacted].fortinet.com/phoenix/rest/pub/

Authentication | HTTP Request

REST Messages support the following Authentication types:
Basic authentication
Mutual (two-way authentication)
OAuth 2.0

Authentication configured on the REST Message will automatically apply to child HTTP Methods. Authentication configured on child HTTP Methods will override the parent configuration.

More info

Authentication type: Basic

Use mutual authentication: □

Basic auth profile: FSMBasicAuth

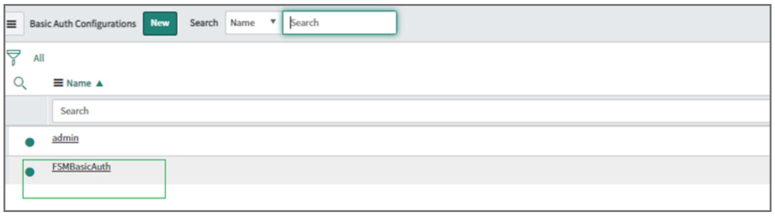
Update | Delete

HTTP Methods | New | Search: for text | Search

REST Message = FSMAPI

Name	HTTP method	Endpoint
FSMUpdateIncident	POST	https://sn.[redacted].fortinet.com/pho...
FSMGetTriggeringEvents	GET	https://sn.[redacted].fortinet.com/pho...

8. Click **FSMBasicAuth**, and change the user name and password accordingly. You may also create a new Basic auth profile.



Basic Auth Configurations | New | Search: Name | Search

All

Name ▲
admin
FSMBasicAuth

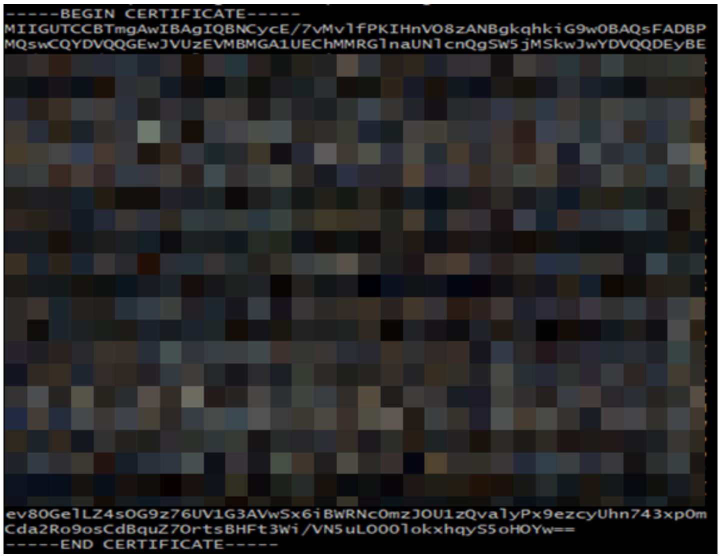
9. The integration uses a “HTTPS outbound REST end point”, and requires the FortiSIEM certificate to be added to the ServiceNow Certificate Trust Store. Please follow the sub-steps here before proceeding to step 11.
   a. Retrieve destination server SSL certificates. This can be given by the network administrator of the destination server, or by using the Linux command:

   ```
   openssl s_client -connect <destination_server_name>:443 –showcerts
   ```

   To gather the specific certificate, run this command from a Linux server:

   ```
   echo | openssl s_client -connect <destination_server_name>:443 2>&1 | sed
   --quiet '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > <destination_
   server_name>.pem
   ```

   A sample SSL certificate is shown here.

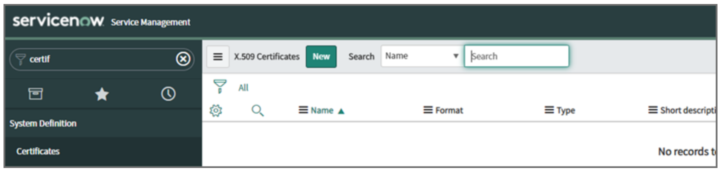


```
-----BEGIN CERTIFICATE-----
MIIGUTCCBTmgAwIBAgIQBNCycE/7vMvlfPKIHnVO8zANBgkqhkiG9w0BAQsFADBP
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMSkwJwYDVQQDEyBE
[redacted]
ev80GelLZ4sOG9z76UV1G3AVwSx6iBWRNcOmzJOU1zQvalyPx9ezcyUhn743xpOm
Cda2Ro9osCdBquZ7OrtsBHFt3Wi/VN5uLOO0lokxhqyS5oHOYw==
-----END CERTIFICATE-----
```

b. Validate retrieved SSL certificate in part a to see if it has any issues or errors. It can be done through https://www.digicert.com/help/ or through the Linux command:
`openssl s_client -connect <destination_server_name>:443 -showcerts`

If the certificate has issues or errors, please contact the destination server administrator for a correct one. For any reason that a correct SSL certificate cannot be obtained, please refer to step 10g for a temporary workaround in a ServiceNow instance. **Note that this workaround is not recommended for ServiceNow production instances**.

c. Now, upload the retrieved SSL certificate in part a to the ServiceNow instance. Navigate to **System Definition/Certificates** and on the right panel, click **New**.



d. On the new dialog box, take the following steps:

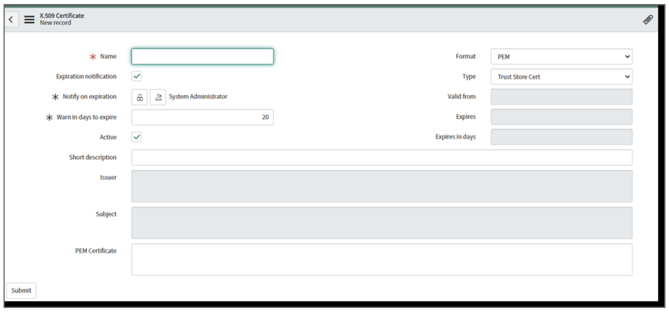
i. In the **Name** field, enter a name for the certificate.

ii. From the **Format** drop-down list, select **PEM**.

iii. From the **Type** drop-down list, select **Trust Store Cert**.

iv. In the **PEM Certificate** field, enter/paste the SSL certificate retrieved in 10a.

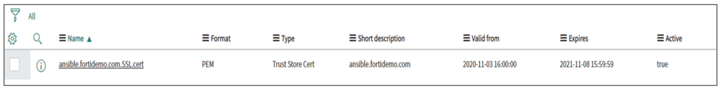
v. When done, click **Submit**.



X.509 Certificate
New record

* Name		Format	PEM
Expiration notification	☑	Type	Trust Store Cert
* Notify on expiration	System Administrator	Valid from	
* Warn in days to expire	20	Expires	
Active	☑	Expires in days	
Short description			
Issuer			
Subject			
PEM Certificate			

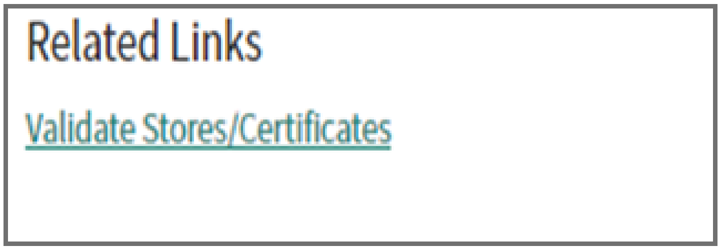
e. Once the certificate has been created, click on it.



All

		Name ▲	Format	Type	Short description	Valid from	Expires	Active
□	ⓘ	ansible.fortidemo.com.SSL.cert	PEM	Trust Store Cert	ansible.fortidemo.com	2020-11-03 16:00:00	2021-11-08 15:59:59	true

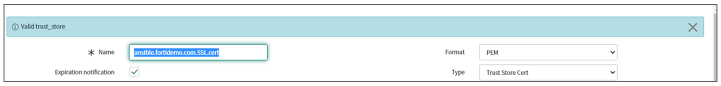
f. Click **Validate Stores/Certificates** to ensure it is valid.



Related Links

Validate Stores/Certificates

If it is valid, a “Valid trust_store” message will show. If you get an invalid certificate, please contact the destination server administrator.



ⓘ Valid trust_store

* Name: ansible.fortidemo.com.SSL.cert

Format: PEM

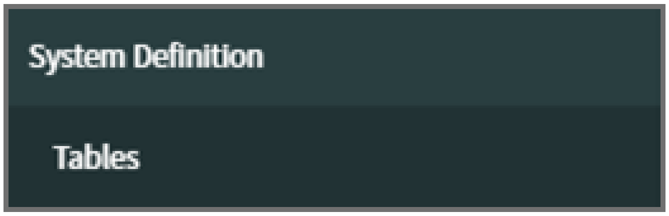
Expiration notification: ☑

Type: Trust Store Cert

g. **Note**: This is workaround step in ServiceNow instance to solve invalid certification issue encountered in step 10b.
This is only recommended for ServiceNow developer instances.

To proceed, take the following steps:

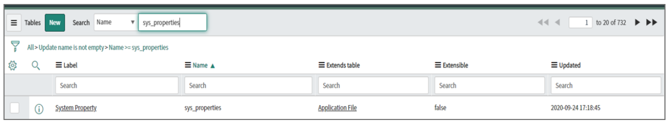
i. Navigate to **System Definition / Tables**.



System Definition

Tables

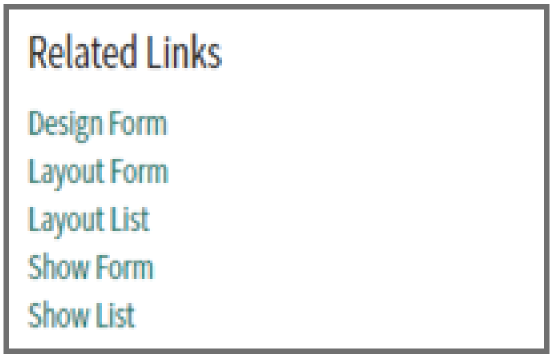
ii. Search for “sys_properties”, click on **System Property** from the displayed records and navigate to **Related Links**.



All > Update name is not empty > Name >= sys_properties

		Label	Name ▲	Extends table	Extensible	Updated
		Search	Search	Search	Search	Search
□	ⓘ	System Property	sys_properties	Application File	false	2020-09-24 17:18:45

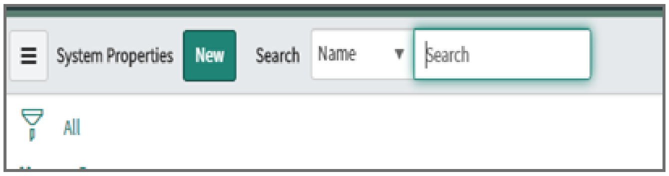
iii. Click **Show List** to open up all system properties entries stored in the current instance.



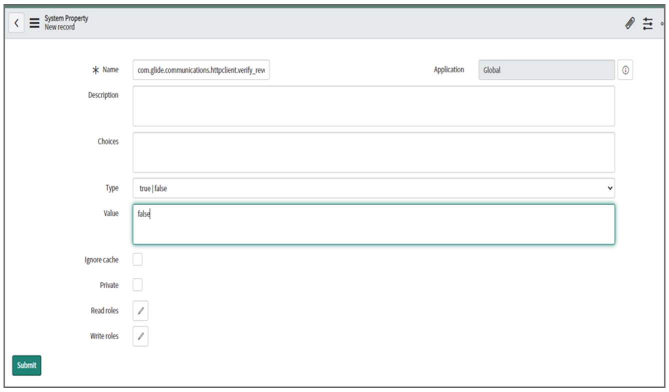
Related Links

Design Form
Layout Form
Layout List
Show Form
Show List

iv. Next to the System Properties header, click **New**.



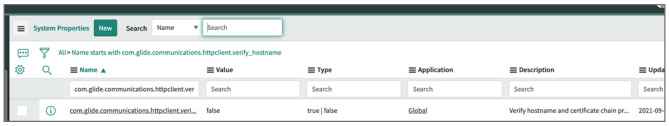
v. Enter the following:
In the **Name** field, enter "com.glide.communications.httpclient.verify_revoked_certificate".
In the **Type** field, enter "true|false".
In the **Value** field, enter "false".



* Name	com.glide.communications.httpclient.verify_rev
Application	Global
Description	
Choices	
Type	true | false
Value	false
Ignore cache	□
Private	□
Read roles	
Write roles	

vi. Click **Submit**.

vii. If the certificate in use by FortiSIEM is also Self Signed, then set the following System Property to false . Under the same section, search for *com.glide.communications.httpclient.verify_hostname* and change to false.



All > Name starts with com.glide.communications.httpclient.verify_hostname

Name ▲	Value	Type	Application	Description	Upda
com.glide.communications.httpclient.ver	Search	Search	Search	Search	Search
com.glide.communications.httpclient.veri...	false	true | false	Global	Verify hostname and certificate chain pr...	2021-09-

Once this record has been created, the ServiceNow instance will ignore any SSL certification validation issues or errors encountered.

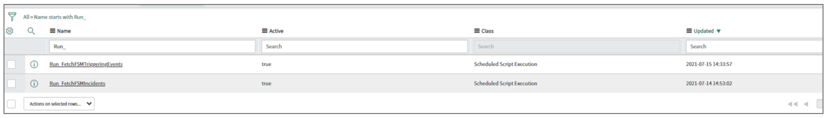
The installation is now complete.

ServiceNow FortiSIEM Integration Usage

The ServiceNow FortiSIEM Integration can be used in the following ways:

View Scheduled Jobs

The ServiceNow system administrator can view scheduled jobs that are running every 30 seconds to pull FSM incidents and FSM triggering events in “System Definitions/ Scheduled Jobs”.

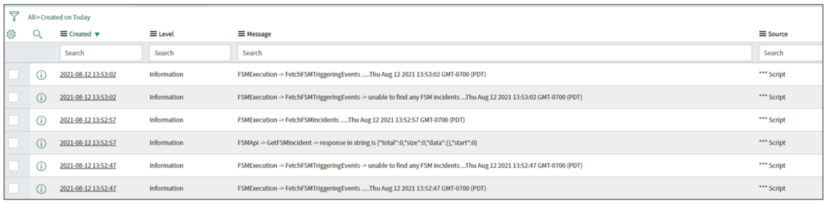


All > Name starts with Run_

Name	Active	Class	Updated ▼
Run_	Search	Search	Search
Run_FetchFSMTriggeringEvents	true	Scheduled Script Execution	2021-07-15 14:33:57
Run_FetchFSMIncidents	true	Scheduled Script Execution	2021-07-14 14:53:02

Monitor Scheduled Job Execution Logs

The ServiceNow system administrator can monitor the scheduled job execution logs in **System Log / All**.

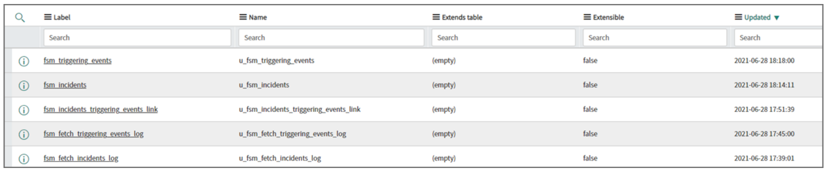


All > Created on Today

Created	Level	Message	Source
2021-08-12 13:53:02	Information	FSMExecution -> FetchFSMTriggeringEvents .....Thu Aug 12 2021 13:53:02 GMT-0700 (PDT)	*** Script
2021-08-12 13:53:02	Information	FSMExecution -> FetchFSMTriggeringEvents -> unable to find any FSM incidents ...Thu Aug 12 2021 13:53:02 GMT-0700 (PDT)	*** Script
2021-08-12 13:52:57	Information	FSMExecution -> FetchFSMIncidents .....Thu Aug 12 2021 13:52:57 GMT-0700 (PDT)	*** Script
2021-08-12 13:52:57	Information	FSMApi -> GetFSMIncident -> response in string is {"total":0,"size":0,"data":[],"start":0}	*** Script
2021-08-12 13:52:47	Information	FSMExecution -> FetchFSMTriggeringEvents -> unable to find any FSM incidents ...Thu Aug 12 2021 13:52:47 GMT-0700 (PDT)	*** Script
2021-08-12 13:52:47	Information	FSMExecution -> FetchFSMTriggeringEvents .....Thu Aug 12 2021 13:52:47 GMT-0700 (PDT)	*** Script

Examine FortiSIEM Incidents, Logs, and Triggering Events

Fetched FortiSIEM incidents will be stored in the “fsm_incidents” table, and logs will be stored in “fsm_fetch_incidents_log” table. Fetched FSM triggering events will be stored in “fsm_triggering_events” table, and logs will be stored in the “fsm_riggering_events_log” table. The link between incidents and events will be stored in the “fsm_incidents_triggering_events_link” table.

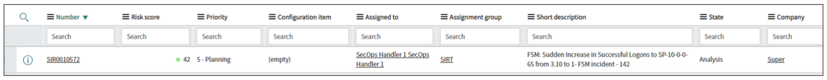


Label	Name	Extends table	Extensible	Updated
fsm_triggering_events	u_fsm_triggering_events	(empty)	false	2021-06-28 18:18:00
fsm_incidents	u_fsm_incidents	(empty)	false	2021-06-28 18:14:11
fsm_incidents_triggering_events_link	u_fsm_incidents_triggering_events_link	(empty)	false	2021-06-28 17:51:39
fsm_fetch_triggering_events_log	u_fsm_fetch_triggering_events_log	(empty)	false	2021-06-28 17:45:00
fsm_fetch_incidents_log	u_fsm_fetch_incidents_log	(empty)	false	2021-06-28 17:39:01

View Corresponding Security Incidents

After a FortiSIEM incident has been fetched, a corresponding security incident will be created with the short description:

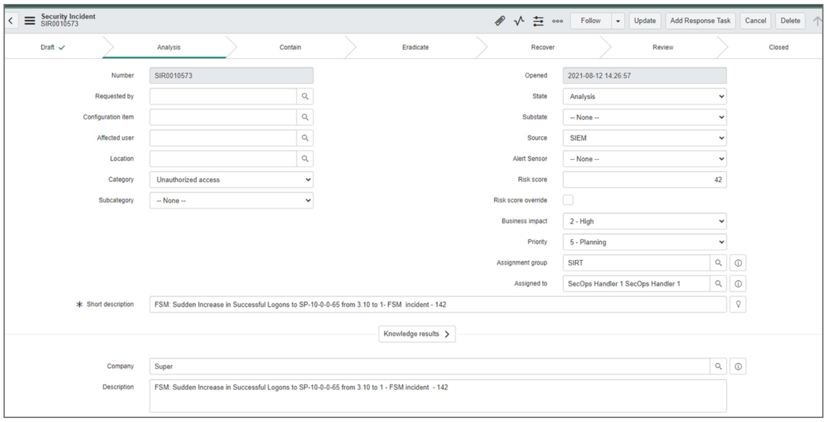
```
FSM : <IncidentTitle> - FSM Incident - <IncidentID>
```



Number	Risk score	Priority	Configuration item	Assigned to	Assignment group	Short description	State	Company
SIR0010572	● 42	5 - Planning	(empty)	SecOps Handler 1 SecOps Handler 1	SIRT	FSM: Sudden Increase in Successful Logons to SP-10-0-0-65 from 3.10 to 1- FSM incident - 142	Analysis	Super

Examine Security Incidents in Detail

Security incidents created by FortiSIEM incident contain the “Category”, “Source”, “Priority”, “Description”, “Short Description”, and “Company” fields, pre-defined based on corresponding FortiSIEM incident fields.



Number	SIR0010573	Opened	2021-08-12 14:26:57
Requested by		State	Analysis
Configuration item		Substate	-- None --
Affected user		Source	SIEM
Location		Alert Sensor	-- None --
Category	Unauthorized access	Risk score	42
Subcategory	-- None --	Risk score override	□
		Business impact	2 - High
		Priority	5 - Planning
		Assignment group	SIRT
		Assigned to	SecOps Handler 1 SecOps Handler 1

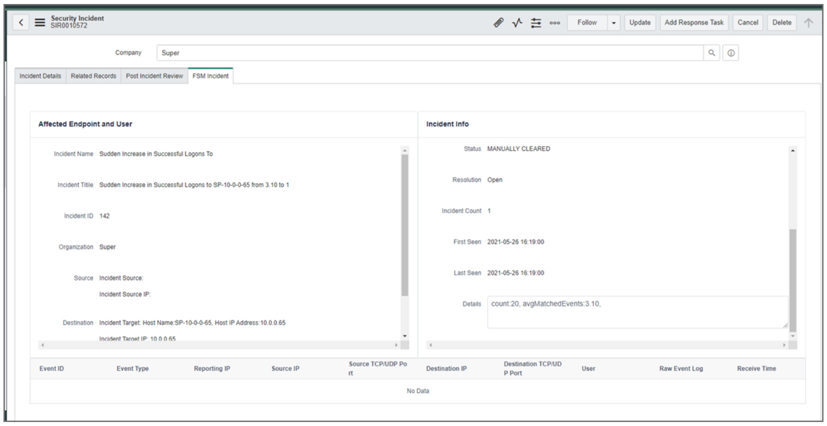
∗ Short description: FSM: Sudden Increase in Successful Logons to SP-10-0-0-65 from 3.10 to 1- FSM incident - 142

Company: Super

Description: FSM: Sudden Increase in Successful Logons to SP-10-0-0-65 from 3.10 to 1 - FSM incident - 142

Customized "FortiSIEM Incident" Page

Security incident created by FortiSIEM incidents also have a customized UI section **FSM Incident**, which can be used to view FortiSIEM incident details and triggering events. For the current version V1.3.6, 10 triggering events are fetched per FortiSIEM incident.



Security Incident
SIR0010572

Company: Super

Affected Endpoint and User

Incident Name: Sudden Increase in Successful Logons To

Incident Title: Sudden Increase in Successful Logons to SP-10-0-0-65 from 3.10 to 1

Incident ID: 142

Organization: Super

Source: Incident Source:
Incident Source IP:

Destination: Incident Target: Host Name:SP-10-0-0-65, Host IP Address:10.0.0.65
Incident Target IP: 10.0.0.65

Incident Info

Status: MANUALLY CLEARED

Resolution: Open

Incident Count: 1

First Seen: 2021-05-26 16:19:00

Last Seen: 2021-05-26 16:19:00

Details: count:20, avgMatchedEvents:3.10,

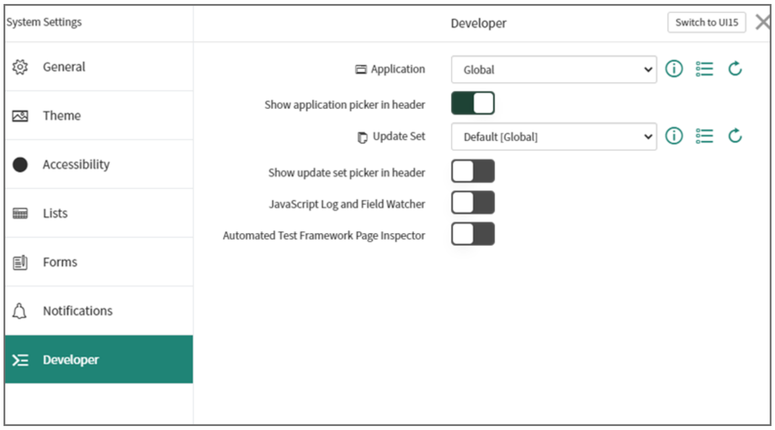
Event ID	Event Type	Reporting IP	Source IP	Source TCP/UDP Port	Destination IP	Destination TCP/UDP Port	User	Raw Event Log	Receive Time
No Data									

ServiceNow FortiSIEM Integration Deletion

Deleting the Integration will remove the FortiSIEM configuration, scheduled jobs, GUI elements, Incident information from FortiSIEM and Triggering events in ServiceNow. **Do not proceed if these ServiceNow elements and FortiSIEM Incident data is needed in your ServiceNow instance.**

To remove ServiceNow FortiSIEM Integration, take the following steps as a ServiceNow system administrator:

1. Navigate to System Settings, and set Application to **Global**.



System Settings — Developer

Application: Global

Show application picker in header: on

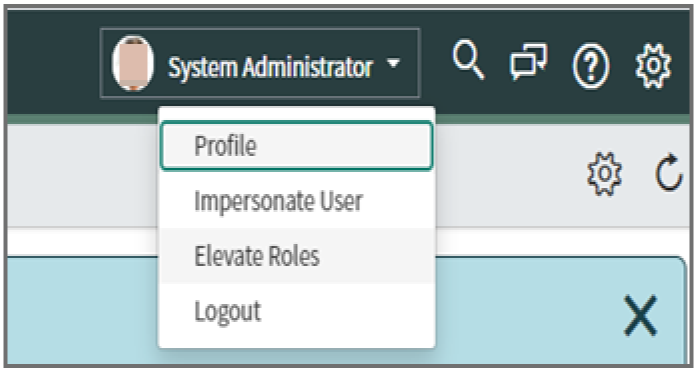
Update Set: Default [Global]

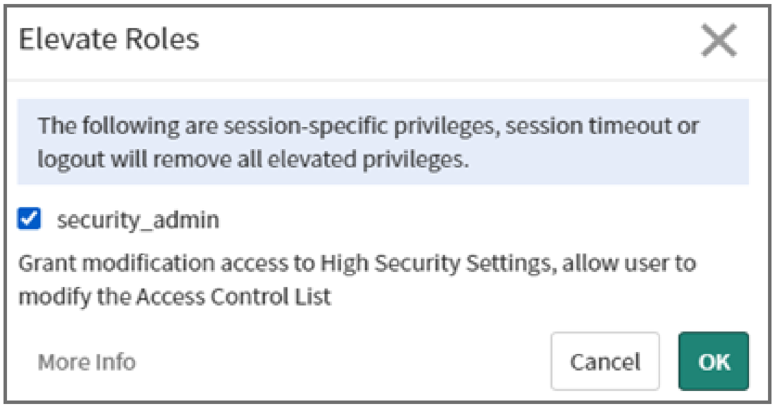
Show update set picker in header: off

JavaScript Log and Field Watcher: off

Automated Test Framework Page Inspector: off

2. Click on the role drop down list and select **Elevate Roles**. Elevate the "System Administrator" role to "Security Admin". This role ensures the success of the ServiceNow FortiSIEM integration import in the next step.





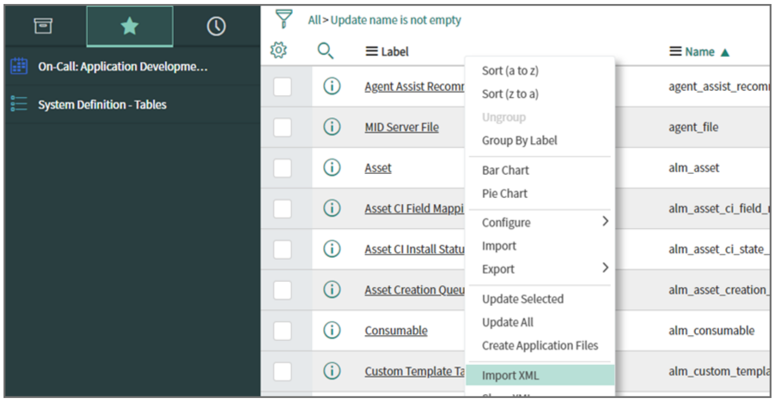
Elevate Roles

The following are session-specific privileges, session timeout or logout will remove all elevated privileges.

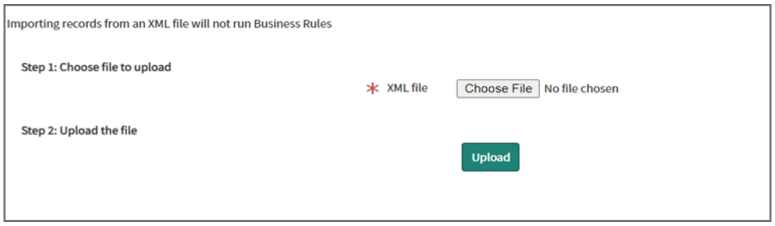
☑ security_admin

Grant modification access to High Security Settings, allow user to modify the Access Control List

3. With the elevated role, navigate to **System Definition - Tables**. Right click on “table headers” on the page and select **Import XML**.



4. In “Import XML”, select the provided `FSMSNIntegrationDeleteData` file (See XML Assets) and click **Upload**.

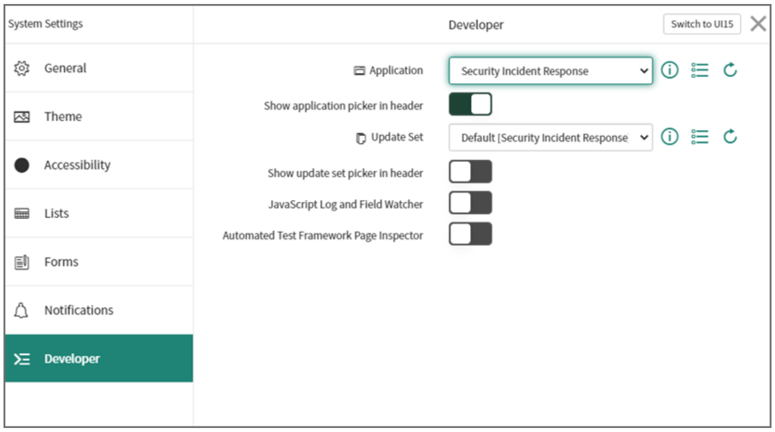


Importing records from an XML file will not run Business Rules

Step 1: Choose file to upload

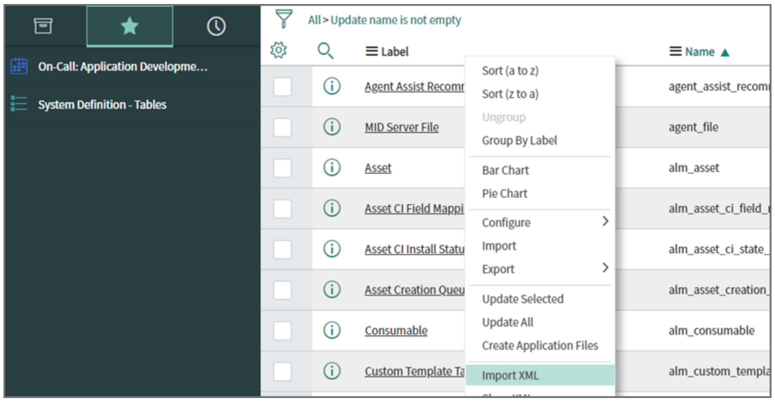
Step 2: Upload the file

5. To complete the deletion process, you must have the elevated “Security Admin” permission, and change **Application** to “Security Incident Response”.



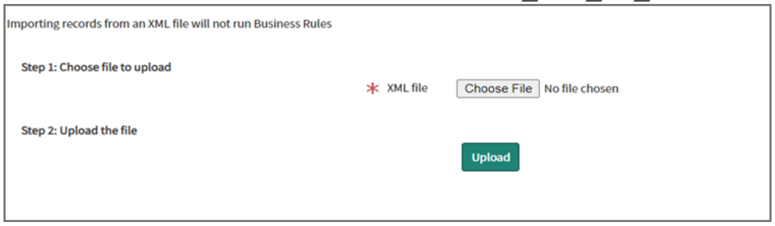
Application: Security Incident Response
Show application picker in header
Update Set: Default [Security Incident Response
Show update set picker in header
JavaScript Log and Field Watcher
Automated Test Framework Page Inspector

6. Navigate to **System Definition - Tables**, right click on “table headers” of the page and select **Import XML**.



Label	Name ▲
Agent Assist Recomm	agent_assist_recomm
MID Server File	agent_file
Asset	alm_asset
Asset CI Field Mappi	alm_asset_ci_field_
Asset CI Install Statu	alm_asset_ci_state_
Asset Creation Queu	alm_asset_creation_
Consumable	alm_consumable
Custom Template Ta	alm_custom_templa

7. In “Import XML”, select the provided `delete_sys_ui_section` file (See XML Assets) and click **Upload**.



Importing records from an XML file will not run Business Rules

Step 1: Choose file to upload

* XML file: Choose File No file chosen

Step 2: Upload the file

The ServiceNow FortiSIEM Integration deletion is now complete.

ServiceNow and FortiSIEM Field Mappings

FortiSIEM Closed State Mappings

FortiSIEM Incident State	ServiceNow Incident State
MANUALLY CLEARED, 2	Closed

FortiSIEM Incident Category Field: "phSubIncidentCategory" Mappings

FortiSIEM Incident Category	ServiceNow Category	FortiSIEM Major Rule Categories
Audit	Policy violation	Change
Authentication	Failed login	Security
Command and Control	Malware	Security
Command and Control	Malware	Security
Credential Access	Unauthorized access	Security
Defense Evasion	Privilege escalation	Security
Discovery	Reconnaissance activity	Security
Execution	Malicious code activity	Security
Exfiltration	Confidential personal identity data exposure	Security
Exploit	Malware	Security
Initial Access	Unauthorized access	Security
Lateral Movement	Privilege esclation	Security
Mail Server	Spam source	Security
Malware	Malware	Security
Persistence	Malware	Security
Policy Violation	Policy violation	Security
Privilege Escalation	Privilege escalation	Security
Reconnaissance	Reconnaissance activity	Security
Suspicious Activity	Reconnaissance activity	Security
UEBA	Insider Breach	Security

The following FortiSIEM incidents do not have a mapping to ServiceNow SecOps categories.

FortiSIEM	ServiceNow	FortiSIEM Major Rule Categories
Application		Performance
Behavioral Anomaly		Security
Collection		Security
CPU		Performance
Database		Performance
Domain Controller		Performance
Environmental		Performance
FortiSIEM		Performance
Hardware		Performance
HVAC		Performance
Impact		Performance
Interface		Performance
License		Availability
Memory		Performance
Network		Performance
Performance		Performance
SDN		Performance
Server		Performance
Storage		Performance
Storage I/O		Performance
Storage Space		Performance
UPS		Performance
Video Con-		Performance

FortiSIEM	ServiceNow	FortiSIEM Major Rule Categories
ferencing		
VoIP		Performance
WAN		Performance
Windows Cluster Service		Performance
Windows File System Replication		Performance

FortiSIEM Incident Severity Field: "eventSeverity" Mappings

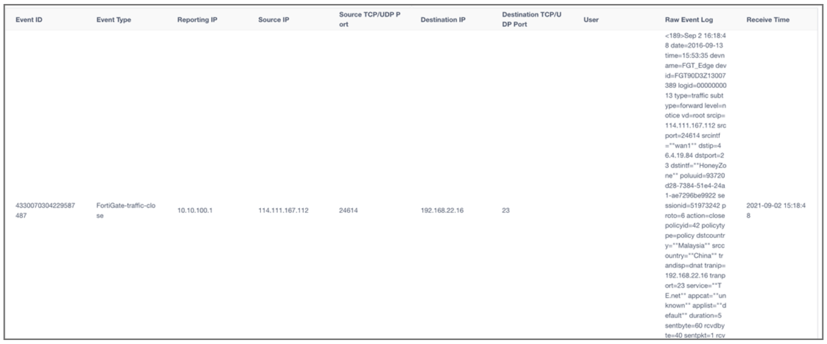
FortiSIEM Severities	ServiceNow Severities
10	1 - Critical
9	2 - High
5 to 8	3 - Moderate
1 to 4	4 - Low
N/A	5 - Planning

FortiSIEM Triggering Events Attributes Displayed in ServiceNow

Name	Attribute Name	Type	Always Present in Triggering Events
Event Receive Time	phRecvTime	date	Yes
Event Type	eventType	string	Yes
Reporting IP	reptDevIpAddr	IP	Yes
Source IP	srcIpAddr	IP	No
Source TCP/UDP Port	srcIpPort	uint16	No

Name	Attribute Name	Type	Always Present in Triggering Events
Destination IP	destipAddr	IP	No
Destination TCP/UDP Port	destipPort	uint16	No
User	User	string	No
Raw Event Log	rawEventMsg	string	Yes

Here is an example.



Event ID	Event Type	Reporting IP	Source IP	Source TCP/UDP Port	Destination IP	Destination TCP/UDP Port	User	Raw Event Log	Receive Time
4330070304229587487	FortiGate-traffic-close	10.10.100.1	114.111.167.112	24614	192.168.22.16	23		<189>Sep 2 16:18:48 date=2016-09-13 time=15:53:35 devname=FGT_Edge devid=FGT90D3Z13007389 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=114.111.167.112 srcport=24614 srcintf=""wan1"" dstip=46.4.19.84 dstport=23 dstintf=""HoneyZone"" poluuid=93720d28-7384-51e4-24a1-ae7296be9922 sessionid=51973242 proto=6 action=close policyid=42 policytype=policy dstcountry=""Malaysia"" srccountry=""China"" trandisp=dnat tranip=192.168.22.16 tranport=23 service=""TE.net"" appcat=""unknown"" applist=""default"" duration=5 sentbyte=60 rcvdbyte=40 sentpkt=1 rcv	2021-09-02 15:18:48

Known Limitations

The following are known limitation for this integration:

- Incidents are synced by ServiceNow to FortiSIEM every 30 seconds. This is not configurable.
- Incident status changes in FortiSIEM, e.g. are not synced to ServiceNow.
- Incident External ID and External Incident Status is not synced to FortiSIEM from ServiceNow until there is a change to the ServiceNow incident such as the State or assignment to a User.

Required Permissions for ServiceNow SOAP Integration

General Requirements

FortiSIEM uses ServiceNow Direct Web Service for integration. FortiSIEM communicates on SOAP port 80.

The following SOA APIs are used:

- Insert
- Update
- getKeys
- get
- getRecords

The following role types are required:

- soap_create
- soap_query
- soap_query_update
- soap_update

The following Table and Field permissions are provided.

Required Table and Field Permissions for CMDB Outbound Integration

Main Table Permissions

ServiceNow Table	FortiSIEM Actions	Required Permissions
configuration item [cmdb_ci]	• Query • Insert • Update	• Read • Write • Create
Running Process [cmdb_running_process]	• Query • Insert / Create • Update	• Read • Write • Create
Software Instance [cmdb_software_instance]	• Query • Insert / Create • Update	• Read • Write • Create

Extended Table Permissions

ServiceNow Table	FortiSIEM Actions	Required Permissions
cmdb_ci_linux_server	• Query • Insert / Create • Update	• Read • Write • Create

ServiceNow Table	FortiSIEM Actions	Required Permissions
cmdb_ci_win_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_hpux_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_unix_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_aix_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_solaris_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_esx_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_web_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_app_server_java	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_app_server_tomcat	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_app_server_weblogic	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_app_server_websphere	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_app_server_jboss	• Query • Insert / Create	• Read • Write

ServiceNow Table	FortiSIEM Actions	Required Permissions
	• Update	• Create
cmdb_ci_netware_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_database	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_vpn	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_ip_router	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_netgear	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_ups	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_printer	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_network_adapter	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_storage_disk	• Query • Insert / Create • Update	• Read • Write • Create

Reference Table Permissions

ServiceNow Table	FortiSIEM Actions	Required Permissions
Company [core_company]	• Query	• Read

Reference Field Permissions

Field	ServiceNow Table	Required Permissions	Need write_role
company	core_company	• Read • Write	Yes. The default role in ServiceNow is : admin

Regular Field Permissions

Need Read/Write and write_role is not required.

Required Table and Field Permissions for Incident Outbound Integration

Main Table Permissions

ServiceNow Table	FortiSIEM Actions	Required Permissions
Incident [incident]	• Query • Insert / Create • Update	• Read • Write • Create

Reference Table Permissions

ServiceNow Table	FortiSIEM Actions	Required Permissions
Company [core_company]	• Query	• Read

Reference Field Permissions

Field	ServiceNow Table	Required Permissions	Need write_role
assigned_to	sys_user	• Read	Yes. The default role in ServiceNow is : itil
company	core_company	• Read • Write	Yes. The default role in ServiceNow is: admin

Regular Field Permissions

Field	Required Permissions	Need write_role
state	• Read	Yes. The default role in ServiceNow is : itil
comments	• Read • Write	Yes. The default role in ServiceNow is : itil
closed_by	• Read	Yes. The default role in ServiceNow is : itil
short_description	• Read • Write	Yes. The default role in ServiceNow is : itil
impact	• Read • Write	Yes. The default role in ServiceNow is : itil
urgency	• Read • Write	Yes. The default role in ServiceNow is : itil
closed_at	• Read	Yes. The default role in ServiceNow is : admin
work_notes	• Read • Write	Yes. The default role in ServiceNow is : itil
Active	• Read • Write	No

Case Escalation Settings

Case Escalation settings allow you to define escalation policies for incident tickets and then use it as an escalation policy when creating a ticket using FortiSIEM Case system.

Follow the below procedures to enable Case Escalation Settings:

- Adding a Case Escalation Policy
- Modifying a Case Escalation Policy

Adding a Case Escalation Policy

Complete these steps to create an escalation ticket and then use it as an escalation policy while creating a ticket, using FortiSIEM Case system.

1. Go to **ADMIN** > **Settings** > **General** > **Case Escalation** tab.
2. Click **New**.
3. In the **Escalation Policy** dialog box, enter or select the following information:

Settings	Guidelines
Name	[Required] Name of the escalation policy.
Remaining Time	Expiration Time of the policy either relative or absolute time.
Email To	Email the policy to the Assignee or Assignee's Manager.

4. Click **Save**.

Modifying a Case Escalation Policy

Complete these steps to create an escalation ticket:

1. Go to **ADMIN** > **Settings** > **General** > **Case Escalation** tab.
2. Select one or more ticket(s).
3. Use the options below to edit an escalation ticket.
   - **Edit** - to edit an escalation ticket.
   - **Delete** - to delete an escalation ticket.
4. Click **Save**.

Configuring SSL Socket Certificates

Before the 6.0.0 release, the mechanism to communicate notifications between backend processes and the app server was through plain sockets. Beginning with the 6.0.0 release, these communications are performed by the safer SSL sockets.

Before starting to transport data through the SSL tunnel, certificates are used to authenticate endpoints. Certificate verification is important, because “man-in-the-middle” attacks can happen when certificate verification is not enabled.

SSL certificate verification is performed in two directions: the client verifies the server’s certificate and the server verifies the client’s certificate.

By default, certificate verification is disabled in both directions in FortiSIEM. This section describes how to configure certificate verification in FortiSIEM

Running the SSL Configuration Script

The `config-ssl-cert.sh` shell script does the work to configure SSL certificates correctly. This script performs the following tasks:

- Provides values for the SSL configuration attributes in the GLOBAL section of the `/opt/phoenix/config/phoenix_config.txt` file.
- Generates files, such as the certificate chain file, trust store, and key store.
- Restarts backend processes to apply the configuration.

To run the `config-ssl-cert.sh` shell script, follow these steps:

1. Log in to the system as user `root`.
2. Run the `config-ssl-cert.sh` shell script with the appropriate options for your environment. See Script Options and Script Examples.

Note:

- When running the script, use the absolute path for all files and directories.
- The script will back-up the existing `phoenix_config.txt` file and `cert_store`, before modifying it. You can restore the previous version if you need to.

Script Options

The following table describes the options that can be used with the `config-ssl-cert.sh` shell script.

Option	Description
-h	Display the help message of script.
-v <0|1|2|3>	Set certificate verify model. This is a required option, with following possible values. • **0**: Disable certificate verify at both directions • **1**: Enable only the verifying server's certificate. This means that the client will verify the certificate from server, but server will not require or verify the certificate from client. • **2**: Enable only the verifying client's certificate. This means that the server will require and verify certificate from client, but client will not verify the certificate from server • **3**: Enable certificate verification in both directions. This means that the client will verify the certificate from server, and server will require and verify the certificate from client.
-p	This option indicates whether the provided certificate is public. Public certificates are signed by a well-known CA organization. It should not be signed by a private CA, or by itself. This option is useful, because it indicates whether you need a CA for the certificate. As you know, if the certificate is public, then the ROOT CA for that certificate is always installed in the system by default. You do not have to provide one. However, if the certificate is private, then a private CA is required.
-c <Certificate file> -k <Key file>	The **-c** and **-k** options are used together to specify the Certificate File and corresponding Key file.
-a <CA file> -d <CA dir>	The CA is used to verify the certificate. The **-a** and **-d** options are used together to specify the CA file and the directory where it is stored. If the provided certificate is private, then the CA is required. If the provided certificate is public, then the CA is optional (typically, it is not needed).

Option	Description

-i <Intermediate CA chain file>	If the certificate is not signed by the ROOT CA directly (this is typically the case for public certificates), then there is a trust chain:
	`Certificate -> Intermediate CA1 -> Intermediate CA2 ->…-> Root CA`
	Use this option to provide the intermediate CA (`Intermediate CA`) chain. If there is only one intermediate CA, then that intermediate CA certificate can act as the intermediate CA chain file directly. If there is more than one intermediate CA, then you must create a chain file for them by using the `cat` command, for example:
	`cat IntermediateCA1 Intermediate CA2 … IntermediateCAn > IntermediateCAChain`

-s <cert_store>	You might need to generate some useful files, such as the trust store file and key store file. Use this option to specify where you want to store those files. By default, they will be stored in the `/opt/phoenix/config/cert_store` directory.

-r	Typically, you must restart backend processes to apply the configuration changes. Use this option, to instruct the script to restart the processes automatically.
	NOTE: because you are configuring the notification communicating mechanism, it might fail if you try to restart the backend processes using tools such as `phtools --stop` all or `monctl stop`.
	If you want to restart the backend processes manually, use following commands:
	`phstatus.py |grep ph |cut -d' ' -f1 |xargs killall -9`
	`monctl start`
	`phtools --start all`

Script Examples

- Disable Certificate Verification in Both Directions
- Enable Verification in Both Directions Using a Public Certificate
- Enable Verification in Both Directions with a Self-Signed Certificate

Disable Certificate Verification in Both Directions

This command disables verification in both directions:

```
config-ssl-cert.sh -v 0 -r
```

where:

- `-v 0` - disables verification in both directions.
- `-r` - restarts backend processes to apply the changes.

Enable Verification in Both Directions Using a Public Certificate

This command enables verification in both directions using a public certificate.

```
config-ssl-cert.sh -v 3 -p -c /opt/star_qa_fortisiem_fortinet_com.crt -k /opt/star_
qa_fortisiem_fortinet_com.key -i /opt/DigiCertCA.crt -r
```

where:

- `-v 3` - enables verification in both directions. You can change to `1` to verify only the server's certificate, or change to `2` to verify only the client's certificate.
- `-p` - specifies that the `-c` and `-k` options identify the <certificate, key> pair of a public certificate.
- `-i` – specifies that there is an intermediate CA for the certificate. This means that there is a trust chain here: `star_qa_fortisiem_fortinet_com.crt -> DigiCertCA.crt -> Root CA`.

Because this is a public certificate, the CA (`-a`) option is not required.

Enable Verification in Both Directions with a Self-Signed Certificate

This command enables verification in both directions using a self-signed certificate.

```
config-ssl-cert.sh -v 3 -c /etc/pki/tls/certs/localhost.crt -k /etc/p-
ki/tls/private/localhost.key -a /etc/pki/tls/certs/localhost.crt -r
```

where:

- The absence of the `-p` option indicates that the provided `-c` and `-k` options are specifying a private <certificate, key> pair.
- `-a` – specifies the CA file used to verify the certificate. This is the certificate itself, in the self-signed case.

Cloud Machine Learning

This document describes how to configure AWS SageMaker for running FortiSIEM Machine Learning jobs in AWS.

Set Up AWS SageMaker

To set up AWS SageMaker, take the following steps.

Step 1: Create an AWS Account

If you already have an AWS account, proceed to Step 2. Make sure you have your AWS account ID for the next step.

To create an AWS account, navigate to https://portal.aws.amazon.com/billing/signup, follow the instructions there, and record your AWS account ID for use in Step 2.

Step 2: Create an IAM Administrator User and Group

When you create an AWS account, you get a single sign-in identity that has complete access to all of the AWS services and resources in the account. This identity is called the AWS account root user. Signing in to the AWS console using the email address and password that you used to create the account gives you complete access to all of the

AWS resources in your account. Fortinet strongly recommends that you not use the root user for everyday tasks, even administrative ones. Instead, adhere to the Security best practices in IAM.

To create an administrator user, follow the instructions here: Creating Your First IAM User and Administrators Group.

Step 3: Create SageMaker Execution Role and Policy

To create a SageMaker execution role and policy, take the following steps.

1. Open your IAM console at https://console.aws.amazon.com/iam/.
2. In the left pane, under **Access management**, select **Roles**, then click **Create role**.
3. Click on the **SageMaker** drop-down list, select **SageMaker - Execution**, then click **Next** to go to "Step 2 Add permissions".
4. Select **Next** to go to "Step 3 Name, review, and create".
   Note: The IAM managed policy, AmazonSageMakerFullAccess, is automatically attached to the role being created. To see the permissions included in this policy, click the carat next to the policy name.
5. In the **Role name** field, enter a name for the role, then click **Create role**.
6. On the Roles section of the IAM console, select the role you just created.
   Note: You can locate your role name by entering it partially in the *Search* field.
7. Select **Add permissions**, then click **Create inline policy**.
8. Click **Choose a service**.
9. In the **Service** field, enter "s3", then select s3.
10. Under **Actions**, under **Access level**, select **List**, **Read** and **Write**.
11. Under **Resources**, locate **bucket**, check the **Any** checkbox, then click **Review policy**.
12. Under **Review policy**, in the **Name** field, enter the name of your policy, then click **Create policy**.

Configure FortiSIEM to use AWS SageMaker

Note: Ensure Amazon SageMaker is set up first.

To configure AWS for Cloud Machine Learning, take the following steps:

1. Navigate to **ADMIN > Settings > General > Cloud Machine Learning**.
2. In the **Access Key** field, enter the Access Key for your AWS Cloud account.
3. In the **Secret Access Key** field, enter the Secret Access Key of your AWS Cloud account.
4. In the **Region** field, enter the region where your AWS resides.
5. In the **S3 Bucket** field, enter the S3 bucket.
6. In the **SageMaker Execution Role** field, enter the SageMaker Execution role.
7. Click **Test**.
8. If Test is successful, click **Save**.

Other Tasks

- Checking AWS SageMaker Training Job Status
- Checking AWS SageMaker Hyperparameter Tuning Job Status
- Checking AWS SageMaker Inference Job Status

Checking AWS SageMaker Training Job Status

To monitor your SageMaker training jobs, take the following steps.

1. Navigate to https://console.aws.amazon.com/sagemaker/.
2. In the left navigation pane, expand **Training**, select **Training jobs**, and from the center pane, choose the relevant task name.

Checking AWS SageMaker Hyperparameter Tuning Job Status

To check on the status of your SageMaker Hyperparameter tuning jobs, take the following steps.

1. Navigate to https://console.aws.amazon.com/sagemaker/.
2. In the left navigation pane, expand **Training**, select **Hyperparameter tuning jobs**, and from the center pane, choose the relevant task name.

Checking AWS SageMaker Inference Job Status

1. Navigate to https://console.aws.amazon.com/sagemaker/.
2. In the left navigation pane, expand **Inference**, select **Batch transform jobs**, and from the center pane, choose the relevant task name.

Implementation Notes

- AWS Auto Mode Running Time

AWS Auto Mode Running Time

Training time for AWS Auto mode is relatively long and only suitable for large amounts of data (e.g. more than 20K rows).

Managing CMDB

FortiSIEM Configuration Management Database (CMDB) contains the following:

- Discovery information about your IT infrastructure such as devices, applications, and users.
- Information derived from your discovered infrastructure, including inter-device relationships such as the relationship of WLAN Access Points to Controller, and Virtual Machines to ESX Hosts.
- Information about system objects such as business services and CMDB reports.

The following topics provide more information about managing CMDB:

Devices

You can add devices to the CMDB through the Discovering Infrastructure process. However, there may be situations in which you want to add devices to the CMDB manually. For example, you may not have access credentials for a device but still want to include network information about it so that logs received by FortiSIEM can be parsed properly.

These topics describe those situations and provide instructions for adding a device to the CMDB:

Viewing Device Information

To view device information, open the **CMDB** page and click **Devices** in the left panel. Expand **Devices** to see all of the subgroups belonging to it. Click **Devices**, or on one of its subgroups, to see the devices in the table associated with that group. The icons above the panel allow you to add, edit, and delete subgroups. System-defined subgroups cannot be deleted, but they can be edited. For more information on managing device groups, see Working with Device Groups.

The headings and numbers at the top of the page, such as above **Routers**, **Firewall**, **Windows**, and so on, represent the number of devices of that type that are active in FortiSIEM. Click the heading to see the devices associated with that device type.

The table on the right of the page displays a list of all of the devices known to FortiSIEM. The table contains columns such as the **Device Name**, **IP** address, **Device Type**, **Status**, and so on.

On the **CMDB** page you can do the following:

- Choose which columns to display by clicking the **Choose columns** icon. For more information, see Changing Display Columns.
- Create, edit, and delete devices by clicking the **New**, **Edit**, and **Delete** buttons. See Creating and Editing Devices for more information.
- Filter the list of devices by organization by opening the drop-down list to the right of the **Delete** button.
- Perform a variety of operations on a selected device by making a selection from the **Actions** drop-down list. For more information on the operations you can perform, see Performing Operations on Devices.
- Get more information about a device by clicking a device name and then clicking one of the buttons beneath the table: **Summary**, **Properties**, **Monitor**, **Software**, **Hardware**, **Configuration**, **Relationships**, and **File**. The information returned is described in the following table.

Selection	Description
Summary	Click **Summary** to return general information about the device such as the **Name**, **Device Type**, **Importance**, **IP address**, and so on. It also displays information regarding the device's health, what group it is a member of, and various statistics (such as **Created**, **Last Discovered**, **Last Updated**, and so on.
Properties	Click **Properties** to view general device location information.
Monitor	Click **Monitor** to return tables describing the **Event Received Status** and **Monitor Status**.
Software	Click **Software** and make a selection from the drop-down list: **Installed Software**, **Running Applications**, **Windows Services**, or **Installed Patches** to get more detailed information. For **Installed Software**, you have the following options: • **Diff...** - Click to compare two selected files/revisions. **Note**: Use Ctrl-Click to select a second file. • **Delete** - Click to delete selected file(s). You will be prompted to confirm the deletion. **Note**: You can use Ctrl-Click and Shift-Click to select multiple files. • **Export** - Click to export selected files as a PDF report.

Selection	Description
Hardware	Click **Hardware** and make a selection from the drop-down list: **Interfaces**, **Processes**, **Storage**, **SAN Storage**, **System BIOS**, **Components**, or **SAN Ports**.
Configuration	Click **Configuration** to view the existing configuration files for your router device. For **Configuration**, you have the following options: • **Diff...** - Click to compare two selected files/revisions. **Note**: Use Ctrl-Click to select a second file. • **Delete** - Click to delete selected file(s). You will be prompted to confirm the deletion. **Note**: You can use Ctrl-Click and Shift-Click to select multiple files. • **Export** - Click to export selected files as a PDF report.
Relationships	Click **Relationships** to return the device's **Node Name**, **Access IP**, **Version**, **Device Type**, and **Description**.
File	Click **File** to view any version or content files from your Windows/Linux agent devices. You have the following options: • **Diff...** - Click to compare two selected files/revisions. **Note**: Use Ctrl-Click to select a second file. • **Delete** - Click to delete selected file(s). You will be prompted to confirm the deletion. **Note**: You can use Ctrl-Click and Shift-Click to select multiple files.

Working with Device Groups

This section provides the procedures to set up Device Groups.

- Adding Device Groups
- Modifying Device Groups
- Performing Operations on Device Groups
- Changing Display Columns

Adding Device Groups

Complete these steps to add device groups:

1. Go to **CMDB** and click **Devices** folder on the left panel.
2. Click **+** above the list of CMDB groups list.
3. In the **Create New Device Group** dialog box, enter/select the information below:

Settings	Guidelines
Organization	Select the organization from the drop-down list.

Settings	Guidelines
Group	[Required] Enter a name for the group.
Description	Enter a description of the device group.
Folders	Choose a folder under **Devices** where you want to create the new group.
Items	Displays the devices in the selected folder. Use the **|<**, **<**, **>** and **>|** buttons to page through the list of devices. Select the devices you want to include in the new group.
Selections	Click **>** to shuttle the selected devices into the **Selections** column. These devices will be the members of the new group.

4. Click **Save**.
   The new device group appears on the left panel.

Modifying Device Groups

Complete these steps to modify a Device Group:

1. Click **Devices** from the left panel and navigate to the device group.
2. Select the required change from the table below:

Settings	Guidelines
Edit	To modify any Device Group.
Delete	To delete any Device Group.

3. Click **Save**.

Performing Operations on Device Groups

You can perform a number of operations on devices or device groups by selecting the **Actions** drop-down list. For more information on these actions, see Performing Operations on Devices and Device Groups.

Changing Display Columns

Complete these steps to choose which columns appear in the device table.

1. Click the **Choose columns** icon.
2. In the Select Columns dialog box, select the columns you want to display from **Available Columns** and use the **>** button to shuttle them to **Selected Columns**. Likewise, you can remove columns from the display by selecting columns in **Selected Columns** and using the **<** button to shuttle them to **Available Columns**.
3. Click **Save**.

The table will display your chosen columns.

Creating and Editing Devices

Complete these steps to add a new device.

1. Click **CMDB** and select the device group under **Devices** on the left panel.
2. Click **New**.
3. In the **Add New Device** dialog box, enter the information under **Summary**, **Contact**, **Interfaces**, and **Properties** tabs.
4. Click **Save**.
   The new device appears in the list.
5. Click on the device from the list.
   A second pane opens below with information under various tabs.

Complete these steps to edit a device:

1. Go to **CMDB** tab.
2. From the left panel, select the device type under **Devices** folder.
3. Select the Device from the list displayed on the table and click **Edit**.
4. In the **Edit Device** dialog box, modify the settings under **Summary**, **Contact**, **Interfaces**, **Properties** and **Parser** tabs.
5. Click **Save**.

Performing Operations on Devices and Device Groups

You can perform various operations on individual devices or device groups by selecting the device or device group and clicking the **Actions** drop-down list. The following table describes the operations you can perform.

Action Settings	Function description
Quick Info	Displays the a summary of information about the device. The information can include the Device Name, Access IP, Device Type , Version, and so on.
Device Health	Displays Availability Status, Performance Status, and a variety of health reports for the device, such as Monitor Status, Incident Status, and so on. Click the **<** and **>** buttons to move through additional health information.
Vulnerabilities	By default, displays the top 10 vulnerabilities of the past week. You can also choose a time interval of 15 minutes, 1 hour, one day, or 30 days.
Incidents	Displays the summary of incidents associated with the device. Click an incident and open the **Actions** drop-down list to drill down on the incident for more information.
Risk	Displays incidents information under **INCIDENTS > Risk** tab.

Action Settings	Function description
Real-time Events	Opens a Real Time Search window for events for the selected device. For more information, see Viewing Real-time Search Results.
Historical Events	Displays the historical events under **ANALYTICS** tab. Use **Actions** tab on top-left corner to email, export, copy to a new tab or save results. For more information, see Viewing Historical Search Results.
Real-time Performance	Displays the real-time Performance Metrics of the selected device. You can choose a **Monitor**, and **Collector** from the drop-down lists, and set the polling **Frequency** and the number of **Runs**.
Impacted Business Services	Displays the Business services that contain the selected device.
Change Status	Changes the status of the device to **Approved** or **Unmanaged**. The devices under license are called 'Managed' while the remaining devices are called "Unmanaged".
Edit Location	Changes the device location address: Country, State, City, Latitude, Longitude, Region, Building and Floor.
Change Organization	Changes the organization in the **New Organization** drop-down list.
Impacted Organization	Select the **Impacted Orgs** from the drop-down list.
Decommission	Decommissions the selected device. Enter a reason in the Decommission Device dialog box.
Recommission	Recommissions the selected device.
Connect To	Connects to a specific Protocol or Port. Select a **Protocol** from the drop-down list and enter a **Port** number and **User** name. A Secure Shell plugin is required. **Note**:If you have upgraded or performed a fresh install of FortiSIEM 6.3.0 or later, and attempt to connect via a tunnel, it will appear that the tunnel is opened. However, the displayed Supervisor's port on which the tunneled connection is running is actually not open so you will not be able to connect either via plugin or directly. To re-enable open tunnels, follow the steps in Open Tunnel Re-Configuration Required after 6.3.0 or later Upgrade/Fresh Install. Tunnels are closed by default to address bug 602294: CVE-2004-1653 SSH port forwarding exposes unprotected internal services.

Action Settings	Function description
Re-Discover	Specify the **Range Definition** information to rediscover the device. For a description of the options in the Discovery Definition dialog box, see the table in Creating a discovery entry.
Add to WatchList	Add the device to Watchlist. In the Add to Watch List dialog, select the **Attribute**, **Organization**, and **Expires** on time. Make selections from the list using the **>** button.
Enable Agent	Enables Agent monitoring for the selected device.
Disable Agent	Disables Agent monitoring for the selected device.

Associating Parsers to a Device

You can attach a set of parsers to a device in CMDB. This overrides the default parser selection mechanism based on the Event Format Recognizer. When a device with a list of attached parsers sends a log, the specified parsers are attempted first.

1. Go to **CMDB** tab.
2. From the left panel, select the device(s) under **Devices** folder.
3. Click **Edit** and select the **Parsers** tab.
4. Select the parsers from the **Available Parsers** list and move to the **Selected Parsers** list using the right arrow.
   You can use the up and down arrows to re-arrange the order of the parsers. Note that the parsers will be attempted in order.
5. Click **Save** to confirm the parser selection.
   The selected parsers are now associated to the device.

Searching for Devices

FortiSIEM allows you to search for CMDB devices based on system device properties and custom device properties.

Note: For custom properties to appear in the search list, you must first select them in **ADMIN > Device Support > Custom Property**. To select and define custom properties, see Working with Custom Properties.

1. Go to **CMDB > Devices**.
2. Click the **Search** icon.
3. Select the value(s) you want to search for:
   - In the drop-down list, click a device attribute (for example, **Device Type**). All possible values of the selected attribute (for example, Cent OS, VMware, Cisco, and so on) are displayed with a count next to it. You can select multiple attributes and values in the drop-down list. The results will be ANDed together.
   - If you need to search for a column or an attribute value, enter it in the **Search** field.
4. Click **Search** at the top of the drop-down list.
   The top 5 items are returned. Click **Show All** to display all of the returned items.
5. The CMDB device list updates based on your search criteria.

6. To refine your search, click the **Search** icon again and select other CMDB device attributes or click **X** to cancel a selection.

Applications

Applications in the CMDB are grouped at the highest level by Infrastructure and User apps, with further sub-categorization in each of those two categories.

Viewing Application Information

Complete these steps to add and view application information:

1. Click **CMDB** and select the application group under **Applications** on the left panel.
2. Click **New**.
3. In the **Add New Application** dialog box, enter the information related to the Application.
4. To add an IP to the Application, click the edit icon near **Running on**.
    a. Click **Add by IP** and enter the IP in the search box.
    b. Click the tick mark.
5. Click **Save**.
   The new application appears in the list.
6. Click on the application from the list.
   A second pane opens below with information under various tabs.

Editing Applications

Complete these steps to edit an application:

1. From the left panel tree, select the application group under **Applications**.
2. Select the Application from the list and click **Edit**.
3. In the **Edit Application** dialog box, modify the settings.
4. To modify an IP, click the edit icon near **Running on** and select the IP.
    - Click **Add by IP** to add a new IP.
    - Click **Delete** to delete the IP.
5. Click **Save**.

Working with Application Groups

This section provides the procedures to set up Application Groups.

- Adding Application Groups
- Modifying Application Groups

Adding Application Groups

Complete these steps to add Application groups:

1. Go to **CMDB** and click **Applications** folder on the left panel.
2. Click **+** above the list of CMDB groups list.
3. In the **Create New application Group** dialog box, enter/select the information below:

Settings	Guidelines
Organization	Select the Organization.
Group	[Required] Group name.
Description	Description about the application group.
Folders	Folder under **Applications** where the group has to be created.
Items	Items to add under the application group.
Selections	Click **>** to confirm the selections from **Folders** and **Items**.

4. Click **Save**.
   The new application group appears on the left panel.

Modifying Application Groups

Complete these steps to modify an Application Group:

1. Click **Applications** from the left panel and navigate to the Application group.
2. Use the delete, edit or move icon above the application groups list for the required modification.
3. Click **Save**.

Users

FortiSIEM CMDB Users page contains information about the users of your system.

Adding Users

The following section describes how to add users to FortiSIEM CMDB. Once an user is defined, you can do the following functions:

- Allow the user to log in to FortiSIEM GUI
- Allow the user to receive FortiSIEM notification
- Use the users in Analytics (Rules and Reports)

You can add users in one of the following ways:

- Add Users Manually
- Discover Users from Microsoft Active Directory
- Discover Users from OKTA

See Implementation Notes for additional information.

Add Users Manually

Complete these steps to add a user:

1. Navigate to **CMDB > Users > Ungrouped**.
2. Click **New** to create a new user.
3. In the **New User** dialog box, enter the detailed information about this user:
   a. Add the user profile information including **User Name**, **Full Name**, **Job Title** and **Company**.
   b. Click the drop-down list to select the **Importance** of this user - "Normal", "Important", "Critical", or "Mission Critical".
   c. Enable **Active** if this is an active user.
   d. Enter the user's **Domain**.
   e. Enter the user's Distinguished Name **DN**.
   f. For **User Lockout**, select **Unlock by Administrator** or **Delay next login for ## minutes**. If **Delay next login for ## minutes** is selected, enter the number of minutes the user will be unable to log into the system after five successive authentication failures.
   g. Select the **Inactivity Lockout** if you wish to enable lockout after a period of inactivity.
   h. For **Password Reset**, enter the number of days after which a user’s current password for logging in to the system will automatically expire. If left blank, the user's password will never expire.
   i. For **Idle Timeout**, enter the number of minutes after which an inactive user will be logged out.
   j. Enter the **Employee ID** of the user.
   k. Select the **Manager** to which this user belongs.

l. For **System Admin**, enable by selecting the System Admin checkbox.
   i. For **Mode**, select **Local** or **External**.
      If you select **Local**, enter and then reconfirm the user password. For **External**, see Authentication Settings for more information about using external authentication.
      Note: If more than one authentication profile is associated with a user, then the servers will be contacted one-by-one until a connection to one of them is successful. Once a server has been contacted, if the authentication fails, the process ends, and the user is notified that the authentication failed.
   ii. Select a **Default Role** for the user.
      See the topic Role Settings for a list of default roles and permission. You can also create new roles, which will be available in this menu after you create them.

      If this System Admin user should be allowed to approve de-anonymization requests, ensure the **Deobfuscation Approver** role has been configured in Role Settings and that this configured role is selected here.

      If the System Admin user should be allowed to approve remediation requests, ensure the **Remediation Approver** role has been configured in Role Settings and that this configured role is selected here.
   iii. Click **Back** when done.

m. Click **Contact Info** to enter your personal contact information.
   i. Add user contact information to the appropriate contact information fields - **Work Phone**, **Mobile Phone**, **Home Phone**, **SMS**, **SMS Provider**, **ZIP**, **Email**, **Address**, **City**, **State**, and **Country** field.
   ii. If your company uses S/MIME for email, make sure the **Email** field is filled out, and upload the S/MIME certificate in the **Certificate** field by clicking **Upload**, and selecting your certificate.
   iii. Click **Back** when done.

n. Click **Alias** to enter any alias information for the user.
   i. In the **Alias** field, provide the alias user name.
   ii. From the **Identity Provider** field, enter/select from AWS IAM, DUO, or Microsoft AD.
   iii. In the **Description** field, enter any additional information about the alias.
   iv. If another Alias is needed, in the **Row** column, click **+** to add another row for another alias, and repeat steps i-iii.
   v. Click **Save** when done.

o. Enter any **Description** about the user.

4. Click **Save**.
   The new user details appear in the list.

Discover Users from Microsoft Active Directory

- Step 1: Create LDAP Login Credentials and Associate with LDAP Server IP Address
- Step 2: Discover Active Directory Server and Users
- Step 3: Set FortiSIEM Attributes for Users

Step 1: Create LDAP Login Credentials and Associate with LDAP Server IP Address

1. Log in to your Supervisor node.
2. Go to **ADMIN** > **Setup** > **Credentials**.

3. Click **New**.
4. Enter a **Name**.
5. For **Device Type**, select **Microsoft Windows**.
6. Select your **Access Protocol.**
   FortiSIEM supports these LDAP protocols:

Protocol	Settings
LDAP	[Required] IP Host - Access IP for LDAP Port - Non-secure version on port 389
LDAPS	[Required] IP Host - Access IP for LDAPS Port - Secure version on port 636
LDAP Start TLS	[Required] IP Host - Access IP for LDAP Start TLS Port - Secure version on port 389

7. For **Used For**, select **Microsoft Active Directory**.
8. For **Base DN**, enter the root of the LDAP user tree.
9. Enter the **NetBIOS/Domain** for your LDAP directory.
10. Enter the **User Name** for your LDAP directory.
    For user discovery from OpenLDAP, specify the full DN as the user name. For Active Directory, use your server login name.
11. Enter and confirm the **Password** for your **User Name**.
12. Click **Save**.
    Your LDAP credentials will be added to the list of **Credentials**.
13. Under **Enter IP Range to Credential Associations**, click **Add**.
14. Select your LDAP credentials from the list of **Credentials**. Click **+** to add more.
15. Enter the **IP/IP Range** or host name for your Active Directory server.
16. Click **Save**.
    Your LDAP credentials will appear in the list of credential/IP address associations.
17. Click **Test** > **Test Connectivity** to make sure you can connect to the Active Directory server.

Step 2: Discover Active Directory Server and Users

1. Go to **ADMIN** > **Setup** > **Discovery**.
2. Click **New**.
3. For **Name**, enter **Active Directory**.
4. For **Include Range**, enter the IP address or host name for your Active Directory server.
5. Leave all the default settings, but clear the **Discover Routes** under **Options**.
6. Click **OK**.
   Active Directory will be added to the list of discoverable devices.
7. Select the Active Directory device and click **Discover**.
8. After discovery completes, go to **CMDB > Users** to view the discovered users.
   You may need to click **Refresh** for the user tree hierarchy to load.

Step 3: Set FortiSIEM Attributes for Users

1. From the **CMDB > Users** page, select the user, and click **Edit**.
2. From the **Manager** drop-down list, select the Manager which this user belongs.
3. For **System Admin**, enable by selecting the System Admin checkbox.
   a. For **Mode**, select **Local** or **External**.
      If you select **Local**, enter and then reconfirm the user password. For **External**, see Authentication Settings for more information about using external authentication.
      Note: If more than one authentication profile is associated with a user, then the servers will be contacted one-by-one until a connection to one of them is successful. Once a server has been contacted, if the authentication fails, the process ends, and the user is notified that the authentication failed.
   b. Select a **Default Role** for the user.
      See the topic Role Settings for a list of default roles and permission. You can also create new roles, which will be available in this menu after you create them.
4. Click **Save**.

Discover Users from OKTA

- Step 1: Prepare OKTA for Authentication
- Step 2: Create an OKTA API Token
- Step 3: Create OKTA Login Credentials in FortiSIEM and Associate with OKTA Server
- Step 4: Discover OKTA Users
- Step 5: Set FortiSIEM Attributes for Users

Step 1: Prepare OKTA for Authentication

To use Okta authentication for your FortiSIEM deployment, you must set up a SAML 2.0 Application in Okta, and then use the certificate associated with that application when you configure external authentication.

1. Log into Okta.
2. In the **Applications** tab, create a new application using **Template SAML 2.0 App**.
3. Under **Settings**, configure the settings similar to the table below:

Post Back URL	Post Back URL
Application label	FortiSIEM Demo
Force Authentication	Enable
Post Back URL	https://<FortiSIEMIP>/phoenix/okta
Name ID Format	EmailAddress
Recipient	FortiSIEM
Audience Restriction	Super

Post Back URL	Post Back URL
authnContextClassRef	PasswordProtectedTransport
Response	Signed
Assertion	Signed
Request	Uncompressed
Destination	https://<FortiSIEMIP>/phoenix/okta

4. Click **Save**.
5. In the **Sign On** tab, click **View Setup Instructions**.
6. Click **Download Certificate**.
7. Follow the instructions above and enter the downloaded certificate for Okta authentication.

Step 2: Create an OKTA API Token

1. Log in to Okta using your Okta credentials.
2. Got to **Administration** > **Security** > **API Tokens**.
3. Click **Create Token**.
   You will use this token when you set up the Okta login credentials in the next section. Note that this token will have the same permissions as the person who generated it.

Step 3: Create OKTA Login Credentials in FortiSIEM and Associate with OKTA Server

1. Log in to your Supervisor node.
2. Go to **ADMIN** > **Setup** > **Credentials**.
3. Click **New**.
4. Enter a **Name**.
5. For **Device Type**, select **OKTA.com OKTA**.
6. For **Access Protocol**, select **OKTA API**.
7. Enter the **Pull Interval** in minutes.
8. Enter the **Domain** associated with your Okta account.
   For example, `FortiSIEM.okta.com`.
9. Enter and reconfirm the **Security Token** you created.
10. Enter any related information in **Description**.
11. Click **Save**.
    Your Okta credentials will be added to the list of **Credentials**.
12. Under **Enter IP Range to Credential Associations**, click **New**.
13. Enter the **IP/IP range** or host name for your Okta account.
14. Select your Okta credentials from the list of **Credentials**. Click **+** to add more.
15. Click **Save**.
    Your Okta credentials will appear in the list of credential/IP address associations.
16. Click **Test** > **Test Connectivity** to make sure you can connect to the Okta server.

Step 4: Discover OKTA Users

If the number of users is less than 200, then Test Connectivity will discover all the users. Okta API has some restrictions that do not allow FortiSIEM to pull more than 200 users. In this case, follow these steps:

1. Log in to **Okta**.
2. Download user list CSV file (OktaPasswordHealth.csv) by visiting **Admin** > **Reports** > **Okta Password Health**.
3. Rename the CSV file to `all_user_list_%s.csv`. (`%s` is the placeholder of token obtained in Create an Okta API Token - Step 3, e.g. `all_user_list_00UbCrgrU9b1Uab0cHCuup-5h-6Hi9I-tokVDH8nRRT.csv`).
4. Log in to **FortiSIEM Supervisor node**:
   a. Upload CSV file `all_user_list_%s.csv` to this directory `/opt/phoenix/config/okta/`
   b. Make sure the permissions are `admin` and `admin` (Run `chown -R admin:admin /opt/phoenix/config/okta/`)
   c. Go to **ADMIN > Setup > Credentials > Enter IP Range to Credential Associations**.
   d. Select the Okta entry and run **Test** > **Test connectivity** to import all users.

Step 5: Set FortiSIEM Attributes for Users

1. From the **CMDB > Users** page, select the user, and click **Edit**.
2. From the **Manager** drop-down list, select the Manager which this user belongs.
3. For **System Admin**, enable by selecting the System Admin checkbox.
   a. For **Mode**, select **Local** or **External**.
   If you select **Local**, enter and then reconfirm the user password. For **External**, see Authentication Settings for more information about using external authentication.
   Note: If more than one authentication profile is associated with a user, then the servers will be contacted one-by-one until a connection to one of them is successful. Once a server has been contacted, if the authentication fails, the process ends, and the user is notified that the authentication failed.
   b. Select a **Default Role** for the user.
   See the topic Role Settings for a list of default roles and permission. You can also create new roles, which will be available in this menu after you create them.
4. Click **Save**.

Implementation Notes

- For Service Provider deployments:
  - If you add users as a Super/Global admin, then the added users will be in the Super/Global group.
  - If you login to a specific Organization and create users there, then the users will belong to that Organization.

- When viewing this user list as a Super global user, you may see repetitions of a few **User Names**, where those names exist in multiple Organizations. This can be determined by checking the contents of the **Organization** column.
- Repetition of **User Names** may also occur if an LDAP server has moved from one Organization to another and discovery of that LDAP server introduces users from the previous organization who may share the same user name. In this case, the administrator may wish to remove users that are no longer applicable.
- An Agent User can be created by navigating to **ADMIN > Setup > Organization**, and clicking **New** or **Edit**. These types of Admin Users are not allowed to log into the UI. Their primary purpose is for Windows Agent registration

against the FortiSIEM environment. See Setting Organizations and Collectors (Service Provider) for more information.

Editing User Information

Complete these steps to edit a CMDB user:

1. Navigate to **CMDB > Users >**.
2. Click **Edit**.
3. In the **Edit User** dialog box, update any detailed information about this user:
   a. Edit user profile information including **User Name**, **Full Name**, **Job Title** and **Company**.
   b. Click the drop-down list to select the **Importance** of this user - "Normal", "Important", "Critical", or "Mission Critical".
   c. Enable **Active** if this is an active user.
   d. Update the user's **Domain**.
   e. Update the user's Distinguished Name **DN**.
   f. For **User Lockout**, select **Unlock by Administrator** or **Delay next login for ## minutes**. If **Delay next login for ## minutes** is selected, enter the number of minutes the user will be unable to log into the system after three successive authentication failures.
   g. Select the **Inactivity Lockout** if you wish to enable lockout after a period of inactivity.
   h. For **Password Reset**, enter the number of days after which a user’s current password for logging in to the system will automatically expire. If left blank, the user's password will never expire.
   i. For **Idle Timeout**, enter the number of minutes after which an inactive user will be logged out. By default, when empty, this is set to 15 minutes.
   j. Enter the **Employee ID** of the user.
   k. Select the **Manager** to which this user belongs.
   l. For **System Admin**, enable by selecting the System Admin checkbox.
      i. For **Mode**, select **Local** or **External**.
         If you select **Local**, enter and then reconfirm the user password. For **External**, see Authentication Settings for more information about using external authentication.
         Note: If more than one authentication profile is associated with a user, then the servers will be contacted one-by-one until a connection to one of them is successful. Once a server has been contacted, if the authentication fails, the process ends, and the user is notified that the authentication failed.
      ii. Select a **Default Role** for the user.
         See the topic Role Settings for a list of default roles and permission. You can also create new roles, which will be available in this menu after you create them.

         If this System Admin user should be allowed to approve de-anonymization requests, ensure the **Deobfuscation Approver** role has been configured in Role Settings and that this configured role is selected here.

         If the System Admin user should be allowed to approve remediation requests, ensure the **Remediation Approver** role has been configured in Role Settings and that this configured role is selected here.
      iii. Click **Back** when done.

m. Click **Contact Info** to update the user's personal contact information.
   i. Update the user contact information in the appropriate contact information fields - **Work Phone**, **Mobile Phone**, **Home Phone**, **SMS**, **SMS Provider**, **ZIP**, **Email**, **Address**, **City**, **State**, and **Country** field.
   ii. If your company uses S/MIME for email, make sure the **Email** field is filled out, and upload the S/MIME certificate in the **Certificate** field by clicking **Upload**, and selecting your certificate.
   iii. Click **Back** when done.

n. Update the **Description** about the user.

4. Click **Save**.

Performing Operations on Users

You can perform various operations on an individual user by selecting the user and clicking the **Actions** drop-down list. The following table describes the operations you can perform.

Action Settings	Function description
Unlock	To unlock a user, select the user from the list and click **Actions** >**Unlock**.
Add to WatchList	Select the user from the list and click **Actions** > **Add to WatchList**. In the **Add to Watch List** dialog, select the **Organization** and **Expires on** time. Make the selections from the list using the **>** button and click **Save** to save.
Risk	To view a risk summary of a user, click **Actions > Risk**.

Working with User Groups

This section provides the procedures to set up User Groups.

- Adding User Groups
- Modifying User Groups

Adding User Groups

Complete these steps to add User groups:

1. Go to **CMDB** and click the **Users** folder on the left panel.
2. Click **+** above the list of CMDB groups.
3. In the **Create New User Group** dialog box, provide the following information:

Settings	Guidelines
Organization	Select the Organization.
Group	[Required] Group name.

Settings	Guidelines
Description	Description about the User group.
Folders	Folder under **Users** where the group has to be created.
Items	Items to add under the User group.
Selections	Click **>** to confirm the selections from **Folders** and **Items**.

4. Click **Save**.
   The new User group appears on the left panel.

Modifying User Groups

Complete these steps to modify a User Group:

1. Click **Users** from the left panel and navigate to the User group.
2. Use the delete, edit or move icon above the User groups list for the required modification.
3. Click **Save**.

Business Services

A business service lets you view FortiSIEM metrics and prioritize alerts from a business service perspective. A business service is defined within FortiSIEM as a smart container of relevant devices and applications serving a business purpose. Once defined, all monitoring and analysis can be presented from a business service perspective. It is possible to track service level metrics, efficiently respond to incidents on a prioritized basis, record business impact, and provide business intelligence on IT best practices, compliance reporting, and IT service improvement. What is also novel about FortiSIEM is how easily a business service can be defined and maintained. Because FortiSIEM automatically discovers the applications running on the servers as well as the network connectivity and the traffic flow, you can simply choose the applications and respective servers and be intelligently guided to choose the rest of components of the business service. This business service discovery and definition capability in FortiSIEM completely automates a process that would normally take many people and considerable effort to complete and maintain.

Defining an IT or Business Service can create a logical grouping of devices and IT components which can be monitored together.

Viewing Business Services

Complete these steps to view Business Services:

1. Go to **CMDB** and select a service under **Business Services** in the left panel.
   The services are: IT Srvc, Biz Srvc, Compliance, or Ungrouped.
2. Select the service from the list.
   The lower panel displays the information about the service including the following details: Type, Name, Running on, Access IP, Details, and Maintenance.

Creating Business Services

Complete these steps to create a Business Service:

1. Go to **CMDB** and select a service under **Business Services** in the left panel.
2. Click **New**.
3. In the **New Business Service** dialog box, enter the following information.

Settings	Guidelines
Name	Name of the Business Service group.
Description	Description about the Business Service group.
Filter	Click this field to add the **Filter**.
Devices	Browse this folder to select or search the devices and also the adjacent network devices. Click **>** to move the device selections to the **Selected Devices/Apps** table.
Applications	Browse this folder to select or search the applications, instance running on and adjacent network devices. Click **>** to move the application selections to the **Selected Devices/Apps** table.

4. Click **Save** to save the selections or **Apply Filter and Save** to proceed with adding the service.

You can use the links in the drilldown menu on the Business Services Summary Dashboard to find out more information about incidents, device availability, device and application performance, interface and event status, and real-time and historical search for a selected business service.

Working with Business Service Groups

This section provides the procedures to set up Business Service Groups.

- Adding Business Service Groups
- Modifying Business Service Groups

Adding Business Service Groups

Complete these steps to add Business Service groups:

1. Go to **CMDB** and click **Business Services** folder on the left panel.
2. Click **+** above the list of CMDB groups list.

3. In the **Create New Business Service Group** dialog box, enter/select the information below:

Settings	Guidelines
Organization	Select the Organization.
Group	[Required] Group name.
Description	Description about the Business Service group.
Folders	Folder under **Business Service** where the group has to be created.
Items	Items to add under the Business Service group.
Selections	Click **>** to confirm the selections from **Folders** and **Items**.

4. Click **Save**.
   The new Business Service group appears on the left panel.

Modifying Business Service Groups

Complete these steps to modify a Business Service Group:

1. Click **Business Services** from the left panel and select a Business Service group.
2. Click the required option:
   - **Edit** to modify the settings of a Business Service.
   - **Delete** to remove a Business Service.
3. Click **Save**.

CMDB Reports

You can find all system-defined reports under **CMDB** > **CMDB Reports**. The reports are organized into folders as shown on the left tree. Click a report to view Summary and Schedule information. the report conditions, and the columns included in the report.

CMDB Report Folder	Object to Report On	Report Name
Overall	Device Approval Status	• Approved Devices • Not Approved Devices
	Users	• Discovered Users • Externally Authenticated FortiSIEM Users • Locally Authenticated FortiSIEM Users • Manually Defined Users

CMDB Report Folder	Object to Report On	Report Name
	Rules	- Active Rules - Rules with Exceptions
	Reports	- Scheduled Reports
	Performance Monitors	- Active Performance Monitors
	Task	- All Existing Tasks
	Business Service	- Business Service Membership
Network	Inventory	- Network Device Components with Serial Number - Network Interface Report - Router/Switch Inventory - Router/Switch Image Distribution
	Ports	- Network Open Ports
	Relationship	- WLAN-AP Relationship
Server	Inventory	- Server Inventory - Server OS Distribution - Server Hardware: Processor - Server Hardware: Memory and Storage
	Ports	- Server Open Ports
	Running Services	- Windows Auto Running Services - Windows Auto Stopped Services - Windows Exchange Running Services - Windows IIS Running Services - Windows Manual Running Services - Windows Manual Stopped Services - Windows SNMP Running Services - Windows VNC Running Services - Windows WMI Running Services
	Installed Software / Patches	- Windows Installed Software - Windows Installed Patches - Windows Installed Software Distribution

CMDB Report Folder	Object to Report On	Report Name
Virtualization	Relationship	• VM-ESX Relationship
Beaconing		• CMDB Device Types • CMDB Network Device Count • CMDB Server Count • CMDB Storage Device Count • PING Monitored Device Count • Performance Monitor Status
FortiCare		• FortiCare 360 Device Inventory Report • FortiCare 360 Software License Report • FortiCare 360 Software Update Report • Top FortiCare 360 Customers By Devices Monitored • Top FortiCare 360 Customers and Hardware Models By Count • Top FortiCare 360 Customers and OS Versions By Count
Ungrouped	user-defined	user-defined

The following topics provides information about using CMDB reports.

Creating CMDB Reports

There are two ways you can create new CMDB reports:

- Create a new report from scratch.
- Clone and modify an existing system or user-defined report by selecting a report and clicking **Clone**.

Follow these procedures to create or modify a CMDB Report.

- Creating a CMDB Report
- Cloning and Modifying a CMDB Report
- Exporting a CMDB Report
- Importing and Exporting CMDB Report Definitions

Creating a CMDB Report

1. Go to **CMDB** and select the CMDB report folder where you want to create the report.
2. Click **New**.
3. In the **New CMDB Report** dialog box, enter the following information.

Settings	Guidelines
Report Name	Name of the CMDB report.
Description	Any information related to the new report.
Target	Select the target type.
Conditions	Set the filter conditions by selecting (Attributes, Operator and Value) together with Next Operators. Parenthesis can be added by clicking **+** to give higher precedence to any evaluation conditions.
Display Columns	The columns in the report result. The order can be changed by selecting a column and clicking the Up or Down icons. You can specify the **Order** as ASC or DESC.

4. Click **Save**.

You can also import a report under CMDB by clicking **Import** to browse and choose.

Cloning and Modifying a CMDB Report

You can modify user-defined reports by selecting the report and clicking **Edit**. However, you cannot directly edit a system-defined report. Instead, you have to clone it, then save it as a new report and modify.

1. Go to **CMDB** > **CMDB Reports**.
2. Select the system-defined report you want to modify, and click **Clone**.
3. Enter a name for the new report, and click **Save**.
   The cloned report will be added to the folder of the original report.
4. Select the new report, and then click **Edit**.
5. Modify the report, and click **Save**.

Exporting a CMDB Report

1. Go to **CMDB** > **CMDB Reports**.
2. Select the CMDB Report folder from where the report will be exported.
3. Click **Export** to download and save the report.

Importing and Exporting CMDB Report Definitions

Instead of using the user interface to define a report, you can import report definitions, or you can export a definition, modify it, and import it back into your FortiSIEM virtual appliance. Report definitions follow an XML schema.

Importing a CMDB Report Definition

1. Go to **CMDB** > **CMDB Reports**.
2. Select the CMDB Report folder to where the report will be imported.
3. Click **Import**. The report will appear in the selected folder.

Exporting a Report Definition

1. Go to **CMDB** > **CMDB Reports**.
2. Select the CMDB report to be imported.
3. Click **Export**. The report will appear in the selected folder.
4. Paste the report definition into a text editor, modify it, and then follow the instructions for importing it back into your virtual appliance.

XML Schema for Report Definitions

The XML schema for the report definition is:

```
<cmdbReports>
<cmdbReport>
<name></name>
<naturalid></naturalid>
<description></description>
<selectClause></selectClause>
<orderByClause></orderByClause>
<whereClause></whereClause>
</cmdbReport>
</cmdbReports>
```

This is an example for the **Active Rules** report:

```
<cmdbReports>
<cmdbReport>
<name>Active Rules</name>
<naturalId>PH_CMDB_Report_Overall_8</naturalId>
<target>com.ph.phoenix.model.query.Rule</target>
<description>This report captures active rules on a per organization
basis</description>
<selectClause>ph_drq_rule.ph_incident_category,ph_drq_rule.name,ph_sys_d
omain.name</selectClause>
<orderByClause>ph_drq_rule.ph_incident_category ASC</orderByClause>
<whereClause>ph_drq_rule.active = true</whereClause>
```

```
</cmdbReport>
</cmdbReports>
```

Scheduling a CMDB Report

Complete these steps to schedule a CMDB report to run at a later time:

1. Go to **CMDB** and browse to select the report under **CMDB Reports** on the left tree.
2. Select the report from the list.
3. Click **Schedule**.
4. In the **Schedule** dialog box, select the required information.

Settings	Guidelines
Organization	Organization type. Select whether to **Run this report for** or **Schedule this report for** the remaining settings. • Choose **Run this report for** if you would like to run the report for only Global administrators. This choice will combine event data from all selected Organizations within one PDF, RTF, or CSV report and sent to the Global Administrators added in the notification settings while scheduling report alerts. • Choose **Schedule this report for** if you would like to run this report for each selected Organization seperately same as your login to each of these Organizations and schedule this report there. In this case, each selected Organization will receive its own copy of PDF, RTF, or CSV report containing the event data for its own Organization based on the notification settings added while scheduling report alerts.
Schedule Time Range	Enter the Time range to run the report.
Schedule Recurrence Pattern	Recurrence pattern: once, hourly, daily, weekly or monthly. Enter the start date in the **Start From** field.
Notification	Use the options as required: • Default Notification - to send notification to new recipients by adding them using the **+** icon. • Custom Notification - to send the notification to the specific email addresses added under **ADMIN > Settings > System**. • Copy to a remote location - To copy the report to a remote directory, first define the remote location in **ADMIN > Set-**

Settings	Guidelines
	tings > Analytics > Scheduled Report to be copied to this remote location when scheduler runs any report and then select this option.

5. Click **OK**.

You can also schedule a CMDB report by selecting the report from the list and clicking **+**under **Schedule** tab in the lower pane.

Running a CMDB Report

Complete these steps to run a CMDB Report.

1. Go to **CMDB > CMDB Reports** and select the report you want to run from the folder.
2. Click **Run**.
3. In the **Run CMDB for** dialog box, select the Organization and click **Run**.

Reports are saved only for the duration of your login session. You can view saved reports by clicking **Results**. You can use the **Export** button to export any report in PDF or CSV format.

Adding CMDB Report to Dashboard

Complete these steps to add CMDB reports to Dashboard:

1. Select the dashboard to which you want to add a CMDB report.
2. Click **+** to the right of the dashboard.
3. In the **Create New Dashboard** dialog box, enter a name for the Dashboard and select the Widget Dashboard from the drop-down list. For more information, refer to Dashboard.
4. Click **+** below the Dashboard drop-down list.
5. Select a report from the **CMDB Reports** folder, then click **>**. The report will be added to the dashboard.

Managing Resources

The following sections provide the procedures for managing Resources:

Reports

Reports as similar to pre-defined versions of searches that you can load and run at any time. FortiSIEM includes over 2000 pre-defined reports that you can access in **RESOURCES > Reports**.

Viewing System Reports

Complete these steps to view system-defined Reports:

1. Go to **RESOURCES** > **Reports**.
2. Select the **Organization** for which you want to view the available reports.
3. Expand the **Reports** folder on the left panel and select the sub-category of report to view.
4. Select the report you want to view information about.
   The reports display the information below under various tabs in the lower pane:
   - **Summary** - Includes the **Condition** and **Group By** conditions for the report, and the report's **Display** attributes.

- **Schedule** - Information about when the report is scheduled to run. See Scheduling a Report for more information. Click the **+** icon to set a schedule for the report to run.
- **Results** - The results from any scheduled runs of the report, or results you have saved by running the report.

Note: If Data Obfuscation is turned on for a FortiSIEM user:

- The value for that object marked for data obfuscation is obfuscated. For example, if IP is marked for data obfuscation, the IP address is obfuscated. In earlier versions of FortiSIEM, raw events were completely obfuscated.
- CSV Export feature is disabled.

Working with Report Design Templates

FortiSIEM gives you the flexibility of designing custom templates for each of your reports. When you select **RESOURCES > Reports**, notice that the table of reports includes a **Report Design Template** column. This column identifies the template to be used when generating and exporting a report. By default, all reports are assigned the same template. The default template name has the format *organization_name scope* **Reports Template**. For example, Global System Reports Template would be a report for the Global organization with System scope.

The Global System Reports Template can be edited when you log in as Super/Global. In this case, an Edit icon will appear next to Global System Reports Template after you modify the report design template.

A Template can be created at various levels:

- For each Report in **RESOURCES > Reports**
- For each Report folder in **RESOURCES > Reports**
- For each Report Bundle defined in **RESOURCES > Reports > Report Bundles**

When you run a report under **RESOURCES > Reports**, FortiSIEM will choose the appropriate Report Template in the following order:

1. If a specific template is defined for the selected report, then that template will be chosen.
2. If a template in the previous step is not found, then the template for the folder to which the Report belongs will be chosen.
3. If no matching template is found in Steps 1 and 2, then the system-defined template for the root folder **RESOURCES > Reports** will be chosen. System-defined templates cannot be edited.

If you load and run a report in **RESOURCES > Reports** from the **ANALYTICS** page and then manually export the Report in PDF format:

- If you choose the **Defined** option, then FortiSIEM will use the rules above to find the matching template.
- If you choose the **New** option, then you can define a new Report format for this report instance only.

Note:

- For Service Provider deployments, the Report templates can only be defined at the Super/Global level and applies for all customers.
- If a report is part of two folders and each folder has its own template defined, then the template of the current folder being viewed will be used.

The following sections provide information about:

- Creating a Report Template
- Designing a Report Template

Creating a Report Template

A Report template for PDF can be created as follows:

1. Go to **RESOURCES > Reports** and select one of the subcategories from the left pane.
2. Select the desired row from the table.
3. (Optional) Select the **Sync** checkbox in the row to synchronize the report with the Report Server.
4. Open the **More** drop-down list and select **Report Design**. The Report Design page opens.
5. Notice that the **Name** given to the report template is in the form *organization_name scope report_name* **Template**. You can edit this name if you want.
6. Follow the instructions in Designing a Report Template to design the cover page and add sections, objects, attachments, and so on, to the report.
7. Click **Save**.
   The name of the new template will be displayed in the **Report Design Template** column of the table. Notice that an edit icon appears next to the name of the template.

Creating Report Templates for a Report Folder or Resource Bundle

To create a report template for a Resource folder, choose any Report folder from the left pane. The steps to create the template are similar to Creating a Report Template.

To create a report template for a Report Bundle, complete these steps:

1. Select any system-defined or user-defined report bundle in this group.
2. Select all of the reports in the table.
3. Click **More** > **Report Design**.

Notice that the **Name** of the template for a Report Bundle cannot be edited.

Modifying an Existing Report Template

1. Click the edit icon next to the name of the existing report design template. The Report Design page opens.
2. Make the desired changes to the template design.
3. Click **Save**.

Designing a Report Template

You can design or modify the following template sections using the settings under Report Design for PDF reports:

- Overview
- Cover Page
- Report - Sections and Objects

Overview

Report Designer allows you to build a report out the following objects, the Cover Page, Table of Contents, Pages (Sections), and Objects.

Visual PDF Report Designer Interface

The main interface consists of the **Template Name** field, that allows you to rename your report template, an **Organization** drop-down list to select the organization that the report template belongs to, an **Orientation** drop-down list to choose a Portrait or Landscape generated PDF report, and a horizontal control bar that has the following buttons.

- New Page - Clicking this adds a new page (Section) to your report template structure. A page can contain any number of elements, which include text, images, charts, and report tables.
- Discard Changes - Clicking this removes all prior work done before you saved (Save appears at the bottom of the interface).
- Layout - Allows you to make size and positional adjustments to an element as well as being able to adjust the margins of an element that is selected. To make a positional adjustment, select the Section or Object, and click an arrow (up, down, left, right) to change its position to where you want to move it. To adjust a margin, select the appropriate margin box and enter the new pixel value.
  Note: Only valid position options will be displayed, for example a Page/Section can only be moved up or down, and cannot be positioned left or right, so lef t and right options will not appear if a Page/Section is selected.
- Cover - When selected, a cover will be included with your PDF report. If unselected, no cover page is included with the report.
- TOC - When selected, a table of contents (TOC) will be included with your PDF report. If unselected, no TOC is included with the report.

The buttons that are available depend on how you entered the Visual PDF Report Designer.

If you entered the Visual PDF Report Designer via **Resources**, the following options are available:

At the upper right of the page:

- **Organization**: Select the organization the report is for.
- **Orientation**: Select between Portrait or Landscape.

At the bottom of the page:

- **Save** - Click to save your changes.
  Note: This will overwrite the default template stored for a Report or Report Bundle.
- **Cancel** - Click to cancel out of the Visual PDF Report Designer.
- **Preview** - Click to see a preview of the how the exported data will appear in PDF.
- **Restore to Default** - Removes custom templates that have been created, leaving only the default templates available.

If you entered the Visual PDF Report Designer via **Analytics**, the following options are available:

At the upper right of the page:

- **Orientation**: Select between Portrait or Landscape.
- **Window Size icon**: Toggle between full window or default window.

At the bottom of the page:

- **Generate** - Click to export the report.
- **Cancel** - Click to abandon the report.

Adding an Object

When you create a new Report Design, a default Cover Page and Table of Contents is automatically created.

To add a page, also known as a section, select an existing page and click the **+** icon, and select **Add page above** or **Add page below**. You can also click on the **New Page** button to add a new page/section.

To add an Object, select an existing Object where you wish to add an Object to, then click the **+** icon, and select the Object that you wish to add (Image, Text, Chart, Report Table, Legend, PDF).

Note: Only allowable objects will be available from the drop-down list. For example, a PDF are only available to create from the last page.

Deleting an Object

A report can have a maximum of one Cover Page and one Table of Contents. The Table of Contents is based off the section(s) that you create, or that already exist. To delete any existing object, select the object and then click the trash icon that appears in the upper right corner for that object.

Orientation

You can choose the page orientation that your report appears in by clicking on the **Orientation** drop-down list button and selecting **Portrait** or **Landscape**.

Using the Text Editor when Adding Text to an Object

When you choose to add text to a cover page, section, a text Object will appear. Click on the edit icon to open the text editor. Use the editor to add any text you wish to display with your report in the **Text** window. When done, click **Save**.The text editor also provides the following tools:

Icon	Description
Undo	Click to undo the last typing action.
Redo	Click to re-apply the last undo action.
Size	Click the drop-down list, and select a font

Icon	Description
	size. To apply to existing text, select the text first, then click the icon and select a size.
Font Color	Click the icon and select a color. To apply to existing text, select the text first, then click the icon and select a color.
Bold	Click the icon to begin bolding text. To apply to existing text, select the text first, then click the icon.
Underline	Click the icon to begin underling text. To apply to existing text, select the text first, then click the icon.
Italic	Click the icon to begin italicizing text. To apply to existing text, select

Icon	Description
	the text first, then click the icon.
Strikethrough	Click the icon to begin strikethrough text. To apply to existing text, select the text first, then click the icon.
Remove Format	Click the icon to remove any existing formatting information that is currently being applied. To apply to existing text, select the text first, then click the icon.
Align	Click the Align icon and select one of the following alignments: • Align left - Aligns the text to start at the left side of the window. • Align center - Aligns the text to appear in the center of the window. • Align right - Aligns the

Icon	Description
	text to end at the right side of the window. - Align justify - Aligns text so it is both left and right aligned by inserting spaces between words.
Full Screen/Text Editor	Click to toggle between expanding to full screen and the standard text editor window.
Code view	Click to toggle between normal and code view.

Cover Page

The default Cover Page template includes the Report title, current Organization, Start Time, End Time, Generated Time, and Device Time Zone as Default Text. These sections can be deleted, rearranged, or have text content and images added to them. To modify an existing section, select it, then select the type from the **Cover Type** drop-down list.

- Adding Text to Cover Page
- Adding Images to Cover Page

Adding Text to Cover Page

1. Click the **Cover Page** bar to expand the section.
2. Click on any Object in the Cover page, click the **+** icon, and select **Text** from the drop-down list to add text content to the cover page.
3. Add the text in the **Text** window. For information on text tools, see Using the Text Editor when Adding Text to an Object.
4. Click **Save** to apply the changes.

Adding Images to Cover Page

1. Click the **Cover Page** bar to expand the section.
2. Click on any Object in the Cover page, click the **+** icon, and select **Image** from the drop-down list to add any JPG, PNG, or SVG image in the cover page.
3. Click **Select File** to add the image.
4. From the **Scale** drop-down list, select one of the following:
   - **Not Scale** - The image will not be resized.
   - **Fit Width** - The image will be resized to fit width.
   - **Fit Height** - The image will be resized to fit height.
   - **Fill all** - The image will be resized to fill the entire space available for it.
5. Click on the Left, Center, or Right Alignment icon to adjust the image alignment.

Note:

1. To fill the width of a page, the image size must be set to 5000 x 5000.
2. Even when enlarged, the JPG, PNG, or SVG image will appear pixelated (it does not use vector graphics). the more you zoom the page, the worse the image will look.

Report - Sections and Objects

This section allows you to add new **Sections (Pages)** and **Objects** to your Report. You can also add text content, images, charts, report tables, or a PDF attachment here.

- Adding Sections
- Adding Objects
- Adding Text to a Section or Object
- Adding an Image to a Section or Object
- Adding a PDF to a Custom Report
- Adding a Chart
- Adding a Report Table
- Adding a Legend to a Section
- Adding a CMDB Report to a Section or Object

Adding Sections

Click the **New Page** button to add a section, or from an existing section, take the following step.

1. Select the Section, and click on the **+** icon at the top or bottom of the Section to respectively add a page above the Section, or below it. After clicking the + icon, select **Add page above**, or **Add page below** to add a new Section.

Adding Objects

To add an Object to a Section, select a Section or Object, and click on the **+** icon. From the drop-down list, select an object (Text, Image, Chart, Report Table, Legend).

Note: Only allowable objects will be available from the drop-down list. For example, a Report Table and Legend are only available from a Section, and are not available when selecting **+** from an Object.

Adding Text to a Section or Object

1. Click the required Section or Object.
2. Click on a **+** icon, and select **Text** from the drop-down list to add text information.
3. Click the Text Edit icon and add the text in the **Text** window. For information on text tools, see Using the Text Editor when Adding Text to an Object.
4. Click **Save** to apply the changes.

Adding an Image to a Section or Object

1. Click on the required Section or Object.
2. Click on a **+** icon, and select **Image** from the drop-down list to add any JPG, PNG, or SVG image.
3. Click **Select File** to add the image.
4. From the **Scale** drop-down list, select one of the following:
   - **Not Scale** - The image will not be resized.
   - **Fit Width** - The image will be resized to fit width.
   - **Fit Height** - The image will be resized to fit height.
   - **Fill all** - The image will be resized to fill the entire space available for it.
5. Click on the Left, Center, or Right Alignment icon to adjust the image alignment.

Note:

1. To fill the width of a page, the image size must be set to 5000 x 5000.
2. Even when enlarged, the JPG, PNG, or SVG image will appear pixelated (it does not use vector graphics). the more you zoom the page, the worse the image will look.

Adding a PDF to a Custom Report

A PDF attachment can only be added to the last page (Section) of a Custom report. To add a PDF attachment, click on the bottom **+** icon from the bottom most Page (Section), and select **PDF**. Click **Select File**, and select the PDF file to attach.

Adding a Chart

1. Click on the required section or object bar to expand the section.
2. To add a **Chart**, select a section or object.
3. Click the **+** icon, and select **Chart** from the drop-down list.
4. In the Report Section window, take the following steps.
   a. In the **Chart Name** field, enter the name of the chart.
   Note: The chart name will named as the Display Attribute unless a Chart Name is provided.
   b. From the **Format** drop-down list, select the chart type. The list displays the available charts.
   c. From the **Items** field, enter the number of items to display.
   Note: If the item number is changed for one chart, all charts and Legend within that page will be also be updated with that change.
   d. From the **Report** drop-down list, select the report to use.
   e. From the **Attribute** drop-down list, select an attribute.

Adding a Report Table

1. Click on the required section or object bar to expand the section.
2. To add a **Report Table**, select a section or object.
   Note: The Report Table option is only available if no Report Table exists on the page.
3. Click the **+** icon, and select **Report Table** from the drop-down list.
4. Select the Report from the **Report** drop-down.
5. To display the event type, add a check to the **Event Type** checkbox.
6. To display a summary, add a check to the **Summary** checkbox.
7. When you define a custom template for **Report Bundles** (excluding the root group), you can select any Event Reports from the **Report** drop-down list.
   Note the following:
   - For Report folders (including the root group), the **Report** setting is not available.
   - For a single Report, the Event Report is automatically selected under the **Report** setting and you cannot modify this.

Adding a Legend to a Section

1. Click on the required section to expand the section.
2. Click on the **+** icon, and select **Legend**.

   Note: The Legend option is only available if no Legend exists on the current section.

Adding a CMDB Report to a Section or Object

Note: You can add **CMDB Reports** only to a **Report Bundle** template.

1. Navigate to **Resources > Reports > Report Bundles > <*Report Bundle*>**.
   For <*Report Bundle*>, select a specific Report Bundle, for example Important PCI, Firewall Health, or Router Health.
2. In the left pane, click the Report Design icon.
3. Click on the required section or object bar to expand the section.
4. Click the **+** icon and select **CMDB Report** from the drop-down list.
5. Click the **Edit** icon, then from the Select CMDB Report window, select the **CMDB Report** from the drop-down list. You can also use the search bar to find a specific CMDB report.
6. Click **Save** to confirm the selection.
7. Select the number of **Items** to display.
8. Click **Save** to apply the changes.

Creating New Reports

Creating a Report

Creating a report or baseline report is like creating a structured historical search, because you set the **Conditions** and **Group By** attributes that will be used to process the report data, and specify **Display Columns** to use in the report summary. You can clone an existing report to use as the basis for a new report by selecting the existing report, and clicking **Clone**.

Complete these steps to create a report:

1. Go to **RESOURCES** > **Reports**.
2. Select the report type from the **Reports** folder on the left panel.
3. Click **New**.
4. Enter a **Report Name** and **Description**.
5. For baseline reports, select **Anomaly Detection Baseline**.
6. Enter the **Conditions** to use in your report.
7. Set the **Display Columns** to use in your search results.
8. Click **Save**.
9. Optional - If you want to create a new PDF report template for this report, follow the steps in Working With Report Templates or else the system-defined template will be used.

Your report will be saved into the selected category, and you can run it or schedule it to run later.

Creating a Report Bundle

Complete these steps to create a report bundle:

1. Go to the **RESOURCES** tab and select a **Report Bundle** from the left panel.
2. Click **New**.
3. Enter a **Report Name** and **Description**.
4. For baseline reports, select **Anomaly Detection Baseline**.
5. Enter the **Conditions** to use in your report.
6. Set the **Display Columns** to use in your search results.
7. Click **Save**.
8. Optional - If you want to create a new PDF report template for this report, follow the steps here or else the system-defined template will be used.

Your report will be saved into the selected category, and you can run it or schedule it to run later.

Editing a Report Bundle

Complete these steps to edit a user-defined resource bundle:

1. Go to the **RESOURCES** tab and select a **Report Bundle** from the left panel.
2. Click the Edit icon (✎) above the left panel. The Edit Report Group dialog box opens.
3. Edit the Report Group **Name** and **Description**, if needed.
4. From the **Folders** column select the report subcategory.
5. In the **Items** column, select the desired report(s) to add to the report bundle.
6. Select **Update Template** if you want to add the selected reports to the previously defined Report Bundle template. See Creating a PDF Report Template.
7. Click **Save**.

Running System Reports

FortiSIEM includes a number of baseline reports for common data center analytics, as well as over 300 reports relating to IT infrastructure. You can also create your own reports.

Complete these steps to run a system-generated or user-defined baseline report:

1. Go to **RESOURCES** tab and select the desired report group from the **Reports** folder.
2. Select the report(s) from the table.
3. Click **Run** to run the report(s) immediately, or select **More** and click **Schedule** to schedule the report.
4. If you have a multi-tenant deployment, select the **Organization** for which you want to run the report.
5. Select one of the **Report Time Range** options:
   - **Relative**: Select the last number of hours from which report has to be generated.
   - **Absolute**: Select the range of start and end date and time.
6. Click **OK**.
   The report will run and the results will be displayed.

Starting in 6.1.1, adhoc reports run from GUI and scheduled reports may time out after running for a long time. In a cluster environment with Worker nodes, the user may see partial results (indicated in the PDF), if some workers are able to finish their queries within the timeout. The default timeouts are specified (in seconds) in the `phoenix_config.txt` file on the Supervisor node.

```
[BEGIN phQueryMaster]
...
interactive_query_timeout=1800 # 30 mins
...
scheduled_query_timeout=3600 # 60mins
...
[END]
```

To change the default timeout values, SSH to the Supervisor node, change the values, save the file, and restart the Query Master process.

Scheduling Reports

You can schedule reports/report bundles to run once or for recurring periods in the future. When you schedule a reports/report bundle, you can specify notifications that can be sent for the report. In addition, you should make sure that the default settings for notifications for all scheduled reports/report bundles have been set up.

- Scheduling a Report
- Scheduling a Report Bundle
- Scheduling Reports Using a Workflow

Starting in 6.1.1, adhoc reports run from GUI and scheduled reports may time out after running for a long time. In a cluster environment with Worker nodes, the user may see partial results (indicated in the PDF, in PDF or RTF starting in 6.3.0), if some workers are able to finish their queries within the timeout. The default timeouts are specified (in seconds) in the `phoenix_config.txt` file on the Supervisor node.

```
[BEGIN phQueryMaster]
...
interactive_query_timeout=1800 # 30 mins
```

```
...
scheduled_query_timeout=3600 # 60mins
...
[END]
```

To change the default timeout values, SSH to the Supervisor node, change the values, save the file, and restart the Query Master process.

Scheduling a Report

Complete these steps to schedule a report:

1. Go to **RESOURCES** tab and select the report under **Reports** folder from the left pane.
2. Select the report(s) to schedule from the list on the right pane.
3. Click **More** > **Schedule**.
   Note: You can also schedule a report from the lower pane - select the **Schedule** tab after selecting the report. Use the **+** icon to enter the **Schedule** settings.
4. In Super/Global scope, under **Organization** section, for **Report Data**, you can choose either **Combine all selected Organizations into one Report** or **Generate separate Report for each selected Organization** with selected organizations:
   - Choose **Combine all selected Organizations into one Report** if you would like to run the report for only Global administrators. This choice will combine event data from all selected Organizations within one PDF or RTF report and sent to the Global Administrators added in the Notification settings while scheduling reports.
   - Choose **Generate separate Report for each selected Organization** if you would like to run this report for each selected Organization separately same as your login to each of these Organizations and schedule this report there. In this case, each selected organization will receive its own copy of the CSV, PDF or RTF report containing the event data for its own Organization based on the Notification settings added while scheduling reports.
5. In Report Time Range, configure the range of time that the report should provide. See Specifying Search Time Window.
6. In Trend Interval, configure appropriately if your report uses trend event attributes, otherwise, leave as **Auto**. See Specifying Trend Interval.
7. Click **Next**.
8. Use the **Schedule Time Range** option if the run time has to be scheduled for a later period and a specific place.
9. Schedule the **Schedule Recurrence Pattern** for the report to run once, hourly, daily, weekly, or monthly or set the range under **Schedule Recurrence Range**.
10. Click **Next**.
11. Select the **Output Format** as **PDF**, **CSV**, or **RTF**.
    For PDF and RTF output, the default template configured under **RESOURCES** > **Reports** is used. You can customize the report templates following the steps under Designing a Report Template.
12. Specify the **Notification** that should be sent when the report runs from the available options:
    - **Default Notifications** - to send default notifications. Click the edit icon to add more **Recipients**.
    - **Custom Notifications** - to send notifications to specific email addresses. Use the edit icon to add more **Recipients**
    - **Copy to a remote directory** - to copy the report to a remote directory.

13. Specify the time that the report should be retained after it has run using the **Retention** setting in hours or number of days.
14. Click **OK**.
    The report will run at the time you scheduled.

Scheduling a Report Bundle

Complete these steps to schedule a report bundle:

1. Go to **RESOURCES > Reports** tab and select a report bundle under **Report Bundles** folder from the left pane.
2. Select the clock icon (🕒) above the left panel folders to open the scheduler settings.
3. In the **Schedule Report Bundle** window, click **+**.
4. In Super/Global scope, under **Organization** section, for **Report Data**, you can choose either **Combine all selected Organizations into one Report** or **Generate separate Report for each selected Organization** with selected organizations:
    - Choose **Combine all selected Organizations into one Report** if you would like to run the report for only Global administrators. This choice will combine event data from all selected Organizations within one PDF or RTF report and sent to the Global Administrators added in the Notification settings while scheduling reports.
    - Choose **Generate separate Report for each selected Organization** if you would like to run this report for each selected Organization separately same as your login to each of these Organizations and schedule this report there. In this case, each selected Organization will receive its own copy of the PDF or RTF report containing the event data for its own Organization based on the Notification settings added while scheduling reports.
5. Select the **Report Time Range**:
    - Select the **Time Zone**.
    - Select **Relative** to enter the last number of hours from which report has to be generated or **Absolute** to enter the range of start and end date and time.
6. Select the Trend Interval for **Trend**. See Specifying Trend Interval.
7. Click **Next**.
8. Use the **Schedule Time Range** if the run time has to be scheduled for a later period and a specific place.
9. Click **Next**.
10. Select the **Output Format** as **PDF** or **RTF**.
    For PDF or RTF output, the default template configured under **RESOURCES** > **Reports** is used. You can customize the report templates following the steps under Designing a Report Template.
11. Schedule the **Schedule Recurrence Pattern** for the report bundle to run once, hourly, daily, weekly, or monthly or set the range under **Schedule Recurrence Range**.
12. Specify the **Notification** that should be sent when the report bundle runs from the available options:
    - **Default Notifications** - to send default notifications. Click **+** to add more **Recipients**.
    - **Custom Notifications** - to send notifications to specific email addresses. Use the edit icon to add more **Recipients**.
    - **Copy to a remote directory** - to copy the report bundle to a remote directory.
13. Specify the Event/CMDB **Attribute**, **Operator**, and **Value**. Click **+** to add more, if required.

14. Click **OK**.
    The report bundle will run at the time you scheduled.

Scheduling Reports Using a Workflow

Follow these steps to schedule a report by using a workflow.

- Step 1 - Create Appropriate Roles for Users
- Step 2 - Map Users to Appropriate Roles
- Step 3 - Request the Report to be Scheduled
- Step 4 - Approve the Report Scheduling Request
- Step 5 - View the Report Scheduling Request Status

Step 1 - Create Appropriate Roles for Users

Complete these steps to create a role that will require report scheduling approval.

1. Go to **ADMIN > Settings > Role > Role Management**.
2. Click **New** to create a new role or edit an existing role by selecting a role from the table and clicking **Edit**.
3. Make sure the **Approver > Report Schedule** option is not checked.
4. Make sure the **Activation > Report Schedule** option is not checked.
5. Save the role definition.

Complete these steps to create a role that can approve report scheduling requests.

1. Go to **ADMIN > Settings > Role > Role Management**.
2. Click **New** to create a new role or edit an existing role by selecting a role from the table and clicking **Edit**.
3. Make sure the **Approver > Report Schedule** option is checked.
4. Make sure the **Activation > Report Schedule** option is not checked.
5. Save the role definition.

Step 2 - Map Users to Appropriate Roles

1. Go to **CMDB > Users**.
2. Select a user from the table and click **Edit**.
3. In the Edit User dialog box, select the **System Admin** option, and click the **Edit** icon.
4. Select the **Requestor** or **Approver** role as appropriate.

Step 3 - Request Report to be Scheduled

1. Go to **RESOURCES > Reports**.
2. Select a report, then select **More > Schedule**. The Create New Request dialog box opens.
3. If the role requires approval, select an approver from the **Approver** drop-down list.
4. Click **Submit**.
5. The approver will receive an email with a link to log back in to FortiSIEM and approve the request.

Step 4 - Approve the Report Scheduling Request

1. Login to FortiSIEM using a role that can approve a report being scheduled .
2. Click **Approval**. The table in the **TASKS** page lists pending requests.
3. To process the requests, scroll to the right-hand end of the row.
4. From the drop-down list, select **Approve** or **Reject**.
   - If you select **Approve**, the Approve Request dialog box opens. You can choose whether the request is valid **Until** or **For the date and time listed in the time stamp field**. You can click the time stamp field to choose a different date and time.
   - If you choose **Reject**, the Reject Request dialog box opens where you can enter a reason for the rejection.
5. If you choose **Approve**, the report will now be scheduled.

Step 5 - View Report Scheduling Request Status

Complete this step to see the status of your report schedule activation requests.

1. Login to FortiSIEM using the same account as in Step 3.
2. Click **Request**. The table in the **TASKS** page shows the status of requests.

Importing and Exporting Reports

Importing a Report

1. Go to **RESOURCES > Reports** and select the folder where you want to import the report.
2. Open the **More** drop-down list and select **Import**.
3. Click **Choose File** and browse to the report file to import.
4. Click **Import**.

Exporting a Report Definition

1. Go to **RESOURCES > Reports** and select the folder where you want to export a report definition.
2. Select a report definition in the main panel.
3. Open the **More** drop-down list and select **Export**.

Exporting Report Results

Complete these steps to export Reports in PDF, RTF, or CSV format:

1. Go to **RESOURCES** tab and select the report under **Reports** folder from the left panel.
2. Select the reports and click **Run** to view the results under **ANALYTICS** tab.
3. Go to **Actions** and select **Export Result**.
4. Optional - Enter any **User Notes** about this report.
5. Select the **Output Format** for the report as CSV, RTF or PDF.
6. Select the **Time Zone** for which the report is to be generated. If the devices are in a different Timezone from the Supervisor, then you can choose the time zone of the devices while configuring the PDF or RTF report.

7. Select the **Template** if PDF or RTF format is selected:
   - **Defined** - to use the default template defined for this report defined under **RESOURCES** > **Reports**.
   - **New** - to create a new custom report template for one-time use. The **Report Design** settings appear on choosing this option. Note that this template will not replace the template defined under **RESOURCES** > **Reports**. See Designing a Report Template for the steps to customize the report template.
8. Click **Generate** to create the report.
9. Click **View** to open and save the report.

Note: If Data Obfuscation is turned on for a FortiSIEM user:
- The value for that object marked for data obfuscation is obfuscated. For example, if IP is marked for data obfuscation, the IP address is obfuscated. In earlier versions of FortiSIEM, raw events were completely obfuscated.
- CSV Export feature is disabled.

Rules

FortiSIEM continuously monitors your IT infrastructure and provides information to analyze performance, availability, and security. There may also be situations in which you want to receive alerts when exceptional, suspicious, or potential failure conditions arise. You can accomplish this using rules that define the conditions to watch out for, and which trigger an incident when those conditions arise. You can configure a notification policy that will send email and SNMP alerts that the incident has occurred. FortiSIEM includes over 500 system-defined rules, which you can see in **RESOURCES > Rules**, but you can also create your own rules as described in the topics in this section.

Viewing Rules

FortiSIEM includes a large set of rules for Availability, Performance, Change, Security, and Beaconing groups in addition to the rules that you can define for your system.

Complete these steps to view all system and user-defined rules:

1. Go to **RESOURCES** > **Rules**.
2. Use the **System** drop-down menu of the Rules list pane to filter rules by Organization.
3. Select any rule in the Rules list to view related information in the lower pane.

   All rules have two information tabs:

Tabs	Description
Summary	This tab provides an overview of the rule logic, its status, and notification settings.
Test Results	If you are testing a rule, you can view the results here. **Note**: Active rules cannot be tested. You must deactivate a rule before testing.

Creating Rules

Creating a new rule involves defining the attributes of the incident that is triggered by the rule, as well as the triggering conditions and any exceptions or clear conditions. You can also create a rule by cloning an existing rule using the **Clone** button and editing it.

Note: Do not use certain keywords in sub-pattern names - `regexp`.

- Creating a Rule
- Defining Rule Conditions
- Defining the Incident Generated by a Rule
- Defining Rule Exceptions
- Defining Clear Conditions
- Defining an Incident Title

Creating a Rule

Complete these steps to create a rule:

1. Go to **RESOURCES** > **Rules**.
2. Select the group where you want to add the new rule.
3. Click **New** to create a new rule.

Settings	Guidelines
Step 1: General	

Settings	Guidelines
Rule Name	Enter a name for the new Rule.
Description	Enter a description of the new Rule.
Event Type	The name you enter in the Rule Type field is replicated in the Event Type field.
Remediation Note	Enter the **Remediation** script. Make sure that the Remediation script for your scenario is defined. Check the existing Remediation scripts under **ADMIN** > **Settings** > **General** > **Notification Policy** > **Action** column. If your device is not in the list, add the needed Remediation script.
Step 2: Define Conditions	
Conditions	Click **Condition** to create the rule conditions. See Defining Rule Conditions.
Step 3: Define Actions	
Severity	Select a **Severity** to associate with the incident triggered by the rule.
Category	Select the **Category** of incidents to be triggered by the rule.
Subcategory	Select the **Subcategory** from the available list based on the selected incident **Category**. To add custom subcategories, follow the steps under Setting Rule Subcategory.
Technique	Select any techniques from the available **Technique** list. You can choose to select zero, one, or multiple techniques. The Tactics row will update itself based on the techniques selected.
Action	Click the edit icon to define the incident (Incident Attributes and Triggered Attributes) that will be generated by this rule. You must have at least one incident defined before you can save your rule.
Exception	Click the edit icon to define any **Exceptions** for the rule. See Defining Rule Exceptions.
Tag	Click the drop-down list icon to view the tag list. If no tags appear, it means no tags have been created. From the drop-down list, select any tags you wish to associate with the rule. From Incidents View (by Time, by Device, by Incident), tags are displayed in the **Tag** column. See Tags for more information.
Update Status on Summary Dashboard	Add a check mark to the **Update Status on Summary Dashboard** checkbox to add this rule update in the Summary Dashboard, under the **DASHBOARD** tab.

Settings	Guidelines
Notification	Enter a **Notification** frequency for how often you want notifications to be sent when an incident is triggered by this rule.
Impacts	Select the **Impacts** of the incident triggered by this rule from the drop-down.
Watch List	Click the edit icon to add the rule you want to add to the watch list. **Note:** The Type that you set for the watch list must match the Incident Attribute Types for the rule. For example, if your watch list Type is IP, and the Incident Attribute Type for the rule is string, you will not be able to associate the watch list to the rule.
Clear	Click the edit icon to define any **Clear** conditions for the rule. See Defining Clear Conditions.

4. Click **Save**.
   Your new rule will be saved to the group you selected in an inactive state. Before you activate the rule, you should test it.

Defining Rule Conditions

Rule conditions define the event attributes and thresholds that will trigger an incident. Rule conditions are built from sub-patterns of event attribute filters and aggregation functions. You can specify more than one subpattern and the relationships and constraints between them.

Specifying a Subpattern

A subpattern defines the characteristics of events that will cause a rule to trigger an incident. A subpattern involves defining event attributes that will be monitored, and then defining the threshold values for aggregations of event attributes that will trigger an incident.

Event Filters

Event filter criteria determine which event attributes and values will be monitored by the rule, and are set in a way that is similar to the way you set event attributes for structured historical searches and real time searches.

Event Aggregation

While you could have a rule that triggers an incident on a single instance of a particular event, it is more likely that you will want your rule to trigger an incident when some number of events have been found that meet your event filter criteria.

Group By Attributes

This determines which event attributes will be used to group the events before the group constraints are applied, in a way that is similar to the way the Group By attribute is used to aggregate the results of structured searches.

Aggregate Conditions

The group aggregation conditions set the threshold at which some aggregation of events will trigger a rule to create an incident. You create an aggregation condition by using the **Expression Builder** to set a function, and then enter the

Operator and **Value** for the aggregation condition. Examples of Group By and Aggregate Conditions Settings are shown below:

Scenario	Group By Attributes	Aggregate Conditions
10 or more events	none	**COUNT(Matched events) >= 10**
Connections to 100 or more distinct destination IPs from the same source IP	**Source IP**	**COUNT (DISTINCT Destination IP) >= 100**
Connections to 100 or more distinct destination IPs from the same source IP on the same destination port	**Source IP,Destination Port**	**COUNT (DISTINCT destination IP) >= 100**
Average CPU Utilization on the same server > 95% over 3 samples	**Host IP**	**COUNT (Matched Events) >= 3 AND AVG(CPU Util) > 95**
Logins from the same source workstation to 5 or more accounts on the same target server	**Source IP**, **Destination IP**	**COUNT(DISTINCT user) >= 5**

Setting the Relationship between Subpatterns

If you have more than one sub-pattern, you must specify the relationship between them with these operators.

Operator	Meaning
AND	**Sub-pattern P1 AND Sub-pattern P2** means both sub-patterns P1 and P2 have to occur
OR	**Sub-pattern P1 OR Sub-pattern P2** means either P1 or P2 have to occur
FOLLOWED-BY	**Sub-pattern P1 FOLLOWED-BY Sub-pattern P2** means P1 has to be followed by P2 in time
AND-NOT	**Sub-pattern P1 AND-NOT Sub-pattern P2** means P1 must occur while P2 must not; the time order between P1 and P2 is not important
NOT-FOLLOWED-BY	**Sub-pattern P1 NOT-FOLLOWED-BY P2** means P1 must occur and P2 must not occur after P1

Setting Inter-subpattern Constraints

You may want to relate attributes of a sub-pattern to the corresponding attributes of another sub-pattern, in a way that is similar to a JOIN operation in an SQL, by using the relationship operators **<**, **>**, **<=**, **>=**, **=**, **!=**.

Examples of inter-subpattern relationships and constraints

Scenario	Sub-pattern P1 - filter	P1 - Group-by attribute set	P1 Group constraint	Sub-pattern P2 filter	P2-group-by attribute	P2 group constraint	Inter-P1-P2 relationships	Inter-P1-P2 constraints
5 login failures from the same source to a server not followed by a successful logon from the same source to the same server	Event type = Login Success	Source IP, Destination IP	COUNT (Matched Event) >= 5	Event type = Login failure	Source IP, Destination IP	COUNT (Matched Event) > 0	P1 NOT_FOLLOWED_BY P2	P1's Source IP = P2's Source IP
An security attack to a server followed by the server scanning the network, that is, attempting to communicate to 100 distinct destination IP addresses in 5 minute time windows	Event type = Attack	Destination IP	COUNT (Matched Event) > 0	Event Type = Connection Attempted	Source IP	COUNT (DISTINCT Destination IP) > 100	P1 FOLLOWED_BY P2	P1's Destination IP = P2's Source IP
Average CPU > 95% over	Event Type = CPU_	Host IP	COUNT (Matched Event)	Event Type = PING	Host IP	pingLossPct > 75	P1 AND P2	P1's Host IP = P2's Host IP

Scenario	Sub-pattern P1 - filter	P1 - Group-by attribute set	P1 Group constraint	Sub-pattern P2 filter	P2-group-by attribute	P2 group constraint	Inter-P1-P2 relationships	Inter-P1-P2 constraints
3 sample on a server AND Ping loss > 75%	Stat		>= 3 AND AVG (cpuUtil) > 95	Stat				

Defining the Incident Generated by a Rule

Defining an incident involves setting attributes for the incident based on the subpatterns you created as conditions for the rule, and then setting attributes for the incident that will be used in analytics and reports.

Note: You must have at least one incident defined before you can save your rule.

1. Select the rule you want to define an incident for.
2. Click **Edit** and go to **Step 2: Define Condition**.
3. Select a **Subpattern** from the drop-down list and click the edit icon to define the conditions for the rule. See Defining Rule Conditions.
   Define attributes for the incident based on the **Filter**, **Aggregate**, and **Group By** attributes you set for your subpatterns. Typically, you will set the Incident attributes to be the same as the Group By attributes in the subpattern:
   a. Select the **Attribute** you want to add to Incident.
   b. Select a **Subpattern**.
   c. This will populate values from the **Group By** attributes in the subpattern to the **Filter** menu.
   d. In the **Filter** menu, select the attribute you want to set as equivalent to the **Event Attribute**.
4. In **Step 3: Define Action**, provide values for the **Severity**, **Category**, **Subcategory**, **Dashboard**, **Notification**, **Impacts**, and **Watch List** fields as described in Creating a Rule. For information on exceptions, see Defining Rule Exceptions.
5. Click the **Action** edit icon to define the incident events and triggered attributes in the **Generate Incident for** dialog box. This dialog box is is pre-populated with typical attributes you would want included in an incident report.
6. Under **Triggered Attributes**, select the attributes from the triggering events that you want to include in Dashboards and Analytics for this event.
7. Click **Save**.

Defining Rule Exceptions

Once you activate a rule, it continuously monitors your IT infrastructure for conditions that would trigger an event. However, you may also want to define exceptions to those conditions. For example, you may know that a server will be going down for maintenance during a specific time period and you don't want your **Server Down - No Ping Response** rule to trigger an incident for it.

1. In **RESOURCES** > **Rules**, select the rule you want to add the exception to, and click **Edit**.
2. Select **Step 3: Define Action**.
3. Next to **Exceptions**, click **Edit**.
4. Select an **Attribute** and **Operator**, and enter a **Value**, for the conditions that will prevent an incident from being generated.
   The values in the Attribute menu are from the **Event Attributes** associated with the incident definition.
5. Click the **+** icon to set an effective time period for the exception.
   You can set effective time periods for single and recurring events, and for durations of time from hours to days.
6. Enter any **Notes** about the exception.
7. Click **Save**.

Defining Clear Conditions

Clear conditions specify conditions in which incidents will have their status changed from **Active** to **Cleared**. You can set the time period that must elapse for the clear condition to occur, and then set the conditions based on the triggering of the original rule, or on a sub pattern based on the Incident Attributes.

1. In **RESOURCES** > **Rules**, select the rule you want to add the clear condition to, and click **Edit**.
2. Select **Step 3: Define Action**.
3. Next to **Clear Condition**, click **Edit**.
4. Set the **Time Period** that should elapse for the clear condition to go into effect.
5. If you want the clear condition to go into effect based on the firing of the original rule, select t**he Original Rule Does Not Trigger**.
   For example, if you wanted the clear condition to change the status of **Active** incidents to **Cleared** after the original rule had not been triggered for ten minutes, you would set **Cleared Within** to **10 Minutes** and select this option.
6. If you want to base the clear condition on a sub-pattern of the incident attributes, select **the following conditions are met**.
   The incident attributes from your rule will load and the clear condition attributes will be set to match.
7. Define the pattern to use by clicking the **Edit** icon next to the clear sub pattern.
8. Click **Save**.

Defining an Incident Title

Defining an incident title makes it convenient to identify an incident without having to search on incident source, target, and details. You can define titles for both user-defined rules and system rules.

These steps assume you have already created a rule or are editing a system rule.

1. In **RESOURCES** > **Rules**, select the rule you want to add a title to, and click **Edit**.
2. Select **Step 3: Define Action**.
3. You can either enter text for the title or build the title using incident attributes defined for the rule.
   To use the incident attributes to build the title, follow these steps:

   a. Open the drop-down list next to **Insert Attribute**.
      Notice that the list contains all of the attributes defined in the **Incident Attributes** field.

   b. Select an attribute and click the **+** symbol to the right of the **Insert Attribute** list.
      The attribute appears in the **Incident Title** field prefixed by a "`$`" symbol, for example, `$user`.

   c. Repeat the previous step for all of the attributes you want to appear in the title.
   d. You can add text to the **Incident Title** field to make it more meaningful to you, for example: `$user` *created* `$fileName` *on* `$hostName`.
4. Click **Save** when you have finished your edits.

Once the title is defined in a rule definition, FortiSIEM will populate Incident **Title** field for all new instances of the Incidents.

To Display the Incident Title Field

Follow these steps to display the **Incident Title** column in the list of incidents table.

1. Go to **INCIDENTS > List by Time** view.
2. Open the **Actions** drop-down list and select **Change Display Columns**.
3. Select **Incident Title** from the list.
4. Click **Close**.

The **Incident Title** column appears in the incidents table.

Activating and Deactivating a Rule

- Activating a Rule Without a Workflow
- Activating a Rule Using a Workflow
- Activating/Deactivating Multiple Rules

Activating a Rule Without a Workflow

If you have permission to activate a rule, follow these steps: You may also want to deactivate a rule, for example to test it, instead of deleting it from the system.

1. Go to **RESOURCES** > **Rules**.
2. Browse or search to find the rule that you want to activate or deactivate.
3. Select **Active** in the Active column to activate the rule, or clear the **Active** option to deactivate the rule.

Activating a Rule Using a Workflow

Follow these steps to activate a rule by using a workflow.

- Step 1 - Create Appropriate Roles for Users
- Step 2 - Map Users to Appropriate Roles
- Step 3 - Rule to be Activated/Deactivated
- Step 4 - Approve the Rule Activation/Deactivation Request
- Step 5 - View the Rule Activation/Deactivation Request Status

Step 1 - Create Appropriate Roles for Users

Complete these steps to create a role that will require approval for rule activation/deactivation requests.

1. Go to **ADMIN > Settings > Role > Role Management**.
2. Click **New** to create a new role or edit an existing role by selecting a role from the table and clicking **Edit**.

3. Make sure the **Approver > Rule Activation/Deactivation** option is not checked.
4. Save the role definition.

Complete these steps to create a role that can approve rule activation/deactivation requests.

1. Go to **ADMIN > Settings > Role > Role Management**
2. Click **New** to create a new role or edit an existing role by selecting a role from the table and clicking **Edit**.
3. Make sure the **Approver > Rule Activation/Deactivation** option is checked.
4. Save the role definition.

Step 2 - Map Users to Appropriate Roles

1. Go to **CMDB > Users**.
2. Select a user from the table and click **Edit**.
3. In the Edit User dialog box, select the **System Admin** option, and click the **Edit** icon.
4. Select the **Requestor** or **Approver** role as appropriate.

Step 3 - Request Rule to be Activated/Deactivated

1. Go to **RESOURCES > Rules**.
2. Select a rule, then check or uncheck the active column status as needed. The Create New Request dialog box opens.
3. If the role requires approval, select an approver from the **Approver** drop-down list.
4. Click **Submit**.
5. The approver will receive an email with a link to log back in to FortiSIEM and approve the request.

Step 4 - Approve the Rule Activation/Deactivation Requests

1. Login to FortiSIEM using a role that can approve rule activation/deactivation requests.
2. Click **Approval**. The table in the **TASKS** page lists pending requests.
3. To process the requests, scroll to the right-hand end of the row.
4. From the drop-down list, select **Approve** or **Reject**.
   - If you select **Approve**, the Approve Request dialog box opens. You can choose whether the request is valid **Until** or **For the date and time listed in the time stamp field**. You can click the time stamp field to choose a different date and time.
   - If you choose **Reject**, the Reject Request dialog box opens where you can enter a reason for the rejection.
5. If you choose **Approve**, the rule will be enabled or disabled.

Step 5 - View the Rule Activation/Deactivation Request Status

Complete this step to see the status of your rule activation/deactivation requests.

1. Login to FortiSIEM using the same account as in Step 3.
2. Click **Request**. The table in the **TASKS** page shows the status of requests.

Activating/Deactivating Multiple Rules

If you have permission to activate a rule, follow these steps to activate/deactivate multiple rules with a single click.

1. Go to **RESOURCES** > **Rules**.
2. Click the Edit icon ( )and select **Multiple Rules**.
3. From the Edit Multiple Rules window, take the following steps:
   A. In the leftmost panel, expand Rules, and rule categories/sub-categories (Availability, Network, etc...) to locate your rule(s) in the middle panel.

   B. In the middle panel, select your rule(s) you wish to make activation/deactivation changes to. You can use Shift-Click to select a group of ascending or descending rules from your first selection. You can also use Ctrl-Click to individually select a group of rules.

   C. Click **>** to add the selected rule(s) for activation/deactivation.
   Note: You can also select a rule in the rightmost panel and click **<** to remove it from the group selection.

   D. When you are done selecting all the rules you wish to make an activation/deactivation change to, in the **Select Actions** panel, take any of the following actions:

   - Select a Severity from the **Severity** drop-down list to change for your selected rules.
   - Select/deselect Active Status for New Org, to make the selected rules active or inactive for new organizations by default.
   - From the **All Status for Existing Orgs** and specific org checkboxes, add a check to the checkbox to make the selected rules for that organization active, or remove the checkmark from a checkbox to make the selected rules inactive for that particular organization.
4. When done, click **Save**.

Testing a Rule

After creating or editing a rule, you should test it to see if it works as expected, before activating.

Note: You can perform rule testing only on the super global organization and not within the local organization.

Complete these steps to test a rule:

1. Go to **RESOURCES** > **Rules**, and deactivate the rule to test.
   Note: If you cannot deactivate a rule for testing, you can clone an inactive version of it.
2. In the **Set Activation Scope** dialog box, deselect the **Activation Status for New Org** and all of the organizations under **Activation Status for This Rule**.
3. Click **Save** to close the **Set Activation Scope** dialog box.
4. Select the rule, and click **Test**.
   This opens the **Rule Debug Events** dialog box.
5. Enter a **Reporting IP** where the synthetic event should originate from.
   If the rule you're testing specifies that the **Reporting IP** should be a member of a group, you should make sure that the Reporting IP you enter here is in that group.
6. Under **Raw Event**, enter the raw event log text that contains the triggering conditions for the rule.
7. Under **Pause**, enter the number of seconds before the next test event will be sent, and click **+** under **Action** to enter additional test events.
   Create as many events as necessary to trigger the rule conditions.
8. Click **Test Rule**.
   If the test succeeds you are now ready to activate the rule.

Exporting and Importing Rule Definitions

Instead of using the user interface to define a rule, you can import rule definitions, or you can export a definition, modify it, and import it back into your FortiSIEM virtual appliance. Rule definitions follow an XML schema.

- Exporting a Rule Definition
- Importing a Rule Definition

Exporting a Rule Definition

Complete these steps to export a Rule Definition:

1. Go to **RESOURCES** > **Rule**.
2. Select the Rule Definition(s) to export from the table.
3. Click **Export** to download and save the Rule Definition.

Importing a Rule Definition

Complete these steps to import a Rule Definition:

1. Go to **RESOURCES** > **Rule**.
2. Select the Rule Definition(s) to import in XML format.
3. Click **Import** to import the Rule Definition.

Networks

The Networks page lists the defined networks in your IT infrastructure.

Adding a Network

Complete these steps to add a network:

1. Go to **RESOURCES** > **Networks**.
2. Select a group where you want to add the Network group, or create a new one by clicking **+** above the **RESOURCES** groups.
3. Click **New**.
4. Enter the following information:
   - **Name** - name of the network
   - **Low** - lower IP address of the network IP range
   - **High** - higher IP address of the network IP range
   - **Mask** - Subnet mask
5. Click **Save**.

Modifying a Network

Complete these steps to modify a network:

1. Go to **RESOURCES** > **Networks**.
2. Select the network to modify from the table.
3. Click **Edit**.
4. Modify the required information:
   - **Name** - name of the network
   - **Low** - lower IP address of the network IP range
   - **High** - higher IP address of the network IP range
   - **Mask** - Subnet mask
5. Click **Save**.

Deleting a Network

Complete these steps to delete a network:

1. Go to **RESOURCES** > **Networks**.
2. Select the network to modify from the table.
3. Click **Delete**.
4. Click **Yes** to delete the network or **Remove only from group** to just remove the network from the group.

Watch Lists

A Watch List is a smart container of similar items such as host names, IP addresses, or user names, that are of significant interest to an administrator and must be watched. Examples of watch lists that are already set up in FortiSIEM are:

- **Frequent Account Lockouts** - users who are frequently locked out
- **Host Scanners** - IP addresses that scan other devices
- **Disk space issues** - hosts with disks that are running out of capacity
- **Denied countries** - countries with an excessive number of access denials at the firewall
- **Blacklisted WLAN endpoints** - Endpoints that have been blacklisted by Wireless IPS systems

Items are added to a watch list dynamically when a rule is triggered, but you can also add items to a watch list manually. When you define a rule, you can also choose a watch list that will be populated with a specific incident attribute, and you can use watch lists as conditions while creating reports, as described in Using a Watch List. You can also define when an entry leaves a watch list - this is time based. For example, if the rule does not trigger for that attribute for defined time-period, then the entry is removed from the watch list. Watch lists are also multi-tenant aware, with organization IDs tracked in relation to watch list items.

The following section provides the procedures to use Watch Lists:

System-defined Watch List

FortiSIEM includes several pre-defined watch lists that are populated by system-defined rules.

Watch list	Description	Attribute Type	Triggering Rules
Accounts Locked	Domain accounts that are locked out frequently	User (STRING)	Account Locked: Domain
Application Issues	Applications exhibiting issues	Host Name (STRING)	IIS Virtual Memory Critical SQL Server Low Buffer Cache Hit Ratio SQL Server Low Log Cache Hit Ratio SQL Server Excessive Deadlock SQL Server Excessive Page Read/Write SQL Server Low Free Pages In Buffer Pool SQL Server Excessive Blocking Database Server Disk Latency Critical SQL Server Excessive Full Scan SQL Server scheduled job failed High Oracle Table Scan Usage High Oracle Non-System Table Space Usage Oracle database not backed up for 1 day Exchange Server SMTP Queue High Exchange Server Mailbox Queue High Exchange Server RPC Request High Exchange Server RPC Latency High Oracle DB Low Buffer Cache Hit Ratio Oracle DB Low Library Cache Hit Ratio

Watch list	Description	Attribute Type	Triggering Rules
			Oracle DB Low Row Cache Hit Ratio Oracle DB Low Memory Sorts Ratio Oracle DB Alert Log Error Excessively Slow Oracle DB Query Excessively Slow SQL Server DB Query Excessively Slow MySQL DB Query
Availability Issues	Servers, networks or storage devices or Applications that are exhibiting availability issues	Host Name (STRING)	Network Device Degraded - Lossy Ping Response Network Device Down - No Ping Response Server Degraded - Lossy Ping Response Server Down - No Ping Response Server Network Interface Staying Down Network Device Interface Flapping Server Network Interface Flapping Important Process Staying Down Important Process Down Auto Service Stopped Critical network Interface Staying Down EC2 Instance Down Storage Port Down Oracle Database Instance Down Oracle Listener Port Down MySQL Database Instance Down SQL Server Instance Down Service Staying Down - Slow Response To STM Service Down - No Response to STM Service Staying Down - No Response to STM
DNS Violators	Sources that send excessive DNS traffic or send traffic to unauthorized DNS gateways	Source IP	Excessive End User DNS Queries to Unauthorized DNS servers Excessive End User DNS Queries Excessive Denied End User DNS Queries Excessive Malware Domain Name Queries Excessive uncommon DNS Queries Excessive Repeated DNS Queries To The Same Domain
Denied Countries	Countries that are seeing a	Destination Country	Excessive Denied Connections From An External Country

Watch list	Description	Attribute Type	Triggering Rules
	high volume of denials on the firewall	(STRING)	
Denied Ports	Ports that are seeing a high volume of denies on the firewall	Destination Port (INT)	Excessive Denied Connection To A Port
Environmental Issues	Environmental Devices that are exhibiting issues	Host name (String)	UPS Battery Metrics Critical UPS Battery Status Critical HVAC Temp High HVAC Temp Low HVAC Humidity High HVAC Humidity Low FPC Voltage THD High FPC Voltage THD Low FPC Current THD High FPC ground current high NetBoz Module Door Open NetBotz Camera Motion Detected Warning APC Trap Critical APC Trap
Hardware Issues	Servers, networks or storage devices that are exhibiting hardware issues	Host Name (String)	Network Device Hardware Warning Network Device Hardware Critical Server Hardware Warning Server Hardware Critical Storage Hardware Warning Storage Hardware Critical Warning NetApp Trap Critical Network Trap
Host Scanners	Hosts that scan other hosts	Source IP	Heavy Half-open TCP Host Scan Heavy Half-open TCP Host Scan On Fixed Port Heavy TCP Host Scan Heavy TCP Host Scan On Fixed Port Heavy UDP Host Scan

Watch list	Description	Attribute Type	Triggering Rules
			Heavy UDP Host Scan On Fixed Port Heavy ICMP Ping Sweep Multiple IPS Scans From The Same Src
Mail Violators	End nodes that send too much mail or send mail to unauthorized gateways		Excessive End User Mail to Unauthorized Gateways Excessive End User Mail
Malware Found	Hosts where malware found by Host IPS /AV based systems and the malware is not remediated	Host Name (String)	Virus found but not remediated Malware found but not remediated Phishing attack found but not remediated Rootkit found Adware process found
Malware Likely	Hosts that are likely to have malware - detected by network devices and the determination is not as certain as host based detection	Source IP or Destination IP	Excessive Denied Connections From Same Src Suspicious BotNet Like End host DNS Behavior Permitted Blacklisted Source Denied Blacklisted Source Permitted Blacklisted Destination Denied Blacklisted Destination Spam/malicious Mail Attachment found but not remediated Spyware found but not remediated DNS Traffic to Malware Domains Traffic to Emerging Threat Shadow server list Traffic to Emerging Threat RBN list Traffic to Emerging Threat Spamhaus list Traffic to Emerging Threat Dshield list Permitted traffic from Emerging Threat Shadow server list Permitted traffic from Emerging Threat RBN list Permitted traffic from Emerging Threat Spamhaus list Permitted traffic from Emerging Threat Dshield list

Watch list	Description	Attribute Type	Triggering Rules
Port Scanners	Hosts that scan ports on a machine	Source IP	Heavy Half-open TCP Port Scan: Single Destination Heavy Half-open TCP Port Scan: Multiple Destinations Heavy TCP Port Scan: Single Destination Heavy TCP Port Scan: Multiple Destinations Heavy UDP Port Scan: Single Destination Heavy UDP Port Scan: Multiple Destinations
Policy Violators	End nodes exhibiting behavior that is not acceptable in typical Corporate networks	Source IP	P2P Traffic detected IRC Traffic detected P2P Traffic consuming high network bandwidth Tunneled Traffic detected Inappropriate website access Inappropriate website access - multiple categories Inappropriate website access - high volume Inbound clear text password usage Outbound clear text password usage Remote desktop from Internet VNC From Internet Long lasting VPN session High throughput VPN session Outbound Traffic to Public DNS Servers
Resource Issues	Servers, networks or storage devices that are exhibiting resource issues: CPU, memory, disk space, disk I/O, network I/O, virtualization resources - either at the system level or application level	Host Name (STRING)	High Process CPU: Server High Process CPU: Network High Process Memory: Server High Process Memory: Network Server CPU Warning Server CPU Critical Network CPU Warning Network CPU Critical Server Memory Warning Server Memory Critical Network Memory Warning Network Memory Critical Server Swap Memory Critical Server Disk space Warning Server Disk space Critical Server Disk Latency Warning

Watch list	Description	Attribute Type	Triggering Rules
			Server Disk Latency Critical Server Intf Util Warning Server Intf Util Critical Network Intf Util Warning Network Intf Util Critical Network IPS Intf Util Warning Network IPS Intf Util Critical Network Intf Error Warning Network Intf Error Critical Server Intf Error Warning Server Intf Error Critical
			Virtual Machine CPU Warning Virtual Machine CPU Critical Virtual Machine Memory Swapping Warning Virtual Machine Memory Swapping Critical ESX CPU Warning ESX CPU Critical ESX Memory Warning ESX Memory Critical ESX Disk I/O Warning ESX Disk I/O Critical ESX Network I/O Warning ESX Network I/O Critical Storage CPU Warning Storage CPU Critical NFS Disk space Warning NFS Disk space Critical
			NetApp NFS Read/Write Latency Warning NetApp NFS Read/Write Latency Critical NetApp CIFS Read/Write Latency Warning NetApp CIFS Read/Write Latency Critical NetApp ISCSI Read/Write Latency Warning NetApp ISCSI Read/Write Latency Critical NetApp FCP Read/Write Latency Warning NetApp FCP Read/Write Latency Critical NetApp Volume Read/Write Latency Warning

Watch list	Description	Attribute Type	Triggering Rules
			NetApp Volume Read/Write Latency Critical EqualLogic Connection Read/Write Latency Warning EqualLogic Connection Read/Write Latency Critical Isilon Protocol Latency Warning
Routing Issues	Network devices exhibiting routing related issues	Host Name (STRING)	OSPF Neighbor Down EIGRP Neighbor down OSPF Neighbor Down
Scanned Hosts	Hosts that are scanned	Destination IP	Half-open TCP DDOS Attack TCP DDOS Attack Excessive Denied Connections to Same Destination
Vulnerable Systems	Systems that have high severity vulnerabilities from scanners	Host Name (STRING)	Scanner found severe vulnerability
Wireless LAN Issues	Wireless nodes triggering violations	MAC Address (String)	Rogue or Unsecure AP detected Wireless Host Blacklisted Excessive WLAN Exploits Excessive WLAN Exploits: Same Source

Creating a Watch List

Complete these steps to create a Watch List:

1. Go to **RESOURCES** > **Watch Lists**.
2. Select an existing group under **Watch Lists** folder or create a new Watch List group.

To create a new Watch List group:

a. Select **Watch Lists** folder from the left panel and click **+** above the **RESOURCES** groups.

b. In the **Create New Watch List** dialog box, select the **Organization** type.

c. Enter the information below:

- **Group** - name of the Watch List group
- **Description** - description about the Watch List group
- **Type** - Watch List type - String, Number, IP, or Date
- **Case Sensitive** - Select if the group name is case-sensitive
- **Expired in** - time period in which the items will expire from the watch if there is no activity for that time

To create a new Watch List:

a. Select a Watch List and click **New**.
In the **Add New Entry** dialog box, the **Watch List** and **Type** values are pre-populated based on the Watch List selection.

b. Enter the information below:
   - **Active** - select whether the Watch List will be active when it is created
   - **Value** - a value for the Watch List
   - **Description** - a description of the Watch List
   - **Expires** - time period in which the items will expire from the watch if there is no activity for that time

c. Click **Save**.

Modifying a Watch List

Complete these steps to modify a Watch List:

1. Go to **RESOURCES** > **Watch Lists**.
2. Select the Watch List to modify from the table.
3. Click **Edit** and make the required changes.
4. Click **Save**.

Use the **Delete** button to select and delete any Watch List(s) from the table.

Using a Watch List

- Adding Watch List to a Rule
- Using Watch Lists as Conditions in Rules and Reports

Adding Watch List to a Rule

You can now add your new watch list to a rule, so that when the rule is triggered, items will be added to the watch list.

1. Go to **RESOURCES** > **Rules**.
2. Select the rule where you want to add the watch list, and click **Edit**.
3. Go to the **Step 3: Define Action** page.
4. Click the edit icon for the **Watch List**.
5. For **Incident Attribute**, select the incident information you want to add to the watch list.
   Note: **Watch List Attribute Type Must Match Incident Attribute**- The Type that you set for the watch list must match the Incident Attribute Types for the rule. For example, if your watch list Type is IP, and the Incident Attribute Type for the rule is string, you will not be able to associate the watch list to the rule.
6. Move the watch list you want to add from **Available** to **Selected** list using the right arrow.
7. Click **Save**.
   The **Watch Lists** field value displays "Defined".

Using Watch Lists as Conditions in Rules and Reports

If you want to create a rule that refers to the attributes in a watch list, for example if you want to create a condition in which a **Source IP** listed in your **DNS Violators** watch list will trigger an incident.

1. Go to **RESOURCES** > **Reports** or **Rules** and select the rule or report where you want to use the watch list.
2. Click **Edit**.
3. Go to the **Step 2: Define Condition** page.
4. Under **Conditions** for the report in your rule sub-pattern, enter the watch list attribute you want to filter for in the **Attribute** field.
   For example, **Source IP**.
5. For **Operator**, select **IN**.
6. Click **... Select from CMDB** under **Value**, and browse the folders to select the watch list using the right arrow.
   For example, **DNS Violators**.
7. Click **OK** and continue creating your search criteria or rule sub pattern.

Exporting and Importing Watch Lists

- Exporting Watch Lists
- Importing Watch Lists

Exporting a Watch List

Complete these steps to export a Watch List:

1. Go to **RESOURCES** > **Watch Lists**.
2. Select the Watch List(s) to export from the table.
3. Click **Export**.
4. Select the file format as **PDF**, **RTF** or **CSV** and click **Generate**.
   "Export successful" message is displayed.
5. Click **Open Report File** to save the file.

Importing a Watch List

Complete these steps to import a Watch List:

1. Go to **RESOURCES** > **Watch Lists**.
2. Select the Watch List to modify from the table.
3. Click **Import**.
4. Select the file to import in CSV format and click **Import**.

Protocols

The Protocols page lists the protocols used by applications and devices to communicate with the FortiSIEM virtual appliance.

Adding a Protocol

Complete these steps to add a Protocol:

1. Go to **RESOURCES** > **Protocols**.
2. Select a group where you want to add the Network group, or create a new one by clicking **+** above the **RESOURCES** groups.
3. Click **New**.
4. Enter the following information:
   a. **Name** - name of the protocol.
   b. **Description** - description about the protocol.
   c. **Protocol/Port(s)** - select the Protocol and Port from the drop-down.
   d. **Apps Group** - enter the group to associate with the Protocol.
5. Click **Save**.

Modifying a Protocol

Complete these steps to modify a Protocol:

1. Go to **RESOURCES** > **Protocols**.
2. Select the protocol to modify from the table.
3. Click **Edit**.
4. Modify the required information:
   - **Name** - name of the protocol.
   - **Description** - description about the protocol.
   - **Protocol/Port(s)** - protocol and port from the drop-down.
   - **Apps Group** - group to associate with the protocol.
5. Click **Save**.

Deleting a Protocol

Complete these steps to delete a Protocol:

1. Go to **RESOURCES** > **Protocols**.
2. Select the Protocol to delete from the table.
3. Click **Delete**.
4. Click **Yes** to confirm.

Event Types

The Event Types page lists the types of events that are collected for supported devices.

Adding an Event Type

Complete these steps to add an event type:

1. Go to **RESOURCES** > **Event Types**.
2. Select a group to add the new event to, or create a new one.
3. Click **New**.
4. Enter a **Name**, and **Description** for the event type.
5. Select the **Device Type** from the drop-down list to associate with this event type.
6. Select the level of **Severity** associated with this event type.
7. For **CVE IDs**, enter links to any vulnerabilities associated with this event type as cataloged by the National Vulnerability Database.
8. Click **Save**.

Modifying an Event Type

Complete these steps to modify an Event Type:

1. Go to **RESOURCES** > **Event Types**.
2. Select the Event Type to modify from the table.
3. Click **Edit** to modify any settings.
4. Click **Save**.

Deleting an Event Type

Complete these steps to delete an Event Type:

1. Go to **RESOURCES** > **Event Types**.
2. Select the Event Type group from the folder structure on the left panel.
3. Select the Event Type from the table and click **Delete** to delete.
4. Confirm whether to **Remove only from group** or to remove completely by clicking **Yes**.

Working with AlienVault OTX

This section describes how to configure FortiSIEM to work with AlienVault OTX malware domains, IPs, URLs, and hashes.

- Working with AlienVault OTX Malware Domains
- Working with AlienVault OTX Malware IPs
- Working with AlienVault OTX Malware URLs
- Working with AlienVault OTX Malware Hash

Working with AlienVault OTX Malware Domains

- Enabling the AlienVault OTX Service
- Disabling the AlienVault OTX Service
- AlienVault OTX Malware Domain Values

Enabling the AlienVault OTX Service

To start the AlienVault OTX service, follow these steps once you have defined the feeds:

1. Go to **RESOURCES > Malware Domains>** select the OTX service you defined.
2. Click **More > Update**. In the **Update AlienVault OTX Service** dialog box, select **Enable AlienVault OTX Service**.
3. (Optional) Schedule the starting of the service. See Specifying a schedule.
4. Click **Save**.

Disabling the AlienVault OTX Service

To stop the AlienVault OTX service, follow these steps:

1. Go to **RESOURCES > Malware Domains** and select the **AlienVault OTX Malware Domain** folder.
2. Click **More > Update**.
3. Disable any schedule you have defined.
4. Click **Save**.

AlienVault OTX Malware Domain Values

Use the following values to configure AlienVault OTX Malware Domains for FortiSIEM.

Parameter	Value
URL	https://otx.alienvault.com
Username	<user> It will prompt you to enter your API user name.
Password	<pwd> It will prompt you to enter your API password.
Plugin Class	com.accelops.service.threatfeed.impl.OTXMalwareDomainUpdateService
Data Format	Select STIX/TAXII Format
Collection	user_AlienVault
Data Update	Select Full

Working with AlienVault OTX Malware IPs

For AlienVault OTX Malware IPs, go to **RESOURCES > Malware IPs,** select the **AlienVault OTX Malware IP** folder, and repeat the same steps as for **AlienVault OTX Malware Domains**.

Use the following values to configure AlienVault OTX Malware IPs for FortiSIEM.

Parameter	Value
URL	https://otx.alienvault.com
Username	<user> It will prompt you to enter your API user name.
Password	<pwd> It will prompt you to enter your API password.
Plugin Class	com.accelops.service.threatfeed.impl.OTXMalwareIPUpdateService
Data Format	Select STIX/TAXII Format
Collection	user_AlienVault
Data Update	Select Full

Working with AlienVault OTX Malware URLs

For AlienVault OTX Malware URLs, go to **RESOURCES > Malware URLs,** select the **AlienVault OTX Malware URL** folder, and repeat the same steps as for **AlienVault OTX Malware Domains**.

Use the following values to configure AlienVault OTX Malware URLs for FortiSIEM.

Parameter	Value
URL	https://otx.alienvault.com
Username	<user> It will prompt you to enter your API user name.
Password	<pwd> It will prompt you to enter your API password.
Plugin Class	com.accelops.service.threatfeed.impl.OTXMalwareUrlUpdateService
Data Format	Select STIX/TAXII Format
Collection	user_AlienVault
Data Update	Select Full

Working with AlienVault OTX Malware Hash

For AlienVault OTX Malware Hash, go to **RESOURCES > Malware Hash,** select the **AlienVault OTX Malware Hash** folder, and repeat the same steps as for **AlienVault OTX Malware Domains**.

Use the following values to configure AlienVault OTX Malware Hash for FortiSIEM.

Parameter	Value
URL	https://otx.alienvault.com
Username	<user> It will prompt you to enter your API user name.
Password	<pwd> It will prompt you to enter your API password.
Plugin Class	com.accelops.service.threatfeed.impl.OTXMalwareHashUpdateService
Data Format	Select STIX/TAXII Format
Collection	user_AlienVault
Data Update	Select Full

Working with Dragos IOCs

The following sections describe how to work with Dragos Worldview malware malware domains, IPs, and hashes.

- Download Dragos Worldview Malware Domains
- Download Dragos Worldview Malware IPs
- Download Dragos Worldview Malware Hashes

Download Dragos Worldview Malware Domains

1. Go to **RESOURCES > Malware Domains** and select the **Dragos Worldview Malware Domain** folder.
2. Click **More > Update**. In the **Update Malware** dialog box, then select **Update via API**.
3. Use your Dragos credentials to complete the **URL**, **API Token**, and **API Secret** fields.
4. **Plugin Class** is provided by default.
5. Select a **Data Format**. In this release, only **Custom** is supported.
6. Select a **Data Update** process. Selecting Full means FortiSIEM will download all data. If Incremental is selected, FortiSIEM will download from the latest recorded update date.
7. Click **Save**.
8. Schedule the download. See Specifying a Schedule.
9. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed.

Download Dragos Worldview Malware IPs

1. Go to **RESOURCES > Malware IPs**, select the **Dragos Worldview Malware IP** folder.
2. Click **More > Update**. In the **Update Malware** dialog box, then select **Update via API**.
3. Use your Dragos credentials to complete the **URL**, **API Token**, and **API Secret** fields.
4. **Plugin Class** is provided by default.
5. Select a **Data Format**. In this release, only **Custom** is supported.
6. Select a **Data Update** process. Selecting Full means FortiSIEM will download all data. If Incremental is selected, FortiSIEM will download from the latest recorded update date.
7. Click **Save**.
8. Schedule the download. See Specifying a Schedule.
9. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed.

Download Dragos Worldview Malware Hashes

1. For Dragos Worldview hash, go to **RESOURCES > Malware Hash** , select the **Dragos Worldview Malware Hash** folder.
2. Click **More > Update**. In the **Update Malware** dialog box, then select **Update via API**.
3. Use your Dragos credentials to complete the **URL**, **API Token**, and **API Secret** fields.
4. **Plugin Class** is provided by default.
5. Select a **Data Format**. In this release, only **Custom** is supported.
6. Select a **Data Update** process. Selecting Full means FortiSIEM will download all data. If Incremental is selected, FortiSIEM will download from the latest recorded update date.
7. Click **Save**.
8. Schedule the download. See Specifying a Schedule.
9. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed.

Specifying a Schedule

1. Click the **+** icon next to **Schedule**.
2. Enter values for the following options:
   - **Time Range** specifies start time (within the day) and the duration of the scheduling window. Select a UTC time and a corresponding location from the drop-down lists.
   - **Recurrence Pattern** specifies if and how the window will repeat.
     - If you are scheduling for one time only:
       a. Select **Once** for **Recurrence Pattern**.
       b. Select the specific date in **Start From**.
     - If you are scheduling for hourly:
       a. Enter the hourly interval.
       b. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.

- If you are scheduling for **Daily**:
    a. Select the interval of days or **Every weekday**.
    b. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.
- If you are scheduling for **Weekly**:
    a. Select the interval of weeks or select particular days of the week.
    b. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.
- If you are scheduling for **Monthly**:
    a. Select the days and months from the drop-down lists.
    b. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.

3. Click **Save** to apply the changes.

Working with FortiGuard IOCs

The following sections describe how to work with FortiGuard malware domains, IPs, and URLs.

- Working with FortiGuard Malware Domains
- Working with FortiGuard Malware IPs
- Working with FortiGuard Malware URLs
- Internet Connectivity Requirements

Working with FortiGuard Malware Domains

The following sections describe how to enable, disable, and setup a proxy for the FortiGuard Malware domain.

- Enabling the FortiGuard IOC Service
- Disabling the FortiGuard IOC Service
- Using a Proxy for the FortiGuard IOC Service

Enabling the FortiGuard IOC Service

To start the FortiGuard IOC service, follow these steps:

1. Go to **RESOURCES > Malware Domains** and select the **FortiGuard Malware Domain** folder.
2. Select an inactive domain from the table.
3. Click **More > Update**. In the **Update FortiGuard IOC Service** dialog box, select **Enable IOC Service**.
4. (Optional) Schedule the starting of the service. See Specifying a schedule.
5. Click **Save**.

Disabling the FortiGuard IOC Service

To stop the FortiGuard IOC service, follow these steps:

1. Go to **RESOURCES > Malware Domains** and select the **FortiGuard Malware Domain** folder.
2. Select an active domain from the table.

3. Click **More > Update**. In the **Update FortiGuard IOC Service** dialog box, select **Disable IOC Service**.
4. Click **Save**.

Using a Proxy for the FortiGuard IOC Service

Follow these steps to use a proxy for the FortiGuard IOC service:

1. Go to **RESOURCES > Malware Domains** and select the **FortiGuard Malware Domain** folder.
2. Select a domain from the table.
3. Click **More > Update**. In the **Update FortiGuard IOC Service** dialog box, select **Use Proxy**.
4. The **Mode** will be **Proxy**. Provide the following information:
    a. **IP/Host**
    b. **Port**
    c. **User Name**
    d. **Password**
5. Click **Save**.

Working with FortiGuard Malware IPs

For FortiGuard Malware IPs, go to **RESOURCES > Malware IPs**, select the **FortiGuard Malware IP** folder, and repeat the same steps as for **FortiGuard Malware Domains**.

Working with FortiGuard Malware URLs

For FortiGuard Malware URLs, go to **RESOURCES > Malware URLs**, select the **FortiGuard Malware URL** folder, and repeat the same steps as for **FortiGuard Malware Domains**.

Working with Malware Patrol

The following section describes how to configure Malware Patrol with FortiSIEM for Malware Domains, Malware IPs, Malware Hashes, and Malware URLs. Additional information is available on the Malware Patrol website https://www.malwarepatrol.net/tech-support/.

- Configuring Malware Patrol Malware Domains
- Configuring Malware Patrol Malware IPs
- Configuring Malware Patrol Malware Hashes
- Configuring Malware Patrol Malware URLs

Configuring Malware Patrol Malware Domains

To configure Malware Patrol Malware Domains, take the following steps.

1. Login to FortiSIEM GUI.
2. Navigate to **RESOURCES > Malware Domains**.
3. In the left pane, click the **+** icon and create a group named “Malware Patrol”.

4. Select the **Malware Patrol** folder you just created.
5. Click **More > Update**. In the **Update Malware** dialog box, select **Update via API**.
6. In the **URL** row, click the Edit icon.
7. In the **URL** field, enter the URL of the threat feed as provided via the Malware Patrol portal.
8. In the **Username** field, enter your Malware Patrol username.
9. In the **Password** field, enter the password associated with your Malware Patrol username.
10. In the **Plugin Class** field, enter:

    ```
    com.accelops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService
    ```

11. For **Field Separator**, enter a comma, by inputting the "," character.
12. For **Data Format**, select **CSV**.

    Note: Currently, only CSV is supported.

13. Select a **Data Update** process. Selecting **Full** means FortiSIEM will download all data. If **Incremental** is selected, FortiSIEM will download from the latest recorded update date.
14. For **Data Mapping**, add your Mapped fields. The following is an example.
    - Domain Name, set to Position 1.
    - Malware Type, set to Position 2.
    - Description, set to Position 3.
    - Date Found, set to Position 4.
    - Last Seen, set to Position 5.
15. Click **Save**.
16. Schedule the download. See Specifying a Schedule.
17. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed.

Configuring Malware Patrol Malware IPs

To configure Malware Patrol Malware IPs, take the following steps.

1. Login to FortiSIEM GUI.
2. Navigate to **RESOURCES > Malware IPs**.
3. In the left pane, click the **+** icon and create a group name “Malware Patrol”.
4. Click **Save**.
5. Select the **Malware Patrol** folder you just created.
6. Click **More > Update**. In the **Update Malware IP** dialog box, select **Update via API**.
7. In the **URL** row, click the Edit icon.
8. In the **URL** field, enter the URL of the threat feed as provided via the Malware Patrol portal.

9. In the **Username** field, enter your Malware Patrol username.
10. In the **Password** field, enter the password associated with your Malware Patrol username.
11. In the **Plugin Class** field, enter:

    `com.accelops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService`
12. For **Field Separator**, enter a comma, by inputting the "," character.
13. For **Data Format**, select **CSV**.

    Note: Currently, only CSV is supported.
14. Select a **Data Update** process. Selecting **Full** means FortiSIEM will download all data. If **Incremental** is selected, FortiSIEM will download from the latest recorded update date.
15. For **Data Mapping**, add your Mapped fields. The following is an example.
    - Name, set to Position 1.
    - Low IP , set to Position 2.
    - High IP, set to Position 3.
    - Malware Type, set to Position 4.
    - Description, set to Position 5.
    - Date Found, set to Position 6.
    - Last Seen, set to Position 7.
16. Click **Save**.
17. Schedule the download. See Specifying a Schedule.
18. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed.

Configuring Malware Patrol Malware Hashes

To configure Malware Patrol Malware Hashes, take the following steps.

1. Login to FortiSIEM GUI.
2. Navigate to **RESOURCES > Malware Hash**.
3. In the left pane, click the **+** icon and create a group name “Malware Patrol”.
4. Click **Save**.
5. Select the **Malware Patrol** folder you just created.
6. Click **More > Update**. In the **Update Malware Hash** dialog box, select **Update via API**.
7. In the **URL** row, click the Edit icon.
8. In the **URL** field, enter the URL of the threat feed as provided via the Malware Patrol portal.
9. In the **Username** field, enter your Malware Patrol username.
10. In the **Password** field, enter the password associated with your Malware Patrol username.

11. In the **Plugin Class** field, enter:

    `com.accelops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService`

12. For **Field Separator**, enter a comma, by inputting the "," character.
13. For **Data Format**, select **CSV**.

    Note: Currently, only CSV is supported.

14. Select a **Data Update** process. Selecting **Full** means FortiSIEM will download all data. If **Incremental** is selected, FortiSIEM will download from the latest recorded update date.
15. For **Data Mapping**, add your Mapped fields. The following is an example.
    - Description, set to Position 1.
    - Algorithm, set to Position 2.
    - HashCode, set to Position 3.
    - Malware Type, set to Position 4.
    - Date Found, set to Position 5.
    - Last Seen, set to Position 6.
16. Click **Save**.
17. Schedule the download. See Specifying a Schedule.
18. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed.

Configuring Malware Patrol Malware URLs

To configure Malware Patrol Malware URLs, take the following steps.

1. Login to FortiSIEM GUI.
2. Navigate to **RESOURCES > Malware URLs**.
3. In the left pane, click the **+** icon and create a group name “Malware Patrol”.
4. Click **Save**.
5. Select the **Malware Patrol** folder you just created.
6. Click **More > Update**. In the **Update Malware Url** dialog box, select **Update via API**.
7. In the **URL** row, click the Edit icon.
8. In the **URL** field, enter the URL of the threat feed as provided via the Malware Patrol portal.
9. In the **Username** field, enter your Malware Patrol username.
10. In the **Password** field, enter the password associated with your Malware Patrol username.
11. In the **Plugin Class** field, enter:

    `com.accelops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService`

12. For **Field Separator**, enter a comma, by inputting the "," character.

13. For **Data Format**, select **CSV**.

    Note: Currently, only CSV is supported.

14. Select a **Data Update** process. Selecting **Full** means FortiSIEM will download all data. If **Incremental** is selected, FortiSIEM will download from the latest recorded update date.
15. For **Data Mapping**, add your Mapped fields. The following is an example.
    - URL, set to Position 1.
    - Malware Type, set to Position 2.
    - Last Seen, set to Position 3.
16. Click **Save**.
17. Schedule the download. See Specifying a Schedule.
18. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed.

Working with ThreatConnect IOCs

ThreatConnect can provide malware IPs, domains, hashes, or URLs which FortiSIEM can use to match in log data The steps are as follows: for each IOC (IP, domain, hash, URL).

1. Discover Collections
2. Create Collection Policy
3. Schedule IOC Download

Since an Organization may subscribe to many Collections (an intelligence source), downloading every IOC for all Collections may result in too much data. Therefore, specifying a Collection Policy is essential.

Download ThreatConnect Malware Domains

1. Go to **RESOURCES > Malware Domains** and select the **ThreatConnect Malware Domain** folder.
2. Click **More > Update**. In the **Update Malware** dialog box, then select **Update via API**.
3. Use your ThreatConnect credentials to complete the **URL**, **User name**, and **Password** fields.
4. **Plugin Class** is provided by default.
5. Select a **Data Format**. In this release, only **STIX-TAXII** is supported.
6. Enter an **Organization** name that is defined in your ThreatConnect account.
7. Define a **Collection**.
8. Click **Discover Collections** to expose all of the collections you are eligible to use.
9. Select a collection policy in the table and click **Edit**.
10. Edit any of the following values in the **Edit Collection Policy** dialog box:
    - **Enabled**: select whether the collection policy is enabled
    - **Collection**: edit the collection name
    - **Tag**: enter an optional user-defined tag for the collection
    - **Max False Positive Count**: enter a number where the frequency of an attack produces a false positive on your network.

   - **Min Rating**: enter a value between 0 and 5.
   - **Confidence**: enter a value between 1 and 100.
11. Click **Save**.
12. Schedule the download. See Specifying a Schedule.
13. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed – organized by each collection.

Note that FortiSIEM does not provide system rules and reports because ThreatConnect folders are dynamic. The user must create them using the Collection folders.

Download Other ThreatConnect IOCs

For ThreatConnect Malware IP, go to **RESOURCES > Malware IPs**, select the **ThreatConnect Malware IP** folder, and repeat the same steps as for **Malware Domains**.

For ThreatConnect Malware URL, go to **RESOURCES > Malware URLs**, select the **ThreatConnect Malware URL** folder, and repeat the same steps as for **Malware Domains**.

For ThreatConnect Malware hash, go to **RESOURCES > Malware Hash** , select the **ThreatConnect Malware Hash** folder and repeat the same steps as for **Malware Domains**.

Specifying a Schedule

1. Click the **+** icon next to **Schedule**.
2. Enter values for the following options:
   - **Time Range** specifies start time (within the day) and the duration of the scheduling window. Select a UTC time and a corresponding location from the drop-down lists.
   - **Recurrence Pattern** specifies if and how the window will repeat.
     - If you are scheduling for one time only:
       a. Select **Once** for **Recurrence Pattern**.
       b. Select the specific date in **Start From**.
     - If you are scheduling for hourly:
       a. Enter the hourly interval.
       b. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.
     - If you are scheduling for **Daily**:
       a. Select the interval of days or **Every weekday**.
       b. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.
     - If you are scheduling for **Weekly**:
       a. Select the interval of weeks or select particular days of the week.
       b. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.
     - If you are scheduling for **Monthly**:
       a. Select the days and months from the drop-down lists.
       b. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.
3. Click **Save** to apply the changes.

Malware Domains

The Malware Domains page lists domains that are known to generate spam, host botnets, create DDoS attacks, and generally contain malware. Since Malware Domains are constantly changing, FortiSIEM recommends maintaining a dynamically generated list of IP addresses provided by services that are updated on a regular schedule, but you can also add or remove blocked IP addresses from these system-defined groups, and create your own groups based on manual entry of IP addresses or file upload.

The following sections describe Malware Domains:

Adding a Malware Domain

Complete these steps to add a Malware domain:

1. Go to **RESOURCES** > **Malware Domains**.
2. Select a group where you want to add the Malware Domains, or create a new one by clicking **+** above the **RESOURCES** groups. To create a new Malware Domain group:
   a. Select Malware Domain folder and click **+** above the **RESOURCES** groups.
   b. Enter the **Group** name and **Description** of the Malware Domain.
3. Select the Malware Domain group (existing or new) and click **New**.
4. Select the **Domain Name** and **Description** of the Malware domain.
5. Click **Save**.

To configure a ThreatConnect Malware Domain, see Working with ThreatConnect IOCs.

To configure a FortiGuard Malware Domain, see Working with FortiGuard Malware Domains.

Modifying a Malware Domain

Complete these steps to edit a Malware Domain:

1. Go to **RESOURCES** > **Malware Domains**.
2. Select the Malware Domain group on the left panel.
3. Select the Malware Domain from the table and click **Edit** to modify the settings.
4. Click **Save**.

To configure a ThreatConnect Malware Domain, see Working with ThreatConnect IOCs.

To configure a FortiGuard Malware Domain, see Working with FortiGuard Malware Domains.

Deleting a Malware Domain

Complete these steps to delete a Malware Domain:

1. Go to **RESOURCES** > **Malware Domains**.
2. Select the Malware Domain on the left panel.
3. Select the Malware Domain from the table and click **Delete**.
4. Click **Yes**.

Importing Malware Domains

You can import Malware Domain information into FortiSIEM from external threat feed websites.

- Custom Threat Feed Websites - CSV Data - One-time Manual Import
- Custom Threat Feed Websites - CSV Data - Programmatic Import via Java
- Custom Threat Feed Websites - Programmatic Import via Python
- Working with Custom Threat Feeds that use HTTPS Connectivity

Custom Threat Feed Websites - CSV Data - One-time Manual Import

This requires that the data to be imported is already in a file in comma-separated value (CSV) format.

Requirements for Importing

1. The CSV file columns must be in the following order:

   ```
   Name, IP Address, Reverse Lookup, Malware  Type, Confidence, Severity, ASN, Ori-
   gin, Country, Description, Date Found (MM/DD/YYYY), Last Seen(MM/DD/YYYY)
   ```

   If the fields are not in this order, then the whole file will not be imported.

2. The `Name` field is required and must be unique. If two or more `Name` fields are identical, the latter ones will not be imported.

   Example Name Field: mydomain.local

1. Select **RESOURCES > Malware Domains**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware Domain Group** dialog box.
3. In the **Group** field, enter a Group name.
4. In the **Description** field, enter a description.
5. Click **Save** to create the folder under **Malware Domains**.
6. Select the folder just created.
7. Select **More > Update**.
8. Click **Choose File**.
9. Browse to the CSV file you want to import and select it.
10. Leave **Data Update** as **Full** (Completely replace all data) or **Incremental** (add on to existing data).
11. Click **Import**.

Custom Threat Feed Websites - CSV Data - Programmatic Import via Java

Requirements for Importing

1. The Web Site Data requires the following:

   a. A file in comma-separated value format (separator can be any special character such as space, tab, hash, dollar etc.).

   b. An individual entry is in one line.

2. The `Name` field is required and must be unique. The Malware domain import will fill this group with only unique

values within the name field.

Example Name Field: mydomain.local

Follow these steps:

1. Select **RESOURCES > Malware Domains**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware Domain Group** dialog box.
3. In the **Group** field, enter a Group name.
4. In the **Description** field, enter a Description.
5. Click **Save** to create the folder under **Malware Domains**.
6. Select the folder just created.
7. Select **More > Update**.
8. From the Update Malware Domain dialog box, select **Update via API**.
9. Click the edit icon next to **URL** and provide the following information:
   a. In the **URL** field, enter the URL of the website.
   Note: Include the "http://" or "https://" prefix.
   b. (optional) In the **User Name** field, enter the username used by the API.
   c. (optional) In the **Password** field, enter the password related to the username.
   d. For **Plugin Type**, select **Java**.
   e. For **Plugin Class**, the default class **com.ac-cel-ops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService** is displayed.
   Note: Do not modify this in any case.
   f. Enter the correct **Field Separator** (by default, it is a comma).
   g. Select **CSV** as the **Data Format**.
   h. Enter the **Data Mapping** by choosing the mapped field and the corresponding position in the website data. For example, if the Domain Name is in third position, then choose 3 in the **Position** column.
   i. Enter the **Data Update** as **Full** (Completely replace all data) or **Incremental** (add on to existing data).
10. Click **Save**.
11. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.
    The imported data will show on the right pane after some time.

Custom Threat Feed Websites - Programmatic Import via Python

Follow these steps:

1. Select **RESOURCES > Malware Domains**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware Domain Group** dialog box.
3. In the **Group** field, enter a Group name.
4. In the **Description** field, enter a Description.
5. Click **Save** to create the folder under **Malware Domains**.
6. Select the folder just created.
7. Select **More > Update**.
8. From the Update Malware Domain dialog box, select **Update via API**.

9. Click the edit icon next to **URL** and provide the following information:
    a. In the **URL** field, enter the URL of the website.
    Note: Include the "http://" or "https://" prefix.
    b. (optional) In the **User Name** field, enter the username used by the API.
    c. (optional) In the **Password** field, enter the password related to the username.
    d. For **Plugin Type**, select **Python**.
    e. From the **Plugin Class** drop-down list, select the python script to use. Python scripts located under `/opt/phoenix/data-definition/threatfeedIntegrations/` will be available.
    Note: For more information on creating/using a Python script, see Appendix: Python Threat Feed Framework.
    f. For **Data Update**, select **Full** (Completely replace all data) or **Incremental** (add on to existing data).
10. Click **Save**.
11. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.
    The imported data will show on the right pane after some time.

Viewing Malware Domains

The Malware Domains Integration Status page shows all your existing Malware Domain feeds. See the following table for more information.

Navigate to **RESOURCES**, and select **Malware Domains** to view the Malware Domains Integration Status page.

Column	Description
Status	Displays the current status of the Malware Domain listed in the Feed column.
Feed	Displays Malware Domain group and its threat feed URL, if the information is available.
Indicators	Shows the current and prior threat feed objects for the Malware Domain group to easier identify the change that occurred.
Last Updated	Displays the last time the threat feed was updated.
Pulling Schedule	Displays the scheduled time, when the threat feed update occurs.
Integration Type	Displays how the threat feed information is gathered, MANUAL or API.
Action	The Action columns allows you to perform one of three actions: • **View Content** - Click to view the existing Malware Domain threat feed objects. • **Update** - Click to update the Malware Domain threat feed.

Working with Custom Threat Feeds that use HTTPS Connectivity

When integrating with a Custom Threat Feed that provides IoC over an HTTPS connection, for example a STIX/TAXII feed, or connecting to a web server hosting a CSV file, the web server Certificate must be imported into FortiSIEM key store. Please follow the steps here from the Configuring CA Certificates Guide to import the certificate into the key store.

Malware IPs

The Malware IP Addresses page lists IP addresses that are known to generate spam, host botnets, create DDoS attacks, and generally contain malware. The default group included in your FortiSIEM deployment, Emerging Threat, contains IP addresses that are derived from the website rules.emergingthreats.net. Because malware IP addresses are constantly changing, FortiSIEM recommends maintaining a dynamically generated list of IP addresses provided by services such as Emerging Threat that are updated on a regular schedule, but you can also add or remove blocked IP addresses from these system-defined groups, and create your own groups based on manual entry of IP addresses or file upload.

The following sections describe Malware IPs:

Adding a Malware IP

Complete these steps to add a Malware IPs:

1. Go to **RESOURCES** > **Malware IPs**.
2. Select a group where you want to add the Malware IPs, or create a new one by clicking **+** above the **RESOURCES** groups.
3. Click **New**.

4. Enter the details of the Malware IP.
5. Click **Save**.

To configure a ThreatConnect Malware IP, see Working with ThreatConnect.

To configure a FortiGuard Malware IP, see Working with FortiGuard Malware IPs.

Modifying a Malware IP

Complete these steps to edit a Malware IP:

1. Go to **RESOURCES** > **Malware IPs**.
2. Select the Malware IP group in the left panel.
3. Select the Malware IP from the table and click **Edit** to modify the settings.
4. Click **Save**.

To configure a ThreatConnect Malware IP, see Working with ThreatConnect IOCs.

To configure a FortiGuard Malware IP, see Working with FortiGuard Malware IPs.

You can use the **Delete** button to select and remove any Malware IP from the list.

Deleting a Malware IP

Complete these steps to delete a Malware IP:

1. Go to **RESOURCES** > **Malware IPs**.
2. Select the Malware IP group from the folder structure on the left panel.
3. Select the Malware IP from the table and click **Delete** to delete.
4. Click **Yes** to confirm.

Importing Malware IPs

You can import Malware IP information into FortiSIEM from external threat feed websites.

- Prerequisites
- Websites with Built-in Support
- Custom Threat Feed Websites - CSV Data - One-time Manual Import
- Custom Threat Feed Websites - CSV Data - Programmatic Import via Java
- Custom Threat Feed Websites - Non-CSV Data - Programmatic Import via Java
- Custom Threat Feed Websites - STIX Formatted Data and TAXII Import via Java
- Custom Threat Feed Websites - Programmatic Import via Python
- Working with Custom Threat Feeds that use HTTPS Connectivity

Prerequisites

Before proceeding, gather the following information about a threat feed web site:

- Website URL
- Credentials required to access the website (optional).

- If the website is not supported by FortiSIEM, you may need to understand the format of the data returned by the URL.
  - If the data is in the comma-separated value format (the separator need not be a comma but could be any separator), then a simple integration is possible.
  - If the data is any other format, for example, XML, then some code must be written for integration using the framework provided by FortiSIEM.

Websites with Built-in Support

The following websites are supported:

- Emerging threat (http://rules.emergingthreats.net)
- Threat Stream Malware IP (https://api.threatstream.com)
- Hail-A-TAXII Malware IP (http://hailataxii.com/)

For Threat Stream Malware IP, the following Malware types are imported:

- Bot IP
- Actor IP
- APT Email
- APT IP
- Bruteforce IP
- Compromised IP
- Malware IP
- DDoS IP
- Phishing email IP
- Phish URL IP
- Scan IP
- Spam IP

To import data from these websites, follow these steps:

1. In the **RESOURCES** > **Malware IPs**, find the website you must import data from.
2. Select the folder.
3. Click **More** > **Update**.
4. Select **Update via API**. The link will show in the edit box.
5. Enter a **Schedule** by clicking the **+** icon.
6. Enter the schedule parameters - when to start and how often to import. FortiSIEM recommends no more frequent than hourly.
7. Select the type of template you want to create.

Custom Threat Feed Websites - CSV Data - One-time Manual Import

This requires that the data to be imported is already in a file in comma-separated value format.

Requirements for Importing

1. The CSV file columns must be in the following order:

   `Name, Low IP, High IP, Malware Type, Confidence, Severity, ASN, Org, Country ,Description, Date Found(MM/DD/YYYY), Last Seen(MM/DD/YYYY)`

   If the fields are not in this order, then the whole file will not be imported.

2. `Name`, `Low IP`, and `High IP` are required fields. All `Name` fields must be unique. If `High IP` is not available, then the `High IP` field should be set to the `Low IP`.

   Example: BadMalware,1.2.3.4,1.2.3.10

1. Select **RESOURCES** > **Malware IPs**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware IP Group** dialog box.
3. Enter a **Group** name and add a **Description**.
4. Click **Save** to create the folder under **Malware IPs**.
5. Select the folder just created.
6. Select **More > Update**.
7. Click **Choose File**.
8. Browse to the file you want to import and select it.
9. Leave **Data Update** as **Full** (Completely replace) or **Incremental** (add on to existing data).
10. Click **Import**.
    The imported data will appear in the right pane.

Custom Threat Feed Websites - CSV Data - Programmatic Import via Java

Requirements for Importing

1. The Web Site Data requires the following:
   a. A file in comma-separated value format (separator can be any special character such as space, tab, hash, dollar etc.).
   b. An individual entry is in one line.
2. The `Low IP` field is required and must be unique.

   Example: 1.2.3.4

Follow these steps:

1. Select **RESOURCES** > **Malware IPs**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware IP Group** dialog.
3. Enter **Group** and add **Description**. Click **Save** to create the folder under **Malware IPs**.
4. Select the folder just created.
5. Select **More** > **Update** > **Update via API**.
6. Click the edit icon next to **URL** and provide the following information:
   a. Enter the **URL** of the website.
   b. Enter **User Name** and **Password** (optional).
   c. For **Plugin Type**, select **Java**.
   d. For **Plugin Class**, the default class **com.accelops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService** is displayed.
      Note: Do not modify this in any case.

    e. Enter the correct **Field Separator** (by default, it is a comma).
    f. Select **CSV** as the **Data Format**.
    g. Enter the **Data Mapping** by choosing the mapped field and the corresponding position in the website data. For example, if the IP is in third position, then choose 3 in the **Position** column.
7. Click **Save**.
8. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.
   The imported data will show on the right pane after some time.

Custom Threat Feed Websites - Non-CSV Data - Programmatic Import via Java

This is the most general case where the website data format does not satisfy the previous conditions. In this case, write a Java plugin class by modifying the default system provided one.

After the class has been written and fully tested for correctness, follow these steps.

1. Select **RESOURCES** > **Malware IPs**.
2. Click on the "**+**" button on the left navigation tree to bring up the **Create New Malware IP Group** dialog.
3. Enter **Group** and add **Description**.
4. Click **Save** to create the folder under **Malware IPs**.
5. Select the folder just created.
6. Select **More** > **Update** > **Update via API**.
7. Click the edit icon and:
    a. Enter the **URL** of the website.
    b. Enter **User Name** and **Password** (optional).
    c. For **Plugin Type**, select **Java**.
    d. For **Plugin Class**, the custom Java class for this case.
    e. Select 'Custom' as the **Data Format**.
    f. Click **Save**.
8. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.
   The imported data will display on the right pane after some time.

Custom Threat Feed Websites - STIX Formatted Data and TAXII Import via Java

In this case, the threat feed data is available formatted as STIX and follows the TAXII protocol.

1. Select **RESOURCES** > **Malware IPs**.
2. Click on the "**+**" button on the left navigation tree to bring up the **Create New Malware IP Group** dialog.
3. Enter **Group** and add **Description**. Click **Save** to create the folder under **Malware IPs**.
4. Select the folder just created.
5. Select **More** > **Update** > **Update via API**.
6. Click the edit icon and:
    a. Enter the **URL** of the website.
    b. Enter **User Name** and **Password** (optional).
    c. For **Plugin Type**, select **Java**.
    d. Select 'STIX-TAXII' as the **Data Format**.

   e. For **Plugin Class**, choose **com.accelops.service.threatfeed.impl.StixMalwareIPUpdateService** and **Full**.
   f. Click **Save**.
7. Select a import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.
   The imported data will show on the right pane after some time.

Custom Threat Feed Websites - Programmatic Import via Python

In this case, the threat feed data is available via python integration.

1. Select **RESOURCES**>**Malware IPs**.
2. Click on the "**+**" button on the left navigation tree to bring up the **Create New Malware IP Group** dialog.
3. Enter **Group** and add **Description**. Click **Save** to create the folder under **Malware IPs**.
4. Select the folder just created.
5. Select **More** > **Update** > **Update via API**.
6. Click the edit icon next to **URL** and provide the following information:
   a. In the **URL** field, enter the URL of the website.
      Note: Include the "http://" or "https://" prefix.
   b. (optional) In the **User Name** field, enter the username used by the API.
   c. (optional) In the **Password** field, enter the password related to the username.
   d. For **Plugin Type**, select **Python**.
   e. From the **Plugin Class** drop-down list, select the python script to use. Python scripts located under `/opt/phoenix/data-definition/threatfeedIntegrations/` will be available.
      Note: For more information on creating/using a Python script, see Appendix: Python Threat Feed Framework.
   f. For **Data Update**, select **Full** (Completely replace all data) or **Incremental** (add on to existing data).
7. Click **Save**.
8. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.
   The imported data will show on the right pane after some time.

Viewing Malware IPs

The Malware IPs Integration Status page shows all your existing Malware IP feeds. See the following table for more information.

Navigate to **RESOURCES**, and select **Malware IPs** to view the Malware IPs Integration Status page.

Column	Description
Status	Displays the current status of the Malware IPs listed in the Feed column.
Feed	Displays Malware IP group and its threat feed URL, if the information is available.
Indicators	Shows the current and prior threat feed objects for the Malware IP group to

Column	Description
	easier identify the change that occurred.
Last Updated	Displays the last time the threat feed was updated.
Pulling Schedule	Displays the scheduled time, when the threat feed update occurs.
Integration Type	Displays how the threat feed information is gathered, MANUAL or API.
Action	The Action columns allows you to perform one of three actions: • **View Content** - Click to view the existing Malware IP threat feed objects. • **Update** - Click to update the Malware IP threat feed.

Malware URLs

The Malware URLs page lists URLs that are known to host malware. The Threat Stream Blocked URL group is included in your FortiSIEM deployment.

The following sections describe Malware URLs:

Adding a Malware URL

Complete these steps to add a Malware URL:

1. Go to **RESOURCES** > **Malware URLs**.
2. Select a group where you want to add the Malware URL, or create a new one by clicking **+** above the **RESOURCES** groups.
3. Click **New**.
4. Enter the following information about the Malware URL:
   - URL
   - Malware Type
   - Confidence
   - Description
   - Last Seen
5. Click **Save**.

To configure a ThreatConnect Malware Domain, see Working with ThreatConnect IOCs.

To configure a FortiGuard Malware URL, see Working with FortiGuard Malware URLs.

Modifying a Malware URL

Complete these steps to edit a Malware URL:

1. Go to **RESOURCES** > **Malware URLs**.
2. Select the Malware URL group from the folder structure on the left panel.
3. Select the Malware URL from the table and click **Edit** to modify the settings.
4. Click **Save**.

To configure a ThreatConnect Malware URL, see Working with ThreatConnect IOCs.

To configure a FortiGuard Malware URL, see Working with FortiGuard Malware URLs.

You can use the **Delete** button to select and remove any Malware URL from the list.

Deleting a Malware URL

Complete these steps to delete a Malware URL:

1. Go to **RESOURCES** > **Malware URLs**.
2. Select the Malware URL group from the folder structure on the left panel.
3. Select the Malware URL from the table and click **Delete** to delete.
4. Click **Yes** to confirm.

Importing Malware URLs

This section describes how to import Malware URL information into FortiSIEM from external threat feed websites.

- Prerequisites
- Threat Feed Websites with Built-in Support
- Custom Threat Feed Websites - CSV Data - One-time Manual Import
- Custom Threat Feed Websites - CSV Data - Programmatic Import via Java
- Custom Threat Feed Websites - Non-CSV Data - Programmatic Import via Java
- Custom Threat Feed Websites - STIX Formatted Data and TAXII Import via Java
- Custom Threat Feed Websites - Programmatic Import via Python
- Working with Custom Threat Feeds that use HTTPS Connectivity

Prerequisites

Before proceeding, gather the following information about a threat feed web site:

- Website URL.
- Credentials required to access the website (optional).
- If the website is not supported by FortiSIEM, you may need to understand the format of the data returned by the URL.
  - If the data is in comma-separated value (CSV) format, then a simple integration is possible. Note that the separator need not be a comma but could be any separator.

- If the data is any other format, for example, XML, then some code must be written for integration using the framework provided by FortiSIEM.

Threat Feed Websites with Built-in Support

The following websites are supported:

- Threat Stream Malware URL (https://api.threatstream.com)
- FortiSandbox Malware URL
- Hail-A-TAXII Malware IP (http://hailataxii.com/)

To import data from these websites, follow these steps:

1. In the **RESOURCES** > **Malware URLs**, find the website you must import data from.
2. Select the folder.
3. Click **More** > **Update**.
4. Select **Update via API**. The link will show in the edit box.
5. Enter a **Schedule** by clicking the **+** icon.
6. Enter the schedule parameters: when to start and how often to import. FortiSIEM recommends no more frequent than hourly.

Custom Threat Feed Websites - CSV Data - One-time Manual Import

This requires that the data to be imported is already in a file in comma-separated value (CSV) format.

Requirements for Importing

1. The CSV file columns must be in the following order:

   ```
   URL, Malware Type, Confidence, Description, Last Seen (MM/DD/YYYY)
   ```

   If the fields are not in this order, then the whole file will not be imported.

2. The `URL` field is required and must be unique.

   Example: www.0800thissite.ru/zone/freebee.php

1. Select **RESOURCES** > **Malware URLs**.
2. Click the + button on the left navigation tree to open the **Create New Malware URL Group** dialog.
3. Enter **Group** and add **Description**. Click **Save** to create the folder under **Malware URLs**.
4. Select the folder just created.
5. Select **Import from a CSV file**.
6. Click **Choose File**; enter the file name and click **Upload**.
   The imported data will show on the right pane.

Custom Threat Feed Websites - CSV Data - Programmatic Import via Java

Requirements for Importing

1. The Web Site Data requires the following:
   a. A file in comma-separated value format (separator can be any special character such as space, tab, hash, dollar etc.).
   b. An individual entry is in one line.
2. The `URL` field is required and must be unique.

   Example: www.0800thissite.ru/zone/freebee.php

Follow these steps:

1. Select **RESOURCES** > **Malware URLs**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware URL Group** dialog box.
3. Enter **Group** and add **Description**. Click **Save** to create the folder under **Malware URLs**.
4. Select the folder just created.
5. Select **More** > **Update** > **Update via API**.
6. Click the edit icon next to **URL** and:
   a. Enter the **URL** of the website.
   b. Enter **User Name** and **Password** (optional).
   c. For **Plugin Type**, select **Java**.
   d. For **Plugin Class**, the default class **com.accelops.service.threatfeed.impl.ThreatstreamMalwareUrlUpdateService** is shown. Do not modify this value for this case.
   e. Enter the correct **Field Separator** (by default it is a comma).
   f. Set **Data Format** to **CSV**.
   g. Select **Data Update** as **Full** to overwrite the existing data or **Incremental** to retain the existing data.
   h. Enter the **Data Mapping** by choosing the mapped field and the corresponding position in the website data. For example if the URL is in third position, then choose 3 in the **Position** column.
   i. Click **Save**.
7. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import new data from the website.
   The imported data will show on the right pane.

Custom Threat Feed Websites - Non-CSV Data - Programmatic Import via Java

This is the most general case where the website data format is not CSV. In this case, write a Java plugin by modifying the default class provided by the system.

After the class has been written and fully tested for correctness, follow these steps:

1. Select **RESOURCES** > **Malware URLs**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware URL Group** dialog.
3. Enter the **Group** name and add a **Description**. Click **Save** to create the folder under **Malware URLs**.
4. Select the folder just created.
5. Select **More** > **Update** > **Update via API**.
6. Click the edit icon and:
   a. Enter the **URL** of the website.
   b. Enter **User Name** and **Password** (optional).

   c. For **Plugin Type**, select **Java**.
   d. For **Plugin Class**, enter the name of the custom Java plugin class.
   e. Select **Custom** as the **Data Format**.
   f. Select **Data Update** as **Full** to overwrite the existing data or **Incremental** to retain the existing data.
   g. Click **Save**.

7. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import new data from the website.
   The imported data will show on the right pane.

Custom Threat Feed Websites - STIX Formatted Data and TAXII Import via Java

In this case, the threat feed data is available formatted as STIX and follows the TAXII protocol.

1. Select **RESOURCES** > **Malware URLs**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware URL Group** dialog box.
3. Enter **Group** and add **Description**. Click **Save** to create the folder under **Malware URLs**.
4. Select the folder just created.
5. Select **More** > **Update** > **Update via API**.
6. Click the edit icon and:
   a. Enter the **URL** of the website.
   b. Enter **User Name** and **Password** (optional).
   c. Do not edit the name of the **Plugin Class**.
   d. For **Plugin Type**, select **Java**.
   e. Select **STIX-TAXII** as the **Data Format**.
   f. Enter the name of the STIX-TAXII **Collection**.
   g. Select **Full** as the **Data Update** value. Existing data will be overwritten.
   h. Click **Save**.
7. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import new data from the website.
   The imported data will display on the right pane.

Custom Threat Feed Websites - Programmatic Import via Python

In this case, the threat feed data is available through Python integration.

1. Select **RESOURCES** > **Malware URLs**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware URL Group** dialog box.
3. Enter **Group** and add **Description**. Click **Save** to create the folder under **Malware URLs**.
4. Select the folder just created.
5. Select **More** > **Update** > **Update via API**.
6. Click the edit icon next to **URL** and provide the following information:
   a. In the **URL** field, enter the URL of the website.
      Note: Include the "http://" or "https://" prefix.
   b. (optional) In the **User Name** field, enter the username used by the API.
   c. (optional) In the **Password** field, enter the password related to the username.
   d. For **Plugin Type**, select **Python**.

   e. From the **Plugin Class** drop-down list, select the python script to use. Python scripts located under `/opt/phoenix/data-definition/threatfeedIntegrations/` will be available.
      Note: For more information on creating/using a Python script, see Appendix: Python Threat Feed Framework.
   f. For **Data Update**, select **Full** (Completely replace all data) or **Incremental** (add on to existing data).
7. Click **Save**.
8. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.
   The imported data will show on the right pane after some time.

Viewing Malware URLs

The Malware URLs Integration Status page shows all your existing Malware URL feeds. See the following table for more information.

Navigate to **RESOURCES**, and select **Malware URLs** to view the Malware URLs Integration Status page.

Column	Description
Status	Displays the current status of the Malware URLs listed in the Feed column.
Feed	Displays Malware URLs group and its threat feed URL, if the information is available.
Indicators	Shows the current and prior threat feed objects for the Malware URL group to easier identify the change that occurred.
Last Updated	Displays the last time the threat feed was updated.
Pulling Schedule	Displays the scheduled time, when the threat feed update occurs.
Integration Type	Displays how the threat feed information is gathered, MANUAL or API.
Action	The Action columns allows you to perform one of three actions: • **View Content** - Click to view the existing Malware URL threat feed objects. • **Update** - Click to update the Malware URL threat feed.

Malware Processes

The following sections describe Malware Processes:

Creating a Malware Process Group

Complete these steps to add a Malware Process group:

1. Go to **RESOURCES** and select **Malware Processes**.
2. Click **+** above the **RESOURCES** groups.
3. Enter a group **Name** and **Description** in the **Create New Malware Process Group** dialog box.
4. Choose processes to include by expanding the tree in the **Folders** panel.
5. Select processes from the **Items** panel and move them to the **Selections** panel.
6. Click **Save**.

Adding a Malware Process

Complete these steps to add a Malware Processes:

1. Go to **RESOURCES** > **Malware Processes**.
2. Select a group where you want to add the Malware Processes.
3. Click **New**.
4. Enter the **Process Name** and **Description** of the Malware Process.
5. Click **Save**.

Complete these steps to import Malware processes from a CSV file:

1. Go to **RESOURCES** > **Malware Processes**.
2. Click **More** > **Update** > **Import from a CSV file**.
3. Click **Choose File** to select the CSV file.
4. Click **Import**.

Modifying a Malware Process

Complete these steps to edit a Malware Process:

1. Go to **RESOURCES** > **Malware Processes**.
2. Select the Malware Process group from the folder structure on the left panel.
3. Select the Malware Process from the table and click **Edit** to modify the settings.
4. Click **Save**.

Deleting a Malware Process

Complete these steps to delete a Malware Process:

1. Go to **RESOURCES** > **Malware Processes**.
2. Select the Malware Process group from the folder structure on the left panel.

3. Select the Malware Process from the table and click **Delete** to delete.
4. Confirm whether to **Remove only from group** by clicking **Yes** or **No**.

Importing Malware Processes

- Custom Threat Feed Websites - CSV Data - One-time Manual Import

Custom Threat Feed Websites - CSV Data - One-time Manual Import

This requires that the data to be imported is already in a file in comma-separated value (CSV) format.

Requirements for Importing

1. The CSV file columns must be in the following order:

   ```
   Process Name, Description
   ```

   If the fields are not in this order, then the whole file will not be imported.
2. The `Process Name` field is required and must be unique.

   Example: mscd.exe

1. Select **RESOURCES > Malware Processes**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware Process Group** dialog box.
3. In the **Group** field, enter a Group name.
4. In the **Description** field, enter a description.
5. Click **Save** to create the folder under **Malware Processes**.
6. Select the folder just created.
7. Select **More > Update**.
8. Click **Choose File**.
9. Browse to the CSV file you want to import and select it.
10. Leave **Data Update** as **Full** (Completely replace) or **Incremental** (add on to existing data)
11. Click **Import**.

Viewing Malware Processes

The Malware Processes Integration Status page shows all your existing Malware Process feeds. See the following table for more information.

Navigate to **RESOURCES**, and select **Malware Processes** to view the Malware Processes Integration Status page.

Column	Description
Status	Displays the current status of the Malware Processes listed in the Feed column.
Feed	Displays Malware Processes group and its threat feed URL, if the information is available.
Indicators	Shows the current and prior threat feed objects for the Malware Processes group to easier identify the change that occurred.

Column	Description
Last Updated	Displays the last time the threat feed was updated.
Pulling Schedule	Displays the scheduled time, when the threat feed update occurs.
Integration Type	Displays how the threat feed information is gathered, MANUAL or API.
Action	The Action columns allows you to perform one of three actions: • **View Content** - Click to view the existing Malware Processes threat feed objects. • **Update** - Click to update the Malware Processes threat feed.

Country Groups

The Country Groups page contains a list of all of the country names in the FortiSIEM geolocation database. You can also create folders that represent different organizations of countries for use in analytics.

Creating a Country Group

Complete these steps to add a Country Group:

1. Go to **RESOURCES** > **Country Group**.
2. Click **+** above the **RESOURCES** groups.
3. Enter a group **Name** and **Description** in the **Create New Country Group** dialog box.
4. Choose countries to include by expanding the tree in the **Folders** panel, selecting countries from the **Items** panel, and moving them to the **Selections** panel.
5. Click **Save**.

Adding a Country Group

Complete these steps to add a Country Group:

1. Go to **RESOURCES** > **Country Group**.
2. Select a group where you want to add the Country Group, or create a new one by clicking **+** above the **RESOURCES** groups.
3. Click **New**.

4. Enter the **Country Name** and **Description** of the Country Group.
5. Click **Save**.

Modifying a Country Group

Complete these steps to edit a Country Group:

1. Go to **RESOURCES** > **Country Groups**.
2. Select a Country Group from the left panel.
3. Select the Country Group from the table and click **Edit** to modify the settings.
4. Click **Save**.

Deleting a Country Group

Complete these steps to delete a Country Group:

1. Go to **RESOURCES** > **Country Groups**.
2. Select a Country Group from the left panel.
3. Select **-** above the Resource groups.
4. Confirm whether to **Remove only from group** or to remove the group completely by clicking **Yes**.

Changing the Home Country

Many rules and reports use the My Home CMDB Object as defined in **RESOURCES** > **Country Groups** > **My Home**.

By default, this is set to **United States of America**.

Complete these steps to change your home country:

1. Go to **RESOURCES** > **Country Groups**.
2. Select **My Home** from the left panel.
3. Click the Edit icon (✎) at the top left panel.
4. From the **Edit Country Group : My Home** window, take the following steps:
   a. In the leftmost panel, expand **Country Groups** and select a country group folder.
   b. In the middle panel, select a country.
   c. Click **>** to add the selected country to your My Home.
      Note: You can also select a country in the rightmost panel and click **<** to remove it from My Home.
5. Click **Save**.

Malware Hash

Use the **Malware Hash** page to define a list of malware files and their hash functions. When FortiSIEM monitors a directory, it generates these directory events:

Directory Event	Generated by This Action
`PH_DEV_MON_CUST_FILE_CREATE`	New file creation

Directory Event	Generated by This Action
`PH_DEV_MON_CUST_FILE_SCAN`	Directory is scanned
`PH_DEV_MON_CUST_FILE_CHANGE_CONTENT`	Changes in file content

When FortiSIEM scans a file and collects its hash, it uses the system rule `Malware Hash Check` to check the list of malware hashes. FortiSIEM will then trigger an alert if a match is found.

The following sections describe Malware Hashes:

Adding a Malware Hash

Complete these steps to add a Malware Hash:

1. Go to **RESOURCES** > **Malware Hash**.
2. Select a group where you want to add the Malware Hash, or create a new group by clicking **+** above the **RESOURCES** groups.
3. Click **New** and add the information related to the Malware Hash.
4. Click **Save**.

To add a ThreatConnect Malware Hash, see Working with ThreatConnect.

Modifying a Malware Hash

Complete these steps to edit a Malware Hash:

1. Go to **RESOURCES** > **Malware Hash**.
2. Select the Malware Hash group from the folder structure on the left panel.
3. Select the Malware Hash from the table and click **Edit** to modify the settings.
4. Click **Save**.

To modify a ThreatConnect Malware Hash, see Working with ThreatConnect.

You can use the **Delete** button to select and remove any Malware Hash from the list.

Updating User-defined Malware Hash

System defined groups are updated by its own service:

- Threat Stream Malware Hash
- FortiSandbox Malware Hash

You can update the Malware Hash using the following options:

- Import from a CSV File
- Update via API

Prerequisites:

Before proceeding, gather the following information about a threat feed web site.

- Website URL.
- Credentials required to access the website (optional).
- If the website is not supported by FortiSIEM, you must understand the format of the data returned by the URL.
  - If the data is in the comma-separated value format (the separator need not be a comma but could be any separator, then a simple integration is possible.)
  - If the data is any other format, for example, XML, then some code must be written for integration using the framework provided by FortiSIEM.

Import from a CSV File

Custom Websites - CSV Data - One-time Manual Import

Instead of manually adding Malware Hashes to a group individually, you can upload a CSV file with multiple entries. This requires that the data to be imported is already in a file in a comma-separated value (CSV) format.

Requirements for Importing

1. The CSV file columns must be in the following order:

   ```
   Botnet Name, Algorithm, Hash Code, Controller IP, Malware Type, Confidence,
   Severity, Asn, Origin, Country, Description, Date Found(MM/DD/YYYY), Last Seen
   (MM/DD/YYYY)
   ```

   If the fields are not in this order, then the whole file will not be imported.

2. `Botnet Name`, `Algorithm`, and `Hash Code` are required fields. The 3 required fields are linked, so any changes to the fields within each row will produce a unique entry.

   Examples:

   newbotnet, md5, 4da0bb01a96e70ce43ece0147f8438d1

   newbotnet1,sha256,8e53e4d236c99ba4dcf7c4cbf1cea93d023391ea

1. Go to **RESOURCES** > **Malware Hash**.
2. Select the group from the left panel or create a new group by clicking the **+** icon above the list of RESOURCES groups.
3. Select **More** > **Update**.
4. Select **Import from a CSV file** and choose the file to import.
5. Click **Import**.

Update via API

This section describes how to import Malware Hash information into FortiSIEM from external threat feed websites. Malware Hashes are used by malware to hide their own identity.

- Updating System Defined Malware Hash Group
- Custom Threat Feed Websites - CSV Data - Programmatic Import
- Custom Threat Feed Websites - Non-CSV Data - Programmatic Import via Java
- Custom Threat Feed Websites - Non-CSV Data -STIX Formatted Data and TAXII Import via Java
- Custom Threat Feed Websites - Programmatic Import via Python

Updating System Defined Malware Hash Group

The following websites are supported:

- Threat Stream Open Proxy (https://api.threatstream.com)
- Threat Stream TOR Node (https://api.threatstream.com)

Complete these steps to import data from these websites:

1. Go to **RESOURCES** > **Malware Hash**.
2. Select the folder and find the website you want to import data from.
3. Click **More** > **Update**.
4. Select **Update via API**.
   The link will be displayed in the URL field or else manually enter the URL and details.
5. Enter a **Schedule** by clicking the **+** icon.
6. Enter the schedule parameters - **Start Time** and **Recurrence Pattern**. FortiSIEM recommends no more frequent than hourly.
7. Click **Save**.
   You can use the edit icon to modify or delete icon to remove a **Schedule**.

Custom Threat Feed Websites - CSV Data - Programmatic Import via Java

Requirements for Importing

1. The Web Site Data requires the following:
   a. A file in comma-separated value format (separator can be any special character such as space, tab, hash, dollar etc.).
   b. An individual entry is in one line.
2. The CSV file columns must be in the following order:

   ```
   Botnet Name, Algorithm, Hash Code, Controller IP, Malware Type, Confidence,
   Severity, Asn, Origin, Country, Description, Date Found (MM/DD/YYYY), Last Seen
   (MM/DD/YYYY)
   ```

   If the fields are not in this order, then the whole file will not be imported.
3. The `Botnet Name` field is required and must be unique.

1. Go to **RESOURCES** > **Malware Hash**.
2. Select the folder or click **+** to add a new group under **Malware Hash** folder.
3. Click **More** > **Update**.
4. Select **Update via API**. The link will be displayed in the URL field or else manually enter the URL and details.
5. Click the edit icon near **URL**.
6. Enter the following information:
   a. In the **URL** field, enter the URL of the website.
   Note: Ensure you have an "http://" or "https://" prefix.
   b. (Optional) In the **User Name** field, enter the username associated with the API.
   c. (Optional) In the **Password** field, enter the password associated with the username.
   d. For **Plugin Type**, select **Java**.
   e. For **Plugin Class**, the default class '**com.accelops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService**' is shown. Do not modify this in any case.
   f. Enter the correct **Field Separator** (by default it is a comma).
   g. Select **CSV** as the **Data Format**.
   h. Select **Data Update** as **Full**.
   i. Enter the **Data Mapping** by choosing the mapped field and the corresponding position in the website data. For example, if the Botnet Name is in third position, choose 3 in the **Position** column. Click **+** if you must add more rows.
   j. Click **Save**.
7. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import new data from the website.
   The imported data will show on the right pane after some time.

Custom Threat Feed Websites - Non-CSV Data - Programmatic Import via Java

This is the most general case where the website data format does not satisfy the previous conditions. In this case, write a Java plugin class by modifying the default system provided one.

1. Go to **RESOURCES** > **Malware Hash**.
2. Select the folder or click **+** to add a new group under **Malware Hash** folder.
3. Click **More** > **Update**.
4. Select **Update via API**.
5. Click the edit icon near **URL**.
6. Enter the following information:
   a. Enter the **URL** of the website.
   b. Enter **User Name** and **Password** (optional).
   c. For **Plugin Type**, select **Java**.
   d. For **Plugin Class**, the custom Java class in this case.
   e. Select **Custom** as the **Data Format**.
      - Enter the **Data Mapping** by choosing the mapped field and the corresponding position in the website data. For example, if the IP is in third position, choose 3 in the **Position** column. Click **+** if you must add more rows.
      - Select **Full** as the **Data Update** value. Existing data will be overwritten. Select **Incremental** to preserve the existing data.

For **STIX-TAXII**:

- Enter the name of the STIX-TAXII **Collection**.
- Select **Full** as the **Data Update** value. Existing data will be overwritten.

f. Click **Save**.

7. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import new data from the website.
   The imported data will display in the table after some time.

Custom Threat Feed Websites - Non-CSV Data -STIX Formatted Data and TAXII Import via Java

In this case, the threat feed data is available formatted as STIX and follows the TAXII protocol.

1. Go to **RESOURCES** > **Malware Hash**.
2. Select the folder or click **+** to add a new group under **Malware Hash** folder.
3. Click **More** > **Update**.
4. Select **Update via API**.
5. Click the edit icon near **URL**.
6. Enter the following information:
   a. Enter the **URL** of the website.
   b. Enter **User Name** and **Password** (optional).
   c. For **Plugin Type**, select **Java**.
   d. For **Plugin Class**, the custom Java class in this case.
   e. Enter the name of the STIX-TAXII **Collection**.
   f. Select **STIX-TAXII** as the **Data Format**.
   g. Select **Data Update** as **Full**.
   h. Click **Save**.
7. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import new data from the website.
   The imported data will display in the table after some time.

Custom Threat Feed Websites - Programmatic Import via Python

In this case, the threat feed data is available via Python integration.

1. Go to **RESOURCES** > **Malware Hash**.
2. Select the folder or click **+** to add a new group under **Malware Hash** folder.
3. Click **More** > **Update**.
4. Select **Update via API**.
5. Click the edit icon next to **URL** and provide the following information:

   a. In the **URL** field, enter the URL of the website.
   Note: Include the "http://" or "https://" prefix.

   b. (optional) In the **User Name** field, enter the username used by the API.

   c. (optional) In the **Password** field, enter the password related to the username.

   d. For **Plugin Type**, select **Python**.

e. From the **Plugin Class** drop-down list, select the python script to use. Python scripts located under `/opt/phoenix/data-definition/threatfeedIntegrations/` will be available.

   Note: For more information on creating/using a Python script, see Appendix: Python Threat Feed Framework.

f. For **Data Update**, select **Full** (Completely replace all data) or **Incremental** (add on to existing data).

6. Click **Save**.
7. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.

   The imported data will show on the right pane after some time.

Viewing Malware Hash

The Malware Hash Integration Status page shows all your existing Malware Hash feeds. See the following table for more information.

Navigate to **RESOURCES**, and select **Malware Hash** to view the Malware Hash Integration Status page.

Column	Description
Status	Displays the current status of the Malware Hash listed in the Feed column.
Feed	Displays Malware Hash group and its threat feed URL, if the information is available.
Indicators	Shows the current and prior threat feed objects for the Malware Hash group to easier identify the change that occurred.
Last Updated	Displays the last time the threat feed was updated.
Pulling Schedule	Displays the scheduled time, when the threat feed update occurs.
Integration Type	Displays how the threat feed information is gathered, MANUAL or API.
Action	The Action columns allows you to perform one of three actions: • **View Content** - Click to view the existing Malware Hash threat feed objects. • **Update** - Click to update the Malware Hash threat feed.

Default Password

The Default Password page contains a list of default vendor credentials. These well-known credentials should never be used in production. During device discovery FortiSIEM checks if the device credentials are still set to default, The system rule `Default Password Detected by System` triggers an incident if they are.

This is a sample raw event log for a default password incident:

```
<174>Oct 20   22:50:03   [PH_AUDIT_DEFAULT_PWD_MATCH]:[phEventCategory]=2,[appTrans-
portProto]=SNMP,[reptModel]=Firewall-1   SPLAT,[srcIpAddr]=192.168.19.195,[phCustId]=1,[ses-
sionId]=0f8bdee2b6a265c4bd075fc777ed,[procName]=AppServer,[reptVendor]=Checkpoint,
[hostIpAddr]=172.16.0.1,[hostName]=SJ-QA-F-Lnx-CHK,[eventSeverity]=PHL_INFO,[user]=,[phLo-
gDetail]=Default password matches for   the same composite key (Vendor, Model, Access
method, User Name, Password)
```

The following sections describe Default Passwords:

Adding a Default Password

Complete these steps to add a default password:

1. Go to **RESOURCES** > **Default Password**.
2. Select a group where you want to add the default password, or create a new group by clicking **+** above the **RESOURCE** groups.
3. Click **New**.
4. Select the **Vendor** and **Model** of the device for which you want to enter a default password.
5. Select the **Access Protocol** that is used to connect to the device from the drop-down.
6. Enter the default **User Name** and **Password** for the device.
7. Click **Save**.

Modifying a Default Password

Complete these steps to edit a default password:

1. Go to **RESOURCES** > **Default Password**.
2. Select the default password group from the folder structure on the left panel.
3. Select the default password from the table and click **Edit** to modify the settings.
4. Click **Save**.

Use the **Delete** button to select and remove any default password(s) from the list.

Importing and Exporting a Default Password

The procedures below describe how to import and export a Default Password.

Importing Default Password

Instead of manually adding default passwords to a user-defined or system group individually, you can upload a CSV file with multiple entries into a group.

You must format the file with these fields: `Vendor,Model,Access Protocol,User Name,Password`

For example: `Microsoft,Windows,WMI,Administrator,Administrator`

1. Go to **RESOURCES** > **Default Password**.
2. Select the Default Password group where you want to import the new password from the folder structure.
3. Click **Import** and select the CSV file.
4. Click **Import**.

Exporting Default Password

Complete these steps to export a default password from a Group to a CSV File.

1. Go to **RESOURCES** > **Default Password**.
2. Select the Default Password group from where you want to export the Default Password from the folder structure.
3. Select the Default Password from the table and click **Export**.
4. Click **Generate**.
   'Export successful' message is displayed.
5. Click **Open Report File** and save the report.

Anonymity Network

An anonymity network is used to hide one's network identity, and is typically used by malware to hide its originating IP address. Enterprise network traffic should not be originating from or destined to Anonymity network.

When FortiSIEM discovers traffic destined to or originating from anonymity networks, it triggers these rules:

- Inbound Traffic from Tor Network
- Outbound Traffic to Tor Network
- Inbound Traffic from Open Proxies
- Outbound Traffic to Open Proxies

Adding Anonymity Networks

FortiSIEM provides two default (system-defined) groups for Anonymity Networks:

- **Open Proxies**: A set of open proxies in the internet. This is a static group.
- **Tor Nodes**: This group is dynamically updated from https://check.torproject.org/exit-addresses. To schedule regular updates for this group, click the group name, then click **Update** and provide updated scheduling information.

Complete these steps to add Anonymity Networks:

1. Go to **RESOURCES**> **Anonymity Network** folder on the left panel.
2. Select **Open Proxies** or **Tor Nodes** folder or click **+** to add a new group.
3. Click **New**.
4. Enter **IP**, **Port**, and **Country** information about the anonymity network.
5. Click the **Calendar** icon to select the **Date Found** and **Last Seen**.
6. Click **Save**.

Adding Anonymity Networks to Watch Lists

You can easily add an anonymity network IP address to your watch lists. Hover your mouse cursor over the anonymity network IP address until the icon for the **Options** menu appears, and then select **Add to Watchlist**.

Modifying Anonymity Networks

Complete these steps to edit an Anonymity Network:

1. Go to **RESOURCES** > **Anonymity Network**.
2. Select the Anonymity Network group from the folder structure on the left panel.
3. Select the Anonymity Network from the table and click **Edit** to modify the settings.
4. Click **Save**.

You can use the **Delete** button to select and remove any Anonymity Network from the list.

Updating Anonymity Networks

This section describes how to update Anonymity Network information in FortiSIEM from external threat feed websites.

You can update the Anonymity Network information in the following ways:

- Import from a CSV File
- Update via API

Prerequisites:

Before proceeding, gather the following information about a threat feed web site.

- Website URL.
- Credentials required to access the website (optional).
- If the website is not supported by FortiSIEM, you must understand the format of the data returned by the URL.
  - If the data is in the comma-separated value format (the separator need not be a comma but could be any separator, then a simple integration is possible.)
  - If the data is any other format, for example, XML, then some code needs to be written for integration using the FortiSIEM provided framework.

Import from a CSV File

Custom Websites - CSV Data - One-time Manual Import

Instead of manually adding anonymity networks to a group individually, you can upload a CSV file with multiple entries. This requires that the data to be imported is already in a file in comma-separated value format.

```
IP, Port, Malware Type, Confidence, Severity, Asn, Org, Country, Description, Data
Found(MM/DD/YYYY), Last Seen(MM/DD/YYYY)
```

Note: Although many fields are possible, only the IP is required.

1. Go to **RESOURCES** > **Anonymity Network**.
2. Select the group from the left panel or create a new group by clicking the **+** icon above the list of RESOURCES groups.
3. Select **More** > **Update**.
4. Select **Import from a CSV file** and choose the file to import.
5. Click **Import**.

Update via API

This section describes how to import anonymity networks information into FortiSIEM from external threat feed websites. Anonymity networks are used by malware to hide their own identity.

Websites with Built-in Support

The following websites are supported:

- Threat Stream Open Proxy (https://api.threatstream.com)
- Threat Stream TOR Node (https://api.threatstream.com)

Complete these steps to import data from these websites:

1. Go to **RESOURCES** > **Anonymity Network**.
2. Select the folder and find the website you must import data from.
3. Click **More** > **Update**.
4. Select **Update via API**. The link will be displayed in the URL field or else manually enter the URL and details.
5. Enter a **Schedule** by clicking the **+** icon.
6. Enter the schedule parameters - **Start Time** and **Recurrence Pattern**. FortiSIEM recommends no more frequent than hourly.
7. Click **Save**.
   You can use the edit icon to modify or delete icon to remove a **Schedule**.

Custom Websites - CSV Data - Programmatic Import

This requires that the web site data is:

- a file in comma-separated value format (separator can be any special character such as space, tab, hash, dollar etc.).
- one entry is in a single line.

Note: Although many fields are possible, only the IP is required.

1. Go to **RESOURCES** > **Anonymity Network**.
2. Select the folder or click **+** to add a new group under **Anonymity Network** folder.
3. Click **More** > **Update**.
4. Select **Update via API**. The link will be displayed in the URL field or else manually enter the URL and details.
5. Click the edit icon near **URL**.
6. Enter the following information:
    a. Enter the **URL** of the website.
    b. Enter **User Name** and **Password** (optional).
    c. For **Plugin Class**, the default class `com.accelops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService` is shown. **Do not modify this in this case.**
    d. Enter the correct **Field Separator** (by default it is a comma).
    e. Select **CSV** as the **Data Format**.
    f. Select **Data Update** as **Full** to overwrite the existing data or **Incremental** to retain the existing data.
    g. Enter the **Data Mapping** by choosing the mapped field and the corresponding position in the website data. For example, if the IP is in third position, choose 3 in the **Position** column. Click **+** if you must add more rows.
    h. Click **Save**.
7. Select an import schedule by clicking **+** on the **Schedule Summary**. Select when to start the import and how often to import new data from the website.
   The imported data will show on the right pane after some time.

New Websites - Non-CSV Data - Programmatic Import

This is the most general case where the website data format does not satisfy the previous conditions. In this case, you have to write a Java plugin class by modifying the default system provided one. After the class has been written and fully tested for correctness, follow these steps.

1. Go to **RESOURCES** > **Anonymity Network**.
2. Select the folder or click **+** to add a new group under **Anonymity Network** folder.
3. Click **More** > **Update**.
4. Select **Update via API**.
5. Click the edit icon near **URL**.
6. Enter the following information:
    a. Enter the **URL** of the website.
    b. Enter **User Name** and **Password** (optional).
    c. For **Plugin Class**, the custom Java class in this case.
    d. Enter the correct **Field Separator** (by default it is a comma).
    e. Select **Custom** or **STIX-TAXII** as the **Data Format**.
        - **STIX-TAXII** - provide the name of the **Collection**. Select **Data Update** as **Full** to overwrite the existing data or **Incremental** to retain the existing data.
        - **Custom** - select **Data Update** as **Full** to overwrite the existing data or **Incremental** to retain the existing data.
    f. Click **Save**.

7. Select an import schedule by clicking **+** on the **Schedule Summary**. Select when to start the import and how often to import new data from the website.
   The imported data will display in the table after some time.

User Agents

The User Agent page lists common and uncommon user agents in HTTP communications. The traditional use case for a user agent is to detect browser types so the server can return an optimized page. However, user agents are often misused by malware, and are used to communicate the identity of the client to the BotNet controller over HTTP(S). FortiSIEM monitors HTTP(S) logs and the system rule Blacklist User Agent Match uses regular expression matching to detect blacklisted user agents.

Adding User Agents

Complete these steps to add a User Agent:

1. Go to **RESOURCES** > **User Agents**.
2. Select the **User Agent** group where you want to add the new user agent from the folder structure on the left panel. To create a new User Agent group, click **+** above the **Resources** tree.
3. Click **New**.
4. Enter the **User Agent** using regular expression notation.
5. Click **Save**.

Modifying User Agents

Complete these steps to edit a User Agent:

1. Go to **RESOURCES** > **User Agents**.
2. Select the **User Agent** group from the folder structure on the left panel.
3. Select the User Agent from the table and click **Edit** to modify the settings.
4. Click **Save**.

You can use the **Delete** button to select and remove any User Agent from the list.

Importing and Exporting User Agents

The procedures below describe how to import and export User Agents.

Importing User Agents

Instead of manually adding User Agents to a user-defined or system group individually, you can upload a CSV file with multiple entries into a group.

Note: You must format the User Agent password with regular expression notation: *User Agent (regular expression)*

Complete these steps to import User Agents to a Group from a CSV File.

1. Go to **RESOURCES** > **User Agents**.
2. Select the **User Agent** group where you want to import the new User Agents from the folder structure.
3. Click **Import** and select the CSV file.
4. Click **Import**.

Exporting User Agents

Complete these steps to export User Agents from a Group to a CSV File.

1. Go to **RESOURCES** > **User Agents**.
2. Select the **User Agent** group from where you want to export the User Agents from the folder structure.
3. Select the User Agent from the table and click **Export**.
4. Click **Generate**.
   If the export is successful, an "Export successful" message is displayed.
5. Click **Open Report File** and save the report.

Remediations

Remediation can be performed either on an ad hoc basis or by using a Notification Policy. A Notification Policy directs the system to take a Remediation action when an Incident occurs. To invoke a Remediation, do the following:

- Make sure the Remediation script for your scenario is defined.
- Check the existing Remediation scripts. Go to **ADMIN** > **Settings** > **General** > **Notification Policy**, then choose **Run Remediation/Script** in the **Action** section of the Notification Policy dialog box. See Adding Incident Notification settings.
- If your device is not in the list, add the needed Remediation script.

The system-defined and custom Remediations are listed under **RESOURCES** > **Remediations**. The following sections describe how to create and manage custom Remediations.

- Adding Remediations
- Modifying Remediations
- Deleting Remediations

Adding Remediations

Complete these steps to create a new custom Remediation. You can also select any existing Remediation to **Clone** and customize.

1. Go to **RESOURCES** > **Remediations**.
2. Click **New**.

3. Enter the **Name** of the Remediation.
4. Select the **Device Type** to which this Remediation will be applied.
5. Select the **Protocol** as SSH, HTTP, HTTPS or MS_WMI for the device type.
6. Enter the Remediation **Script Name**.
7. Enter the Remediation **Script Content**.
8. Add any **Description** related to this Remediation.
9. Click **Save**.
   The Remediation will be available in the list along with the system-defined Remediations.

Modifying Remediations

Note that you cannot modify any system-defined Remediations.

Complete these steps to modify a custom Remediation:

1. Go to **RESOURCES** > **Remediations**.
2. Select a custom Remediation from the list.
3. Click **Edit** and modify the remediation settings.
4. Click **Save**.
   The updated Remediation will be available in the list along with the system-defined Remediations.

Deleting Remediations

Note that you cannot remove any system-defined Remediations.

Complete these steps to delete a custom Remediation(s).

1. Go to **RESOURCES** > **Remediations**.
2. Select the custom Remediation to delete from the list.
3. Click **Delete**.
4. Click **Yes** to confirm.
   These Remediation(s) will be deleted from the list.

Lookup Tables

The Lookup Tables page lists existing lookup tables. Lookup table schemas can be added, and Lookup table data can be added or imported on this page.

The Lookup Table page is comprised of the following fields:

Column	Description
Table Name	The name of the table is displayed.
Organization	The organization(s) which the table belongs to is displayed.
Description	Any additional information from the Description field when creating the table is displayed here.

Column	Description
Action	**View** - Click to open a table. From here, you can add data, edit existing data, or import data. **Delete** - Click to delete the table. **Schema** - Click to view the Lookup table's schema.

Adding a Lookup Table

Complete these steps to add a Lookup table:

Note: Once a table is created, the schema cannot be modified.

1. Go to **RESOURCES > Lookup Table**.
2. In the left panel, click on **+**.
3. In the **Create a New Lookup Table** window, from the **Organization** drop-down list, select the Organization that the Lookup table belongs to.
4. In the **Table Name** field, enter the name of the Lookup table.
5. (Optional) In the **Description** field, enter any additional information about the Lookup table.
6. In the **Schema** section, take the following actions.
   a. If adding a key to your Lookup table, select the **Key** checkbox, otherwise, if unselected, it becomes a column.
   b. In the **Name** field, enter a name for the key or the column.
   c. In the **Type** drop-down list, select the value type from LONG (for integers), STRING (character strings), or DOUBLE (for real numbers).
   d. Click **+** to add another Key value, and repeat steps a-c.
   Note: A maximum of 5 Key values may be created for a Lookup table.
   e. When done, click **Save**.

Deleting a Lookup Table

Complete these steps to remove an existing Lookup table:

1. Go to **RESOURCES > Lookup Table**.
2. Select the Lookup Table you wish to delete.

3. In the left panel, click on **-**.
4. Click **Yes** to confirm.

Working with Lookup Table Data

The following sections are available. For information on importing Lookup Table Data APIs, refer to the latest Integration API Guide.

Usage Notes: Lookup table data may not be immediately available for Rules and Reports. Supervisor pushes the Lookup table changes to the Supervisor Redis database once every 5 minutes. Supervisor Master Redis immediately pushes the data to the Worker Slave Redis databases. Rule, Report and Query modules on Supervisor and Worker nodes re-read the Lookup tables from local Redis database, once every 5 minutes. Therefore in the worst case, it may take 10 minutes for data to be propagated to the analytics modules. Rules and Reports using Lookup tables should show the correct results after 10 minutes (worst case). In practice, FortiSIEM will have the results show up between 5 and 10 minutes.

- Adding Lookup Table Data
- Deleting Lookup Table Data
- Editing Lookup Table Data
- Importing Lookup Table Data

Note: A maximum of 10 million entries is allowed before the rest of the data is truncated.

Adding Lookup Table Data

To add Lookup table data to your Lookup table, take the following steps:

1. From the **RESOURCES > Lookup Tables** page, select your Lookup table.
2. Click **View**.
3. Click **New**.
4. Enter the Key or Column data.
5. Click **Save**.

Deleting Lookup Table Data

1. From the **RESOURCES > Lookup Tables** page, select your Lookup table.
2. Click **View**.
3. Select the row of data you wish to delete.
4. Click **Delete**.
5. Click **Yes** to confirm.

Editing Lookup Table Data

To edit Lookup table data in your Lookup table, take the following steps:

1. From the **RESOURCES > Lookup Tables** page, select your Lookup table.
2. Click **View**.
3. Select the row you wish to edit.
4. Click **Edit**.

5. Enter the new Key or Column data.
6. Click **Save**.

Importing Lookup Table Data

You can import lookup table data from user-defined lookup tables or from a system-defined lookup table.

Note: System-defined lookup table data can only be imported via Report.

To import Lookup table data from a Lookup table, take the following steps:

1. From the **RESOURCES > Lookup Tables** page, select the Lookup table you wish to import.
2. Click **Import**.

From the Import window, select one of the following depending on the Lookup table type (user or system defined) and continue with the instructions that follow.

User-defined Lookup Table Data

- Import from a CSV file
- Update via API
- Import via Report

System-defined Lookup Table Data

- Import System Defined Lookup Table Data via Report

Importing from a CSV File

If **Import from a CSV file** is selected, take the following steps:

a. Click **Choose File**, and select your CSV file.
b. In the **Field Separator** field, select the character that represents your separator for data.
c. In the **Field Quote Char** field, select the character that represents the beginning and end quotation used for strings.
d. Select **Ignore Header** to ignore the header from your CSV file.
e. Click the **Mapping** edit icon to define your data with your schema.
    i. From the **Mapped Field** drop-down list, select the key or column.
    ii. From the **Position** drop-down list, select the position of the data from the csv file that should map to the key or column.
    iii. Click **+** to create a new row.
    iv. Click **Save** when done mapping your data.
f. Click **Save**.

Update via API

If **Update via API** is selected, take the following steps:

a. In the **URL** field, enter the API URL endpoint.
b. In the **User** field, enter the user name to access the API endpoint.
c. In the **Password** field, enter the password to access the API endpoint.
d. In the **Field** Separator, enter the character that represents your separator for data.

e. In the **Mapping** field, click the edit icon and take the following steps:
    i. From the **Mapped Field** drop-down list, select an existing mapping to set its position.
    ii. From the **Position** drop-down list, select the position of the data from the csv file that should map to the key or column.
    iii. Click **+** to add a new row for any additional mapping that is needed.
    iv. Click **Save** when done mapping your data.

f. In the **Schedule** field, set the time which the update should occur by doing the following:
    i. In the **Start Time** field, set the time.
    ii. In the **Schedule Recurrence Pattern**, set the period.
    iii. Click **OK** when done.

g. Click **Save**.

Import via Report

If Import via Report is selected, take the following steps:

a. Click the **Report** edit icon.

b. Select a Report or CMDB Report, and click **OK**.

c. Click the **Mapping** edit icon.

d. From the Mapping dialog box, take the following steps:
    i. From the **Mapped** drop-down list, select an existing mapping to set its position.
    ii. In the **Attribute** field, select or type the associated attribute to use.
    iii. Click **+** to add a new row for any additional mapping that is needed.
    iv. Click **Save** when done mapping your data.

e. Click the **Enabled** checkbox to configure a schedule.

f. Click the **Schedule** edit icon.

g. In the **Schedule Report Time Range** dialog box, do the following:
    i. In the **Time Zone** row, select the appropriate time from the drop-down lists.
    ii. Select **Relative** or **Absolute** time, and then enter the information for period of time for recurrence.
    iii. From the **Trend Interval** drop-down list, select the period of recurrence.
    iv. Click **Next**.

h. In the **Schedule Time Range** dialog box, do the following:
    i. Enter the scheduling information using the **Start Time** fields/drop-down list.
    ii. Under **Schedule Recurrence Pattern**, enter/select when the schedeul repeats.
    iii. Under **Schedule Recurrence Range**, enter the Start date.
    iv. Under **Schedule Recurrence Range**, choose/enter the time that the schedule ends.
    v. Click **Next**.

i. In the **Schedule Retention** dialog box, do the following:
    i. Under **Retention**, enter/choose the period of time for retaining reports.
    ii. Click **OK**.

j. Click **Save** to save the Schedule configuration.

k. Click **Run now** to import the data.

Import System Defined Lookup Table Data via Report

If **Import via Report** is selected for a system-defined Lookup table, take the following steps:

a. Click the **Enabled** checkbox to configure a schedule.
b. Click the **Schedule** edit icon.
c. In the **Schedule Report Time Range** dialog box, do the following:
   i. In the **Time Zone** row, select the appropriate time from the drop-down lists.
   ii. Select **Relative** or **Absolute** time, and then enter the information for period of time for recurrence.
   iii. From the **Trend Interval** drop-down list, select the period of recurrence.
   iv. Click **Next**.
d. In the **Schedule Time Range** dialog box, do the following:
   i. Enter the scheduling information using the **Start Time** fields/drop-down list.
   ii. Under **Schedule Recurrence Pattern**, enter/select when the schedeul repeats.
   iii. Under **Schedule Recurrence Range**, enter the Start date.
   iv. Under **Schedule Recurrence Range**, choose/enter the time that the schedule ends.
   v. Click **Next**.
e. In the **Schedule Retention** dialog box, do the following:
   i. Under **Retention**, enter/choose the period of time for retaining reports.
   ii. Click **OK**.
f. Click **Save** to save the Schedule configuration.
g. Click **Run now** to import the data.

Playbooks

A Playbook is a chain of actions that are taken based on logic programmed by a user. A Playbook can only be added, modified, or deleted through FortiSOAR. Playbooks can be executed on an event or incident. After creating a FortiSIEM user in FortiSOAR and configuring Playbook on FortiSIEM, playbooks can be executed through FortiSIEM. Additional information can also be found in Writing FortiSIEM Compatible FortiSOAR Playbooks available in the Appendix.

The following sections provide information on Playbooks:

Viewing Playbooks

FortiSIEM can sync with FortiSOAR to pull the latest FortiSOAR Playbooks. These Playbooks are available on the **RESOURCES > Playbooks** page.

Column	Description
Name	The Playbook name is displayed.
Description	A description of what the Playbook does is displayed.

Updating Playbooks

To update your FortiSOAR playbooks, take the following steps.

Note: You must create a FortiSIEM user in FortiSOAR before proceeding with these steps. For more information, see here.

1. From **RESOURCES > Playbooks > FortiSOAR Playbooks**, click **Update**.
2. From the Update Playbook window, in the **URL** row, click the pencil icon to configure how FortiSIEM will connect with FortiSOAR. If there is an existing configuration, click the Edit icon to modify it.
   a. In the **Host Name** field, enter the IP address of the FortiSOAR application.
   b. In the User Name field, enter the username to access the FortiSOAR application.
   c. In the **Password** field, enter the password associated with the username for FortiSOAR application access.
   d. When done, click **Save**.
3. From the Update Playbook window, in the **Schedule** row, click **+** to create a new schedule, or the Edit icon to modify an existing one.
   a. In the **Start Time** field, enter the time when FortiSIEM will connect to FortiSOAR to retrieve any updated Playbooks.
   b. In the next two drop-down lists, define the time by selecting the appropriate time zone and region.
   c. Under **Recurrence Pattern** , select how frequently FortiSIEM will connect to FortiSOAR to check FortiSOAR Playbooks. Choices are: **Once**, **Hourly**, **Daily**, **Weekly**, or **Monthly**.
   d. Click on the **Start Now** field, and enter or select the Month, Day, and Year when update(s) should occur. The format is `mm/dd/yyyy`.
   e. When done, click **Save**.

Connectors

A connector is a solitary action that can be run by a user. Connectors can only be added, modified, or deleted through FortiSOAR. A connector can be run on an event or incident. After creating a FortiSIEM user in FortiSOAR and configuring Connector on FortiSIEM, connectors can be run through FortiSIEM. Additional information can also be found in Playbooks and Connectors under Writing FortiSIEM Compatible FortiSOAR Playbooks available in the Appendix.

The following sections provide information on Connectors:

Viewing Connectors

FortiSIEM can sync with FortiSOAR to pull the latest FortiSOAR Connectors. These Connectors are available on the **RESOURCES > Connectors** page.

Column	Description
Name	The Connector name is displayed.
Description	A description of what the Connector does is displayed.

Updating Connectors

To update your FortiSOAR connectors, take the following steps.

Note: You must create a FortiSIEM user in FortiSOAR before proceeding with these steps. For more information, see here.

1. From **RESOURCES > Connectors > FortiSOAR Connectors**, click **Update**.
2. From the Update Connectors window, in the **URL** row, click **+** to configure how FortiSIEM will connect with FortiSOAR. If there is an existing configuration, click the Edit icon to modify it.
   a. In the **Host Name** field, enter the IP address of the FortiSOAR application.
   b. In the User Name field, enter the username to access the FortiSOAR application.
   c. In the **Password** field, enter the password associated with the username for FortiSOAR application access.
   d. When done, click **Save**.
3. From the Update Connectors window, in the **Schedule** row, click **+** to create a new schedule, or the Edit icon to modify an existing one.
   a. In the **Start Time** field, enter the time when FortiSIEM will connect to FortiSOAR to retrieve any updated Playbooks.
   b. In the next two drop-down lists, define the time by selecting the appropriate time zone and region.
   c. Under **Recurrence Pattern** , select how frequently FortiSIEM will connect to FortiSOAR to check FortiSOAR Playbooks. Choices are: **Once**, **Hourly**, **Daily**, **Weekly**, or **Monthly**.
   d. Click on the **Start Now** field, and enter or select the Month, Day, and Year when update(s) should occur. The format is `mm/dd/yyyy`.
   e. When done, click **Save**.

Machine Learning Jobs

Machine Learning Jobs are available through **ANALYTICS > Machine Learning**. You can access Machine Learning Jobs in **RESOURCES > Machine Learning Jobs**.

Viewing Machine Learning Jobs

Complete these steps to view existing Machine Learning (ML) Jobs.

1. Go to **RESOURCES** > **Machine Learning Jobs**.
2. Expand the **Machine Learning Jobs** folder on the left panel. If needed, select a category sub-folder under the Machine Learning Jobs folder to view other ML jobs.
3. To view a specific Machine Learning Job, select it and click **View**.

The following information is available for each Machine Learning Job from the main pane.

Column	Description
Enabled	If checked, the job is enabled to execute per its configured schedule.
Job ID	The Job ID
Name	The name of the job
Description	A description of the job
Algorithm	The algorithm used to create the model.
Parameters	The parameters used for the ML algorithm.
For Org	The organization(s) that the ML job belongs to.
Schedule	The schedule when the inference is run.
Action	Displays the actions taken when job is executed.
Scope	The organizational scope that the ML job belongs to.

If a Machine Learning Job is selected, there are two tabs available in the lower part of the main pane to provide more information on the selected Machine Learning Job.

Summary tab - Displays the Machine Learning Job information in a dedicated pane, with additional information.

Schedule Result tab - Displays the schedule history of the selected Machine Learning Job.

Editing a Machine Learning Job

To edit a Machine Learning (ML) Job, take the following steps.

1. Navigate to **RESOURCES > Machine Learning Jobs**.
2. Select the Machine Learning Job you wish to modify and click **Edit**.
   Note: You can select a Machine Learning Job category sub-folder (Anomaly Detection, Classification, Clustering, Forecasting, Regression) or Ungrouped sub-folder to locate other Machine Learning jobs.

3. Make any necessary changes to the available fields (**Job Name**, **Job Description**, **Inference Schedule**, **Re-training Schedule**, **Action**).
4. Click **Save**.

Deleting a Machine Learning Job

To delete an existing Machine Learning (ML) Job, take the following steps.

1. Navigate to **RESOURCES > Machine Learning Jobs**.
2. Select the Machine Learning Job you wish to delete and click **Delete**.
3. Click **Yes** to confirm.

Working with Cases

FortiSIEM allows you to create and assign cases for IT infrastructure tasks, and create tickets. You can see all tickets that have been created under the CASES tab and use filter controls to view tickets by assignees, organization, priority, and other attributes.

The following topics provide instructions for ticket related operations:

Creating a Ticket

FortiSIEM has a built-in ticketing system. A ticket can be created from the following:

- CASES tab
- INCIDENTS tab
- Via Incident Notification Policy

Creating a Ticket from the CASES Tab

To create a ticket from the CASES tab:

1. Go to **CASES**.
2. Click **New**.
3. In the **New Ticket** dialog box, enter the following information:

Settings	Guidelines
Summary	[Required] Summary information about the ticket.
State	State is automatically created by the system once the ticket is created. This can be modified from New to other values later.
Assignee	Click the edit icon to select a user from the list of Users.
Escalation	Escalation policy.
Priority	[Required] Priority of the ticket - High,

Settings	Guidelines
	Medium, or Low.
Due Date	Due date for the ticket.
Attachment	Click the edit icon to select and upload or delete any files related to the ticket.
CC	Email IDs to copy the ticket details to.
Notes	Any description of the ticket.

4. Click **Save**.
   A unique ID is automatically assigned to the ticket.
5. Select the ticket from the list to display tabs for the **Detail**, **Action History**, and **Evidence** information in the lower pane.

Creating a Ticket from the INCIDENTS Tab

To create a ticket from any specific Incident:

1. Go to **INCIDENTS** > **List View**.
2. Select the incident and click the **Actions** drop-down menu to select **Create Case**.
   The Incident details are automatically pulled to the new ticket creation window.
3. Enter the following information for the new ticket:

Settings	Guidelines
Assignee	Click the edit icon to select a user from the list of Users.
Priority	[Required] Priority of the ticket - High, Medium, or Low.
Due Date	Due date for the ticket.
Attachment	Click the edit icon to select and upload or delete any files related to the ticket.
CC	Email IDs of the users who will receive copies of the ticket details.

4. Click **Save**.

Creating a Ticket via Incident Notification Policy

To create a ticket automatically when an Incident triggers:

1. Go to **ADMIN** > **Settings** > **General** > **Notification Policy**.
2. Click **New** and select **Create Case when an incident is created**.
3. Click the edit icon for this setting and add the following details:

Settings	Guidelines
Escalation	Select an escalation policy from the drop-down list. See Escalation Settings.
Expires in	Time after which the ticket expires.
Priority	[Required] Priority of the ticket - High, Medium, or Low.
Assignee	Click the edit icon and assign this ticket to a user in the **Users** group. The user can belong to any Organization.

4. Click **Save**.

Editing a Ticket

The **Edit** option under **CASES** allows you to edit any ticket settings except the **Ticket ID**.

Complete these steps to edit an existing ticket:

1. Go to **CASES** and select a ticket to edit.
2. Click **Edit**.
3. In the **Edit Ticket** dialog box, modify the ticket information.
4. Click **Save**.
   The modified ticket appears in the table.

Managing Cases

You can perform the following operations from the CASES tab:

- Viewing a Ticket
- Searching a Ticket
- Escalating a Ticket
- Exporting a Ticket

Viewing a Ticket

The Ticket Dashboard displays the total number of:

- **New** - tickets in New state.
- **Assigned** - tickets that are Assigned.
- **High** - tickets in high priority state.
- **Overdue** - tickets that crossed the Due Date.
- **Late** - tickets that elapsed more than half of the Due Date but not yet overdue.
- **Closed** - tickets that are closed
- **MTTR** - mean time to repair

Understanding Ticket Settings

The **CASES** tab displays all of the tickets raised in the system in a tabular format with the following information:

Settings	Description
Elapsed	Percentage of time elapsed since the ticket was created. If the time is beyond Due Date, this field displays the "Overdue" status.
State	Current status of the ticket.
Priority	Priority of the ticket - High, Medium or Low.
Ticket ID	Unique ID assigned to the ticket automatically by the system during creation.
Organization	Organization of the reporting device.
Summary	Summary information about the ticket.
Incident ID	Unique ID of the incident in the incident database.
Assignee	User assigned to the ticket.
Creator	User who created the ticket.
Resolution Time	The time to resolve the incident in the external ticketing system.
Due Date	The date by which the ticket should be resolved.
Creation Date	Date when the ticket was created.

For any selected ticket, the Incident and event details are displayed in the **Detail** and **Action History** sections.

Settings	Description
Detail	
Assignee	The user to whom the ticket is assigned.
Close code	The reason for closing the ticket. Choose one of the following from the drop-down list: **Solved (Workaround)**, **Solved (Permanent)**, **Not Solved (Not Reproducible)**, **Not Solved (Expensive)**, **Closed (Resolved by Caller)**
Closed date	The date when the ticket was closed
Creator	User who created the ticket.
Escalation Policies	Escalation policy for the incident tickets.
Priority	The priority assigned tothe ticket: LOW, MEDIUM, or HIGH.
State	Current status of the ticket.
Ticket ID	Unique ID assigned to the ticket automatically by the system during creation.
CC	Email address(es) of the users who will receive a copy of the ticket details.
Close Note	Any description you want to enter when closing the ticket.
Creation Date	Date when the ticket was created.
Elapsed	Percentage of time elapsed since the ticket was created. If the time is beyond Due Date, this field displays the "Overdue" status.
Incident ID	Unique ID of the incident in the incident database.
Resolution Time	The time when the ticket was resolved in the ticketing system.
Summary	Summary information about the ticket.

Settings	Description
Time Zone	The time zone in which the ticket was created.
Action History	
Incident Name	Name of the rule that triggered the incident.
Incident Target	IP or host name where the incident occurred.
Incident Detail	Event attributes that triggered the incident.
Incident ID	To find the events that triggered the incident for the Case, click **Triggering Events**.
Evidence	
Attachments	List of files related to the ticket.
Triggering Event	List of events that triggered the incident for the Case.

Viewing Incident Details

To see the incident details related to a ticket:

1. Go to the **CASES** tab.
2. Select the ticket from the list. You can find the Incident ID from the **Detail** section and the Incident name, target and details from the **Action History** section.
3. Click the **Incident ID** under **Detail** section to open the details under the **INCIDENTS** tab.

Viewing Events that Triggered the Incident

To see the events that triggered the Incident for a ticket:

1. Go to the **CASES** tab.
2. Select the ticket from the list.
3. Click **Action History-List**. The events appear in the **Case action** section. Or you can click **Evidence > Triggering Event** to view the event details.

Creating a Ticket Escalation Policy

To create a ticket escalation policy, follow the steps here.

Searching a Ticket

You can use various attributes mentioned in the table below from the search filter to find more information about any ticket.

Complete these steps to search a ticket:

1. Go to the **CASES** tab.
2. Click the **Add Filter** search field to select any known filter from the drop-down with reference to the table below.
3. Based on the selection, new fields appear including the condition and value fields.

Settings	Guidelines
Time Range	Search any ticket created during a specific time range. Use **LAST** to find the tickets from the last number of days, hours and/or minutes or **FROM** to choose a range of dates and time from the Calendar.
State	Select the state of the ticket from the drop-down list: New, Assigned, Closed, In Progress, or Reopened.
Elapsed	Search using the time elapsed since the ticket was created.
Assignee	Search any ticket by entering the assignee of the ticket.
Creator	Search any ticket using the creator of the ticket.
Priority	Search any ticket by entering the priority: High, Medium, or Low.
Organization	Search any ticket by entering the Organization to which the ticket applies.
Ticket ID	Search any ticket using the Ticket ID auto-generated by the system.
Incident ID	Search any ticket using the Incident ID associated with the ticket.
Summary	Search any ticket using any known information included in the Ticket Summary.

4. Select the check mark to display the results.
   The results are displayed in the table. Select any Ticket to display the **Detail** and **Action History** in the lower pane.

Escalating a Ticket

Complete these steps to escalate a ticket:

1. Go to the **CASES** tab.
2. Click the **Add Filter** search field to select and open a ticket using filters.
   The table displays the tickets matching the filter criteria.
3. Click **Edit** button to open the ticket settings.
4. Select the Escalation type from the drop-down and click **Save**.

Refer to Ticket Escalation Settings for more information about related settings.

Exporting a Ticket

You can export all or selected tickets using filters to a PDF or CSV report.

Complete these steps to export a ticket:

1. Go to the **CASES** tab.
2. Click **Add Filter** search field to search any ticket using filters.
   The table displays the tickets matching the filter criteria.
3. Select one or more tickets from the list and click the **Export** button.
4. In the **Export Report** dialog box, select the following:
   a. Report Option: Select **Summary for all tickets** or **Detailed report for selected tickets**.
   b. User Notes (optional): Description related to the exported document.
   c. Output Format: PDF or CSV.
5. Click **Generate**.
   "Export Successful" message is displayed.
6. Click **View** to download and save the report.

Working with Incidents

When a correlation rule triggers, an incident is created in FortiSIEM. This section describes how to view and manage Incidents in FortiSIEM. There are six views:

- **Overview**: This view provides a "top down" view of the various types of Incidents and impacted hosts.
- **List View**: This tabular view enables the user to search incidents and take actions.
- **Risk View**: This view organizes impacted entities (Devices, Users) by Risk based on the triggered incidents.
- **Incident Explorer View**: This view helps users to correlate Actors (IP, Host, User) across multiple incidents, without creating multiple reports in separate tabs.
- **MITRE ATT&CK View**This view classifies security events detected by FortiSIEM into MITRE ATT&CK categories. You can select Information Technology (**IT**) or Industrial Control Systems (**ICS**) MITRE ATT&CK view.
  Note: Previously this was Attack View.
- **UEBA View**: This view monitors the AI alerts obtained from FortiInsight.

To interact with an incident, see Acting on Incidents.

FortiSIEM can cross-correlate incident data and perform lookups on selected external ticketing/work flow systems. See Filtering in the Incident Explorer View and Lookups Via External Websites.

FortiSIEM can also be configured to collect this host vulnerability data to preform CVE-Based IPS False Positive Analysis.

Overview View

The Overview view provides a "top down" view of various types of Incidents and impacted hosts. Go to **INCIDENTS** > **Overview** to see this view. Overview can set as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list and **Overview** from the **Incident Home** drop-down list.

The panel is divided into three sections:

- **Incidents by Category** – displays Incident Counts By Function and Severity.
- **Top Incidents** – displays the Top Incidents sorted first by Severity and then Count.
- **Top Impacted Hosts** – displays Top impacted hosts by Severity or Risk Score.

To change the incident time range, choose the **Time Range** option on the top right. For Service provider installations, choose the appropriate Organizations on top right. By default, the data combined for all Organizations and the Organization is shown next to each host. This view will automatically refresh every minute by default. The refresh menu on top bar allows the user to disable the automatic refresh or choose a different refresh interval.

Incidents by Category

This pane shows the number of unique Security, Performance, Availability, and Change incidents that have triggered in the specified time range.

To drill into a specific category, click the number and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described in Incidents List View.

Top Incidents

This pane shows the Top Incidents, first by Severity and then by Count.

- Each box represents an Incident.
- The color of the box title reflects the Incident Severity.
- The number reflects the unique incidents that has triggered in the chosen time window.
- The entries inside the box represent the IP address and host names appearing in either the Incident Source or Incident Target.
- Boxes are ordered left to right by Incident Severity and then unique incident count. That means that Red colored boxes (High Severity) appear first, then Yellow (Medium Severity), and finally Green (Low Severity). Within boxes of the same color, boxes with a higher number of Incident counts appear first. You can scroll to the right.

To drill down, click the number in the left side bar or each host and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described in Incidents List View.

Top Impacted Hosts by Severity

This pane shows the Top Impacted Hosts, first by Severity and then by Count.

- Each box represents an impacted host (where an Incident has occurred during the specified time window).
- The color of the box title reflects the maximum of Severity over all Incidents.
- The number on the left of the box reflects the unique incidents that have triggered on the host in the chosen time window.
- The entries inside the box represent the incidents that have triggered for that host.
- Boxes are ordered left to right by Incident Severity and then unique incident count. That means that the Red colored boxes (High Severity) appear first, then Yellow (Medium Severity), and finally Green (Low Severity). Within boxes of the same color, boxes with a higher number of Incident counts appear first. You can scroll to the right.

To drill down, click the number in the left side bar or each incident and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described in Incidents List View.

Top Impacted Hosts by Risk Score

This pane shows the Top Impacted Hosts, first by Risk Score.

- Each Box represents an impacted host (where an Incident has occurred during the specified time window).
- The color of the box title reflects the Risk Score (80 and above is Red, 50-79 is Yellow, and less than 50 is Green).
- The number on the left of the box reflects the risk score.
- The entries inside the box represent the incidents that have triggered for that host.
- Boxes are ordered left to right by Risk Score. That means that Red colored boxes (High Risk) appear first, then Yellow colored boxes (Medium Risk), and Green colored boxes (Low Risk).
- You can scroll to the right.

To drill down, click the number in the left side bar or each incident and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described in Incidents List View.

List View

This tabular view enables the user to search incidents and take actions.

- Viewing Incidents
- Acting on Incidents

Additional Incident related information: Automated Incident Resolution Recommendation

Viewing Incidents

To see this view, click **INCIDENTS** in the FortiSIEM header. By default, the **List by Time** view opens. The **INCIDENTS** view also allows you to filter data by device and by incident.

You can set **INCIDENTS** as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list. You can filter the **INCIDENTS** view further by choosing **List – by Time**, **List – by Device**, or **List – by Incident** from the **Incident Home** drop down list.

An incident's status can be one of the following:

- **Active**: An ongoing incident.
- **Manually Cleared**: Cleared manually by a user - the incident is no longer active.
- **Auto Cleared**: Automatically cleared by the system when the rule clearing condition is met. Rule clearance logic can be set in the rule definition.
- **System Cleared**: Cleared by the system. All non-security related incidents are cleared from the system every night at midnight local time, and will show a status of **System Cleared**.
- **Externally Cleared**: Cleared in the external ticketing system.

The resolution for an incident can be:

- **Open**
- **True Positive**, or
- **False Positive**

When an **Incident Status** is **Active**, Incident Resolution is **Open**. When an Incident is **Cleared**, then the user can set the **Incident Resolution** to be **True Positive** or **False Positive**. If you are changing the **Incident Resolution** to be **True Positive** or **False Positive**, then you must **Clear** the Incident.

The following sections describe the three views that are available through the **INCIDENTS** view:

- List by Time View
- List by Device View
- List by Incident View

List by Time View

The **List by Time** view displays a table of the incidents which have been active in the last 2 hours. The **Last Occurred** column contains the incidents sorted by time, with the most recent first. By default, the view refreshes automatically every minute. The refresh menu on the top bar allows the user to disable automatic refresh or choose a different refresh interval.

Unique to the **List by Time** view is a list of five time range buttons (15m 1h 1d 7d 30d) which appear above the paginator. They allow you to filter data by the last 15 minutes, 1 hour, 1 day, 7 days, or 30 days.

The following attributes are shown for each incident:

- Severity - High (Red), MEDIUM (Yellow), or LOW (Green).
- Last Occurred - last time this incident occurred.
- Incident - name of the incident.
- Tactics - name of the tactic involved with the incident.
- Technique - name of the technique involved with the incident.
- Reporting - set of devices that is reporting the incident.
- Source - source of the incident (host name or IP address).
- Target - target of the incident (host name or IP address or user).
- Detail - other incident details, for example, Counts, Average CPU utilization, file name, and so on.

To see the incident details, click the incident. A bottom panel appears that shows more details about the incident:

- **Details** - includes the full list of incident attributes that are not shown in the top pane.

Column	Description
Biz Service	Impacted biz services to which either the incident source or target belongs.
Category	Category of incidents triggered.
Cleared Reason	For manually cleared incidents, this displays the reason the incident was cleared.
Cleared Time	Time when the incident was cleared.
Cleared User	User who cleared the incident.
Count	Number of times this incident has occurred with the same incident source and target criteria.
Detail	Event attributes that triggered the incident.
Event Type	Event type associated with this incident. All incidents with the same name have the same Incident Type.
External Cleared Time	Time when the incident was resolved in an external ticketing system.
External Resolve Time	Resolution time in an external ticketing system.
External Ticket ID	ID of a ticket in an external ticketing system such as ServiceNow, ConnectWise, etc.

Column	Description
External Ticket State	State of a ticket in an external ticketing system.
External Ticket Type	Type of the external ticketing system (ServiceNow, ConnectWise, Salesforce, Remedy).
External User	External user assigned to a ticket in an external ticketing system.
First Occurred	The first time that the incident was triggered.
Incident	Name of the rule that triggered the incident. Use the drop-down list near the Incident if you must add this incident to filter.
Incident Comments	Comments added by the user.
Incident ID	Unique ID of the incident in the Incident database.
Incident Status	An incident's status can be one of the following: • **Active**: An ongoing incident. • **Manually Cleared**: Cleared manually by a user - the incident is no longer active. • **Auto Cleared**: Automatically cleared by the system when the rule clearing condition is met. Rule clearance logic can be set in the rule definition. • **System Cleared**: Cleared by the system. All non-security related incidents are cleared from the system every night at midnight local time, and will show a status of **System Cleared**. • **Externally Cleared**: Cleared in the external ticketing system.
Incident Title	A system default title or a user-defined title for an incident.
Last Occurred	The last time when the incident was triggered.
Notification Recipients	User who was notified about the incident.
Notification Status	Status of the Notification: Success or Fail.
Organization	Organization of the reporting device (for Service Provider installations).
Reporting	Reporting device.
Reporting Device Status	Status of the device: Approved or Pending. You must approve devices for the incidents to trigger, but they will still be monitored.
Reporting IP	IP addresses of the devices reporting the incident.

Column	Description
Resolution	The resolution for an incident can be: • **Open** (not defined or not known whether the incident is True Positive or False Positive) • **True Positive**, or • **False Positive** When an **Incident Status** is **Active**, Incident Resolution is **Open**. When an Incident is **Cleared**, then the user can set the **Incident Resolution** to be **True Positive** or **False Positive**. If you are changing the **Incident Resolution** to be **True Positive** or **False Positive**, then you must **Clear** the Incident.
Severity	Incident Severity is an integer in the range 0-10 (0-4 is set as Low, 5-8 as Medium, and 9-10 as High).
Severity Category	Incident Severity Category: High, Medium or Low.
Source	Source IP or host name that triggered the incident.
Subcategory	Subcategory of the triggered incident. To add custom subcategories to an incident category, see here.
Tactics	Name of the tactics involved with the incident.
Tag	Name of the tag involved with the rule that triggered the incident.
Target	IP or host name where the incident occurred.
Technique	Name of the technique involved with the incident.
Ticket ID	ID of the ticket if created in FortiSIEM.
Ticket Status	Status of any tickets associated with the incident.
Ticket User	User assigned to a ticket if created in FortiSIEM.
View Status	Whether the Incident has been Read or Not.

- **Events** - this displays the set of events that triggered the incident. If an incident involves multiple sub-patterns, select the sub-pattern to see the events belonging to that sub-pattern. For **Raw Event Log** column, click **Show Details** from the drop-down to see the parsed fields for that event.
- **Rule** - this displays the **Definition of Rule that Triggered the Incident** and the **Triggered Event Attributes**.

To close the incident details pane, click the highlighted incident.

List by Device View

The upper pane of the **List by Device** view lists the devices that are experiencing incidents. In the list, the device can be identified by either an IP or a host name. The name of the device is followed by the number of incidents in parentheses. Click the device name to see the incidents associated with the device. The lower portion of the view contains the same features and functionality as the **List by Time** view.

List by Incident View

The upper pane of the **List by Incident** view lists the incidents detected by FortiSIEM. The name of the incident is followed by the number of incidents in parentheses. Click the incident name to see the incidents associated with the device. The lower portion of the view contains the same features and functionality as the **List by Time** view.

Acting on Incidents

The **Actions** menu provides a list of actions that can be taken on incidents. To see a Location View of the incidents, select **Locations** from the **Actions** menu. FortiSIEM has a built in database of locations of public IP addresses. Private IP address locations can be defined in **ADMIN** > **Settings** > **Discovery** > **Location**.

To change the incident attribute display columns in the List View, select **Change Display Columns** from the **Actions** menu, select the desired attributes and click **Close**.

You can perform the following operations using the **Actions** menu:

- Changing the Severity of an Incident
- Searching Incidents
- Searching for MITRE ATT&CK Incidents
- Clearing One or More Incidents
- Clearing All Incidents from the Incident View
- Disabling One or More Rules
- Adding or Editing Comments for One or More Incidents
- Exporting One or More Incidents into a PDF, RTF, or CSV File
- Fine Tuning a Rule Triggering an Incident
- Creating an Exception for the Rule
- Creating Event Dropping Rules
- Creating a Ticket
- Emailing Incidents
- Executing a Playbook
- Running a Connector
- Creating a Remediation Action
- Resolve Incident
- Running an External Integration
- Show Case History
- Investigate

Changing the Severity of an Incident

1. Select the incident.
2. Select **Change Severity** from the **Actions** menu.
3. Select **Change to HIGH**, **MEDIUM**, or **LOW**.

Searching Incidents

1. Select **Search** from the **Actions** menu.
2. In the left pane, click an Incident attribute (for example, Function). All possible values of the selected attribute with a count next to it is shown (for example, Security, Availability and Performance for Function).
3. Select any value (for example, Performance) and the right pane updates with the relevant incidents.
4. Click and select other Incident Attributes to refine the Search or click **X** to cancel the selection.

Changing the Time Range for the Search

1. Select **Search** from the **Actions** menu.
2. Near the top of the left panel, click the time value.
3. Click **Relative** or **Absolute**:
   - If you click **Relative**, adjust the time value in the **Last** field.
   - If you click **Absolute** enter a time range. If you select **Always Prior**, enter a time period prior to the current time.

Saving the Search Criteria

Once you have performed your search, follow these steps to save the search criteria:

1. Click the **Save** icon (💾)which appears above the list of incident attributes, and to the right of **Search**.
2. In the **Save Search Filter under by Time as** dialog box, enter a name for the filter or accept the default. The default will be a time stamp value such as `Search Filters - 12/17/2019 17:04:59`.

The filter will appear in the **Search** (🔍 Search ▾) drop-down list, for example:

- When saving a filter based on the List by Time View, it displays in the **Search** drop-down list.
- When saving a filter based on the List by Device View, it displays in the **Search** drop-down list.
- When saving a filter based on the List by Incident View, it displays in the **Search** drop-down list.

Searching for MITRE ATT&CK Incidents

To find incidents that fall into any of the MITRE ATT&CK categories, follow these steps:

1. Select **Search**from the **Actions** menu.
2. Click **Tactics** or **Technique** in the left pane.
   The total number of security incidents will appear under the selected MITRE ATT&CK category.
3. Select one or more checkboxes next to the categories of interest.
   The incidents associated with the category are displayed.

For more information on MITRE ATT&CK views and MITRE ATT&CK categories, see MITRE ATT&CK View.

Clearing One or More Incidents

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold the **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Clear Incident** from the **Actions** menu.

5. Select whether the **Resolution** is **True Positive** or **False Positive**.
6. Enter a **Reason** for clearing.
7. Click **OK**.

Clearing All Incidents from the Incident View

You can remove all occurrences of selected incidents from the Incident View. This action can potentially span multiple pages.

1. Search for specific incidents and move them into the right pane.
2. Select **Clear All Incidents in View** from the **Actions** menu.
3. Select whether the **Resolution** is **True Positive** or **False Positive**.
4. Enter a **Reason** for clearing.
5. Click **OK**.

Disabling One or More Rules

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold the **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Disable Rule** from the **Actions** menu.
5. For Service Provider installations, select the Organizations for which to disable the rule.
6. Click **OK**.

Adding or Editing Comments for One or More Incidents

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold the **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Edit Comment** from the **Actions** menu.
5. Enter or edit the comment in the edit box.
6. Click **OK**.

Exporting One or More Incidents into a PDF, RTF or CSV File

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold the **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Export** from the **Actions** menu.
5. Enter or edit the comment in the edit box.
6. Select the **Output Format** and **Maximum Rows**.
7. Click **Generate**.
   A file will be downloaded in your browser.

Fine Tuning a Rule Triggering an Incident

1. Select an incident.
2. Select **Edit Rule** from the **Actions** menu.
3. In the **Edit Rule** dialog box, make the required changes.
4. Click **OK**.

Creating an Exception for the Rule

1. Select an incident.
2. Select **Edit Rule Exception** from the **Actions** menu.
3. In the **Edit Rule Exception** dialog box, make the required changes:
   a. For Service provider deployments, select the Organizations for which the exception will apply.
   b. Select the exception criteria:
      i. For incident attribute based exceptions, select the incident attributes for which rule will not trigger.
      ii. For time based exceptions, select the time for which rule will not trigger.
      iii. Select AND/OR between the two criteria.
      iv. Add Notes.
   c. Click **Save**.

Creating Event Dropping Rules

Event Dropping Rules may need to be created to prevent an incident from triggering. To create such a rule:

1. Select an incident.
2. Select **Event Dropping Rule** from the **Actions** menu.
3. In the **Event Dropping Rule** dialog box, enter the event dropping criteria:
   a. **Organization** - For Service provider deployments, select the organizations for which the exception will apply.
   b. **Reporting Device** - Select the device whose reported events will be dropped.
   c. **Event Type** - Select the matching event types.
   d. **Source IP** - Select the matching source IP address in the event.
   e. **Destination IP** - Select the matching destination IP address in the event.
   f. **Action** - Choose to drop the events completely or store them in the event database. If you store events, you can select the following actions:
      - Do not trigger rules
      - Drop attributes (Click the edit icon to open the selection window and select the attributes to drop)
   g. **Regex filter** - Select a regex filter to match the raw event log.
   h. **Description** - Add a description for the drop rule.
4. Click **Save**.
   The Rule will be appear in **ADMIN** > **Settings** > **Event Handling** > **Dropping**.

Creating a Ticket

See Creating a ticket from the INCIDENTS tab.

Emailing Incidents

Incidents can be emailed to one or more recipients. Make sure that Email settings are defined in **ADMIN** > **Settings** > **System** > **Email**. Note that email notification from the Incident page is somewhat ad hoc and must be manually setup by the user after the incident has triggered. To define an automatic notification, create an Incident Notification Policy in **ADMIN** > **Settings** > **Notification Policy**. To email one or more incidents on demand:

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Notify via Email** from the **Actions** menu and enter the following information:
   a. Send To – a list of receiver email addresses, separated by commas.
   b. Email template – Choose an email template. You can use the default email template, or create your own in **ADMIN** > **Settings** > **System** > **Email** > **Incident Email Template**.

Creating a Remediation Action

Incidents can be mitigated by deploying a mitigation script, for example, blocking an IP in a firewall or disabling a user in Active Directory. Note that this type of incident mitigation from the Incident page is somewhat ad hoc and must be manually setup by the user after the incident has triggered.

To define an automatic remediation, create an Incident Notification Policy in **ADMIN > Settings > General > Notification Policy**. Click **New**, and in the Notification Policy dialog box, select **Run Remediation/Script** in the **Action** section. To create a remediation action:

1. Select an incident.
2. Select **Remediate Incident** from the **Actions** menu.
3. Choose the **Enforce On** devices – the script will run on those devices. Make sure that FortiSIEM has working credentials for these devices defined in **ADMIN** > **Setup** > **Credentials**.
4. Choose the **Remediation** script from the drop-down menu.
   Note: Some Remediation scripts, such as FortiGate/Forti iOS version 7.0 and higher require a **VDOM**. Enter a Virtual Domain (VDOM) in the **VDOM** field for these particular scripts. Be aware that this field is case sensitive, so the VDOM must be entered exactly as it is named.
5. Choose the node on which the remediation will **Run On** from the drop-down list.
6. Click **Run**. If the user does not have permission to run remediation, a Create New Request window will appear. Take the following actions:
7. In the **Approver** drop-down list, select an approver. Fortinet recommends selecting all approvers to better ensure a response.
8. In the **Type** drop-down list, ensure Remediation Request is selected.
9. In the **Justification** field, enter an explanation why you want to run a remediation.
10. Click **Submit**. An email with the your request will be sent to all selected approvers. Approvers will receive a pending task notification in the FortiSIEM console, where they can resolve the request.
11. If you receive an email with an approval, repeat steps 1 through 6 before the expiration. If you received a rejection or received approval that has expired, repeat steps 1-10 if you wish to try again.

Resolve Incident

You can directly resolve an incident by taking the following actions.

1. Select the incident.
2. From the **Actions** drop-down list, select **Resolve Incident**.
3. Select the resolution (Open, In Progress, True Positive, False Positive).
4. Click **OK**.

Running an External Integration

Incidents can be handled by an existing external integration policy configured through FortiSIEM.

To create an external integration policy, navigate to **ADMIN > Settings > General > External Settings**. Click **New** to begin creating an external integration. For more information, see Configuring External Integration.

To run an external integration policy, take the following steps:

1. Select an incident.
2. Select **Run External Integration...** from the **Actions** menu.
3. From the **Choose Integration Policy** window, select the existing Integration Policy you want applied to the incident from the drop-down list.
4. When done, click **OK**.

Show Case History

Note: Prior to FortiSIEM 7.0.0, this was **Show Ticket History**.

1. Select an incident.
2. Select **Show Case History** from the **Actions** menu.
3. The Ticket History dialog box opens and displays the following information:

Field	Description
Detail:	
Incident ID	The unique ID of the incident in the incident database.
Due Date	The date by which the ticket should be resolved.
Escalation Policy	The escalation policy defined for the incident.
Attachment	The list of files related to the incident.
Action History:	
Created at	The time when the incident was created.
Incident Name	The name of the rule that triggered the incident.

Field	Description
Incident Target	The IP or host name where the incident occurred.
Incident Detail	The event attributes that triggered the incident.
Incident ID	The unique ID of the incident in the incident database.

Investigate

1. Select an incident.
2. Select **Investigate** from the **Actions** menu.

You will be taken the **Analytics > Investigation** page. See Investigating Incidents.

Risk View

Risk view displays the Entities (Devices and Users) ordered by Risk. Risk is calculated based on the triggering incidents using a proprietary algorithm that incorporates asset criticality, incident severity, frequency of incident occurrence, and vulnerabilities found. Risk is only computed for devices in CMDB, private IP addresses, and users found in logs or discovered via LDAP.

Go to **INCIDENTS** > **Risk** to see this view. Risk can set as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list and **Risk** from the **Incident Home** drop-down list.

Devices and Users are categorized by Risk as follows:

- Devices - number of devices with Risk
- Users - number of users with Risk
- High Risk - number of devices and users with high risk
- Medium Risk - number of devices and users with medium risk
- Low Risk - number of devices and users with low risk

To see only the above categories of devices and users in the Risk View, click any of the five categories above.

The Risk View displays the following:

- Entity (Device or User name)
- Current Risk - Current value, up or down versus the same period
- 24 Hour Risk Trend (1 day trend)
- Incidents in Last 24 hours (1 day)

To drill down, click one row and the incidents that led to this risk are shown in a time line format. You can select an incident, and select any action from the **Actions** menu. The actions are similar to those described for the List View.

An Entity (Device or User) can be selected. When selected, the Risk View page expands to three panes that provide more information on the selected object. To go back to the main Risk View, click on **<** in the left pane.

Pane Information

Left Pane for Device

If a device is selected, in the left pane, the following tabs are available:

- General - The name of the device, its access IP, device type, version, importance, and additional description are displayed if available.
- Discovery Status - Discovery information for the device is displayed, which includes its creation date, last discovered date, and last update.
- Collection Status - Information collected from the device is displayed, which includes uptime.
- Member of # Group - Any groups that the device is a member of is displayed.
- Properties - Any custom defined properties are listed here.
- Software - Installed Software, Running Applications, Windows Services, Installed Patches. Click on a specific property for more information.
- Hardware - Interfaces, Processors, Storage, Components. Click on a specific property for more information.

Left Pane for User

If a user is selected, in the left pane, the following tabs are available:

- General - User information, such as user name, full name, job title, company, domain, and last domain where the user was logged on is displayed.
- Advanced - Information such as when the domain password was last set, the age of the domain password, system role, and user lockout time is displayed.
  Note: The information that appears here is also provided under **CMDB > Users > Summary > Advanced**.
- Contact - User contact information is displayed, which can include work phone number, mobile phone number, email address, and physical address.
- Member of # Groups - Any groups that the user is a member of is displayed.

Middle Pane For Device and User

In the middle pane, information on incidents and activities is displayed for the device or user.

A Time Range drop-down selector is available to adjust the time range. Additionally, a Refresh button is available to update information from the middle pane.

- Current Risk Score
- Risk Score and Incident Trend graph - The color of a circle represents its event severity (Red: High Severity, Yellow: Medium Severity, Green: Low Severity). The size of the circle represents the incident count.
  Note: In the case of incident overlap, the color will blend, i.e. a high severity and medium severity incident that occurred at the same time would appear as dark orange.

- Incident Timeline
- Overview by Incident Category - Information from triggered incidents are shown by category and severity. Categories are Security, Performance, Availability, Change, and Other.
  Note: This information is the same as that provided by the incident trend report.
- Incidents and Activity Timeline - Incidents are shown by timeline by default. Click the **Show Activities** checkbox to load activities. Once the data is loaded, this section will show a combination of occurred incidents and activities ordered by the occurred time. Incidents are color coded, and also have a notification (bell) icon next to them.

Timeline	Description
Incident	In the timeline, incident status, its name, and number of occurrences including date and time are shown. The incident's name is also color coded to indicate its severity. Links for **Details**, **Triggering Events** (Rules that triggered the event), **Investigate**(for more information on Investigate, see Investigating Incidents), and **Other Actions** are available (for more information on Actions, see Acting on Incidents).
Activity	In the timeline, the activity name, occurrences, and the user who did the activity are displayed. An **Event Details** link provides the raw messages related to the activity when clicked.

Right Pane for Device

The right pane contains a few pre-defined report widgets to provide an overview for the device.

Device Dashboards

- Successful and Failed Logins - Displays the number of successful and failed logins as a graph.
- Top Users by Failed Login - Displays the most frequent users with failed logins as a graph.
- Top Users by Successful Login Type and Count - Displays the most frequent users with successful logins as a graph.
- Top Security Event Types - Displays the most frequent security event types as a graph.
- System CPU and Memory - Displays the system CPU and memory usage as a graph.
- Top Processes by CPU - Displays the most used processes used by the CPU as a graph.
- Top Processes by Memory - Displays the most used processes using memory as a graph.

Right Pane for User

The right pane contains a few pre-defined report widgets to provide an overview for the user.

User Dashboards

- Top User Actions - Displays the top user's actions taken for the time range configured as a graph.
- Top Actions on User Account - Displays the top actions for the user account as a graph.
- Host Logon Activity - Displays the user's logon activities as a graph.
- Successful and Failed Logins - Displays the user's number of successful and failed logins as a graph.

Explorer View

The Incident Explorer view allows you to correlate Actors (IP, Host, User) across multiple incidents, without creating multiple reports in separate tabs. Incident trends, Actor and Incident detail are displayed on the same page. You can choose an actor and see all the incidents that actor is part of. You can then choose a time range and narrow down the incidents. Time ranges, Actors, and Incidents can be chosen in any order. Each time a selection is made, the rest of the dashboard updates to reflect that selection.

To open the Incident Explorer view, click **INCIDENTS**, then click the Explorer icon (📊 Explorer). Explorer can set as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list and **Explorer** from the **Incident Home** drop-down list.

The Incident Explorer view is divided into three layers:

- The top layer displays the Incident Trend graph. The graph displays the incident counts over time, organized by severity, then by count.
  Each bar in the graph represents the number of incidents at a given time. The colors used in the bars reflects the Incident Severity. Red colored boxes (High Severity) appear first then Yellow (Medium Severity), and finally Green (Low Severity). The numbers in the bars reflect the number of unique incidents that triggered in the chosen time window.
- The middle layer displays panels for Incidents, Hosts, IPs, and Users. You can filter the items in the panels by Category, Status, and Time Range. See “Filtering in the Incident Explorer” for more information.
- The bottom layer displays the Incidents Table with these headings: Severity, Last Occurred, Incident, Reporting, Source, Target, Detail, Incident Status, and Resolution. Click an incident row to get more detail.
  Drill down is available from the Reporting, Target, Detail, Resolution columns.

The following tables describe the drill down options available for each column.

Reporting Options

Option	Description
Quick Info	Displays the quick information about the device.
Device Health	Availability, Performance, and Security health reports for the device.
Related Incidents	Switches to List view and displays related incidents.
Add to Filter	Switches to List view. Open the drop-down list next to the Reporting column for the desired incident and select **Add to Filter**. Add to Filter modifies the search on the current tab by including this constraint.

Target Options

Option	Description
Quick Info	Displays the quick information about the device.
External Lookup	Looks up external threat intelligence websites about likely malicious Indicators of Compromise (IOCs).
Device Health	Availability, Performance, and Security health reports for the device.
Related Incidents	Switches to List view and displays related incidents.
Related Real Time Events	Switches to the **ANALYTICS** tab and displays related real time events.
Related Historical Events	Switches to the **ANALYTICS** tab and displays related historical events.
Add to Filter	Switches to List view. Open the drop-down list next to the **Reporting** column for the desired incident and select **Add to Filter**. **Add to Filter** modifies the search on the current tab by including this constraint.
Add to Application Group	Opens the IP Application Group Mapping Definition dialog box where you can choose the group where you want to add the incident.

Detail Options

Displays other incident details, such as Counts, Average CPU utilization, file name, and so on.

Resolution Options

Option	Description
Set Resolution to Open	Sets the resolution status to Open (not defined or not known whether the incident is True Positive or False Positive).
Set Resolution to True Positive	Sets the incident resolution status to True Positive.
Set Resolution to False Positive	Sets the incident resolution status to False Positive. If you are changing the Resolution to False Positive, you must clear the incident at the same time.

To leave the Incident Explorer View, click the **List** icon or select **Actions > Show in Incident List View**, if an incident is already selected.

Using the Incident Explorer View

Click any of the bars in the **Incident Trend** graph. The corresponding Incidents, IP addresses, Hosts and Users are displayed in the panels. The corresponding incidents are also displayed in the **Incident Table**.

Click any of the items in the Incident, IP, Host, or User panels. The corresponding bar is displayed in the **Incident Trend** graph and corresponding incidents are displayed in the **Incident Table**.

Click multiple items in the **Incident Trend** graph and in the panels. Your selections will be ANDed together and the results displayed in the **Incident Table**.

Click any incident in the **Incident Table**. Details on the event that triggered the incident will open beneath the **Incident Table**.

Filtering in the Incident Explorer View

You can filter the incident data by incident category, whether the incident is active or cleared, and the time range when the incident occurred.

- The **Category** drop–down list allows you to filter on unique **Security**, **Performance**, **Availability**, and **Change** incidents that have triggered in the specified time range.

  In order for any Incident to show up on this list, the rule must be configured to be one of the 4 unique categories above (Security, Performance, Availability, Change). Incidents that trigger outside of the above 4 Categories will not show up (eg. Other).

- The **Status** drop-down list allows you to filter on **Active** and/or **Cleared** incidents.
- The **Time Range** dialog box allows you to choose a relative or absolute time range. For **Relative**, enter a numerical value and then either **Minutes**, **Hours**, or **Days** from the drop-down list. For **Absolute**, use the calendar dialog to specify **From** and **To** dates.

MITRE ATT&CK® View

MITRE ATT&CK view provides Information Technology (**IT**) and Industrial Control Systems (**ICS** view summaries by selecting **IT** or **ICS** prior to the following available types of views.

- Rule Coverage View
- Incident Coverage View
- MITRE ATT&CK Incident Explorer View

Rule Coverage View

The Rule Coverage View provides an overview of the tactics and techniques that FortiSIEM covers as defined by MITRE Corporation. Go to **INCIDENTS** > **MITRE ATT&CK®** > **[IT** or **ICS]** > **Rule Coverage** to see this view. Rule Coverage can be set as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list and **MITRE ATT&CK - Rule Coverage** from the **Incident Home** drop-down list.

The ICS and IT Attack (Tactic Categories) are available.

- ICS Attack (Tactic Categories) Table
- IT Attack (Tactic Categories) Table

ICS Attack (Tactic Categories) Table

The following table briefly describes the ICS attack (tactic) categories. See https://attack.mitre.org/tactics/ics/ for more detailed information.

Category (Tactic)	Description
Initial Access	The adversary is trying to get into your network.
Execution	The adversary is trying to run malicious code.
Persistence	The adversary is trying to maintain their foothold.
Privilege Escalation	The adversary is trying to gain higher-level permissions.
Evasion	The adversary is trying to avoid security defenses.
Discovery	The adversary is trying to figure out your environment.
Lateral Movement	The adversary is trying to move through your environment.
Collection	The adversary is trying to gather data of interest to their goal.
Command and Control	The adversary is trying to communicate with compromised systems to control them.
Inhibit Response Function	The adversary is trying to prevent your safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state.
Impair Process Control	The adversary is trying to manipulate, disable, or damage physical control processes.
Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

IT Attack (Tactic Categories) Table

The following table briefly describes the IT attack (tactic) categories. See https://attack.mitre.org/matrices/enterprise/ for more detailed information.

Category (Tactic)	Description
Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
Resource Development	The adversary is trying to establish resources they can use to support operations.
Initial Access	The adversary is trying to get into your network.
Execution	The adversary is trying to run malicious code.
Persistence	The adversary is trying to maintain their foothold.
Privilege Escalation	The adversary is trying to gain higher-level permissions.
Defense Evasion	The adversary is trying to avoid being detected.
Credential Access	The adversary is trying to steal account names and passwords.
Discovery	The adversary is trying to figure out your environment.
Lateral Movement	The adversary is trying to move through your environment.
Collection	The adversary is trying to gather data of interest to their goal.
Command and Control	The adversary is trying to communicate with compromised systems to control them.
Exfiltration	The adversary is trying to steal data.
Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Using the Rule Coverage View

To open the Rule Coverage View, go to **INCIDENTS** > **MITRE ATT&CK®** >**[IT** or **ICS]** > **Rule Coverage View**. The top row displays the number of rules and the percentage of MITRE techniques that FortiSIEM covers. In the main row header, the bolded number that appears under each tactic indicates the number of rules that are covered under it. Clicking a tactic here will show all the rules that belong to it. Each tactic cell also lists the number of major techniques (Tech) and sub-techniques (Sub-Tech) related to the involved tactic. All major techniques related to a tactic are listed underneath their respective tactic column. Tactics and techniques covered by FortiSIEM rules are indicated by a light yellow background. You can hover your mouse cursor over any major technique to view the following information:

- Total number of rules covered by the technique (security category)
- The number of rules covered by each sub-technique (if applicable)

Left clicking on any technique will bring up a small menu, allowing you to select **Detail** or **Show Rules**.

Clicking on **Detail** will provide you with details about the major techniques and sub-techniques.

Clicking on **Show Rules** will display all the rules associated with the specific technique as provided in the following table:

Note: Clicking a tactic displays the rules information for all related techniques.

Note 2: Click the Columns drop-down list to select which headings you want to display.

Heading	Description
Status	Provides information on whether a rule is enabled (checkmark), or is disabled ("X").
Name	The name of the rule is listed. You can left click on a rule to bring up the following selectable options: • **Show in Resources > Rule** - view/edit the selected rule on the Rules page. • **Rule Summary** - view the rule summary description.
Tactics	The tactic involved with the rule is listed here.
Techniques	The involved technique is listed here. You can click on the technique link to get detailed information from the attack.mitre.org site.
Description	Detailed information about the technique is provided here.
Exceptions	Any rule exceptions are listed here.

Searching Techniques in Rule Coverage View

A technique search field is available in the upper left corner. You can enter your query in the **Search technique...** field. Results are shown in real-time as you enter your query. A drop-down filter next to the **Search technique...** field is available. Your choices are:

- Show All - all techniques are highlighted. The "Show All" text appears when Show Covered and Show Not Covered are both selected.
- Show Covered - only techniques covered by FortiSIEM are displayed.
- Show Not Covered - only techniques not covered by FortiSIEM are displayed.

Incident Coverage View

The Incident Coverage View provides an overview of the security incidents detected by FortiSIEM that fall under the tactics and techniques as defined by MITRE Corporation. Go to **INCIDENTS** > **MITRE ATT&CK®** >**[IT** or **ICS]** > **Incident Coverage** to see this view. Incident Coverage can be set as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list and **MITRE ATT&CK - Incident Coverage** from the **Incident Home** drop-down list.

The table in Rule Coverage View briefly describes the attack (tactic) categories also shown in Incident Coverage View.

Using the Incident Coverage View

To open the Incident Coverage View, go to **INCIDENTS** > **MITRE ATT&CK®** > **[IT** or **ICS]** > **Incident Coverage View**.The top row displays the number of incidents detected by FortiSIEM in the time range specified. In the main row header, the bolded number that appears under each tactic indicates the number of incidents associated with a specific tactic. Clicking a tactic will show all related detected incidents. Each tactic cell also lists the number of major techniques (Tech) and sub-techniques (Sub-Tech) related to the involved tactic/incidents. All major techniques related to a tactic are listed underneath their respective tactic column. Tactics and techniques covered by FortiSIEM rules are indicated by a light yellow background. You can hover your mouse cursor over any major technique to view the following information:

- Total number of incidents triggered by this technique
- The number of incidents triggered by each sub-technique (if applicable)

Left clicking on any technique will bring up a small menu, allowing you to select **Detail** or **Show Incidents**.

Clicking on **Detail** will provide you with details about the major technique and sub-techniques.

Clicking on **Show Incidents** will display all the incidents associated with the specific technique. It also provides the following Incident information:

Note: Click the Columns drop-down list to select which headings you want to display.

Heading	Description
Severity Category	The severity/category of the incident is listed.
Last Occurred	The date and time when the incident last occurred is listed.
Event Type	The event type triggering the incident is displayed.
Incident	The event name of the incident is displayed. Clicking on it will bring up a drop-down list with the following options: • Show in Incident List View - displays the incident in Incident List View. • Rule Summary - displays the **Rule Pattern Definitions** that triggered the incident. • Triggering Events - displays the **Event Details** that triggered the event, including triggered event attributes.
Tactics	The tactic involved with the rule is listed here.
Technique	The involved technique is listed here. You can click on the technique link to get detailed information from the attack.mitre.org site.
Reporting	The device that reported the incident is listed.
Source	Source information from the triggered incident is listed. For example, the TCP/UDP Port

Heading	Description
	involved with a protocol tunneling technique is provided.
Target	The object targeted in the incident is listed. For example, the target user in a steal or forge kerberos tickets incident is listed.
Detail	Additional information about the incident is provided here. For example, the command involved, service involved, or registry key is listed, if relevant.
Incident ID	The incident ID is listed.

Searching Techniques in Incident Coverage View

A technique search field is available in the upper left corner. You can enter your query in the **Search technique...** field. Results are shown in real-time as you enter your query. A drop-down filter next to the **Search technique...** field is available. Your choices are:

- Show All - all techniques are displayed. The "Show All" text appears when Show Triggered and Show Not Triggered are both selected.
- Show Triggered - only techniques with triggered incidents are displayed.
- Show Not Triggered - only techniques with no triggered incidents are displayed.

Filtering in Incident Coverage View

You can filter the incident data by attack category, whether the incident is active or cleared, and the time range when the incident occurred.

- The **Status** drop-down list allows you to filter on **Active** and/or **Cleared** incidents.
- The **Time Range** dialog box allows you to choose a relative or absolute time range. For relative times, enter a numerical value and then either **Minutes**, **Hours**, or **Days** from the drop-down list. For absolute times, use the calendar dialog to specify **From** and **To** dates.
- For MSP deployments, the 👤 ▾ drop-down list allows you to filter incidents based on organizations.

MITRE ATT&CK Incident Explorer View

The MITRE ATT&CK Incident Explorer View maps security incidents detected by FortiSIEM into attack categories defined by MITRE Corporation (MITRE ATT&CK). Go to **INCIDENTS** > **MITRE ATT&CK®** > **[IT** or **ICS]** > **Incident Explorer** to see this view. The MITRE ATT&CK Incident Explorer can be set as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list and **MITRE ATT&CK - Incident Explorer** from the **Incident Home** drop-down list.

The table in Rule Coverage View briefly describes the attack (tactic) categories shown in MITRE ATT&CK Incident Explorer View.

Using the MITRE ATT&CK Incident Explorer View

To open the MITRE ATT&CK Incident Explorer View, go to **INCIDENTS** > **MITRE ATT&CK®** >**[IT** or **ICS]** > **Incident Explorer**. The table at the top of the MITRE ATT&CK Incident Explorer View displays the devices experiencing the security incidents and the MITRE ATT&CK categories into which the incidents fall. The circles in the table indicate:

- Number - The number in the middle of the circle indicates the number of incidents in that category. Click the number to get more detail on the incidents. See Getting Detailed Information on an Incident.
- Size - The size of the circle is relative to the number of incidents.
- Color - The color of the circle indicates the severity of the incident: Red=HIGH severity, Yellow=MEDIUM severity, and Green=LOW severity.

Filtering in the MITRE ATT&CK Incident Explorer View

You can filter the incident data by attack category, whether the incident is active or cleared, and the time range when the incident occurred.

- The **Tactics** drop–down list allows you to filter on one or more of the attack categories. You can also display **All** of the categories.
- The **Status** drop-down list allows you to filter on **Active** and/or **Cleared** incidents.
- The **Time Range** dialog box allows you to choose a relative or absolute time range. For relative times, enter a numerical value and then either **Minutes**, **Hours**, or **Days** from the drop-down list. For absolute times, use the calendar dialog to specify **From** and **To** dates.
- For MSP deployments, the 👤▾ drop-down list allows you to filter incidents based on organizations.

Getting Detailed Information on an Incident

The lower pane of the MITRE ATT&CK Incident Explorer View provides a table with more detailed information about a security incident. You can populate the table in any of these ways:

- Click a device to see all of the incidents associated with the device.
- Open the **Tactics** drop-down list and choose one of the attack categories. All of the incidents associated with the selected category or categories are displayed. You can also choose to display **All** of the categories.
- Click the number in the middle of the circle. All of the incidents associated with the selected device and category are displayed.

For more information on the column headings that appear in the lower pane of the Incident Explorer View, see Viewing Incidents.

Displaying Triggering Events for an Incident

Click an incident in the lower table to display its triggering events. Another pane opens below the Incident table. It displays information related to the event that triggered the incident, such as **Host Name**, **Host IP**, and so on.

UEBA View

The UEBA view monitors AI alerts obtained from FortiInsight. To configure what data appears in the UEBA view, see UEBA Settings. The UEBA view is divided into these layers:

- Incident Trend Chart
- Attribute List
- Related Incidents
- Triggering Events

The **Actions** drop-down list displays the operations you can perform on selected incidents. For descriptions of the operations, see Acting on Incidents.

Incidents in the UEBA View can be filtered by activity status or time range. See Filtering in the UEBA View.

Incident Trend Chart

The Incident Trend Chart displays frequency of incidents over time. You can click the bars in the chart to filter both the chart and the attribute list. The attribute lists will update based on the time and severity category of the bar.

Attribute List

The Attribute List table provides the following information about the AI alerts received from FortiInsight:

Attribute	Description
Incident	The name of the incident that was detected. The incident name is defined in Setting Tags.
Host	The host name or IP address where the alert originated.
Application	The name of the application that is the source of the incident.
User	The Windows Agent user. This user is specified in Setting UEBA Higher Risk Entities.
Tag	The tag used to categorize the alert. The tag is defined in Setting Tags.
Activity	The description of the activity which raised the alert.

Related Incidents

The Related Incidents table provides additional information on the incidents selected in the Attribute List table.

Attribute	Description
Severity Category	The severity of the incident: **HIGH**, **MEDIUM**, or **LOW**. You can change the severity value in the **Actions** drop-down list.
Last Occurred	The date and time when the incident was last detected.
Incident	The name of the incident.
Tag	The tag used to categorize the alert.
Host Name	The host name or IP address of the host where the alert originated.
User	The Windows Agent user.
Application	The name of the application that is the source of the incident.
Resource	A resource name, typically a file path.
Activity	The description of the activity which raised the alert.

Triggering Events

The **Triggering Events** layer is typically hidden. Click an incident in the **Related Incidents** table to display its triggering events.

These display options are available above the table:

- **Subpattern: FIN** - Indicates that only FIN events are displayed.
- **Wrap Raw Events** - Select to display the full log event in the table.
- **Show Event Type** - Select to display the event type only.
- **Show Raw Event Only** - Select to display the full log event only.

The following table describes incidents in the Triggering Events table.

Attribute	Description
Event Receive Time	The date and time when the event was received.
Host Name	The IP address or host name that was the source of the event.

Attribute	Description
Domain	The Windows domain that was the source of the event.
User	The Windows Agent user.
Tag Name	The tag used to categorize the alert.
Process Name	The name of the process producing the event.
Activity Name	The description of the activity which raised the alert.
Resource Name	A resource name, typically a file path.

Filtering in the UEBA View

Use the **Status** button in the upper right corner of the UEBA View to filter the display for active or cleared incidents, or both. Use the **Time Range** button to filter the display for incidents within a specific time range:

- **Status** - Use the drop-down list to display **Active** incidents, **Cleared** incidents, or both.
- **Time Range** - Filter the incidents according to a time range:
  - If you click **Relative**, adjust the time value in the **Last** field.
  - If you click **Absolute** enter a time range.

Automated Incident Resolution Recommendation

FortiSIEM provides 2 attributes to record Incident status:

1. **Incident Resolution**: None, True Positive, False Positive
2. **Incident Status**: Active, System Clear and Manually Cleared

When an Incident triggers, Incident Status is set to Active and Incident Resolution is set to None. There are 3 ways an Incident can get resolved:

1. If the Incident turns out to be a false positive, then the user can set Incident Resolution to False Positive and Incident Status to Manually Cleared.
2. The Incident may clear itself because of a clearing condition in the rule. In that case, Incident Resolution is set to True Positive and Incident Status is set to System Cleared.
3. The Incident may be a real issue. In that case, after working through the Issue, the user can set Incident Resolution to True Positive and Incident Status to Manually Cleared.

FortiSIEM uses a Machine Learning Classification algorithm to recommend Incident Resolution. First, it learns the Incident Resolution set by the user for Incidents over the previous 2 days. Then it recommends Incident Resolution for new Incidents as they occur. The algorithm runs daily at midnight (12AM) to cover Incidents over the last 2 days. Recommendation is done as follows:

1. Incident Resolution is set to True Positive or False Positive.
2. A new Incident attribute called Confidence (between 0 and 100) is set. A high confidence number implying high confidence on the result.
3. Incident Comment is updated with the comment "Resolution set by Machine Learning".

Notes:

1. Only Incident Resolution is set. Incident Status is not modified.
2. The Machine Learning algorithm always runs in the background and cannot be disabled. The algorithm uses a set of Incident attributes as features (including Event Receive Time, Event Type, Reporting Device, Source, Target, Category and MITRE Attack Technique) to make its recommendation.

Lookups Via External Websites (e.g. VirusTotal)

Indicators of Compromise (IOC) can be transmitted via external IPs, domain names, URLs, and file hashes.

When a security incident is triggered due to a potentially malicious IOC, you may want to consult an external threat intelligence website to get more information about the IOC. If the website can confidently say that the IOC is malware, then you can take corrective action, such as blocking the IOC. On the other hand, if the website says that the IOC is safe, then you can mark the IOC as a false positive.

There are two types of external lookups:

- Some websites accept an IOC as a parameter in the URL and the website will respond with information about the IOC. In many of these cases, the IOC information in the web page cannot be parsed programmatically, and user must manually determine whether the IOC is malware. For example, see https://www.talosintelligence.com/reputation_center/lookup?search=8.8.8.8.
- Other websites, such as VirusTotal, RiskIQ, and FortiGuard have APIs. FortiSIEM can analyze the data from these websites and present the results in an easily understandable format for user. **Note:** VirusTotal supports domain, URL, and file hash lookups. RiskIQ supports IP and domain lookups. FortiGuard supports IP, domain, URL and file hash lookups.

FortiSIEM supports all three types of lookups. External Website lookups can be performed only from the **Incident List View**.

Prerequisites

Complete these steps before performing external lookups:

1. External lookups that accept an IOC in the URL must be defined in **ADMIN > Settings > System > Lookup**. See Lookup Settings for more information.
2. VirusTotal, RiskIQ, and FortiGuard integrations must be defined in **ADMIN > Settings > General > External Integration**. This involves setting credentials.
   See VirusTotal Integration, RiskIQ Integration, and FortiGuard Integration for more information.

Performing an External Lookup on VirusTotal, RiskIQ, and/or FortiGuard

Follow these steps to perform an external lookup on VirusTotal, RiskIQ, and/or FortiGuard.

1. Go to **INCIDENTS** and click the **List** view.
2. Select an incident from the table.
3. Drill down on either the **Source**, **Target**, **Detail** or **Reporting IP** columns and choose **External Lookup**. FortiSIEM will identify IP, Domain, URL and file hash fields for lookup.
4. Choose one of the following and click **Lookup**.
   a. An External website that accepts IP in the URL
   b. **VirusTotal**, **RiskIQ**, and/or **FortiGuard**
5. For the first case (4a), the page opens in a different tab in the browser.
6. For the second case (4b), FortiSIEM collects information about the IOC from the websites using the API, makes a conclusion as to whether it is Safe/Malware/Not Sure, and presents the data in the **Result** tab.
7. If a FortiGuard result is determined to possibly be malicious, you can click on **Malicious** to get more details as to why FortiGuard flagged the incident as malicious.
8. Based on the information about the IOC, you can click on the **Action** tab and take any of the following actions.
   a. **Update Comment**: You can update Incident comment based on the website findings. Enter an optional comment about the incident and click **Add Summary**, then **Apply**. The comment will appear in the **Incident Comment** panel in the **Details** tab when you select the incident in the **List** view.
   b. **Resolve Incident**: You can resolve the incident. Choose **Open**, **True Positive**, **False Positive**, or In **Progress**. Click **Apply**, and the selection will appear in the Resolution column for that incident.
      - If you choose **False Positive**, you have the option of providing a reason for your choice. You also have the option to **Create a False Positive in ThreatConnect**. Clicking this option will respond with a message describing whether the creation was successful. This option assumes that you have created a malware configuration for ThreatConnect. You can configure IPs, domains, hash, or URLs for ThreatConnect. See Working with ThreatConnect IOCs.
   c. **Create Rule Exception**: If it is a false positive, then you can create a rule exception. Click the edit icon to create an exception to the rule. For more information on using the **Edit Rule Exception** dialog box, see Creating an exception for the rule.
   d. **Set Incident Severity**: You can change the incident severity. Open the drop-down list and choose **Change to LOW**, **Change to MEDIUM**, or **Change to HIGH**.
   e. **Remediate Incident**: You can remediate the Incident, e.g. block the malware domain. Click the edit icon to remediate the incident. For more information on using the **Run Remediation** feature, see Creating a Remediation action.
   f. **Run External Integration**: You can create a ticket in an external ticketing system. Click the edit icon to choose an integration policy from the drop-down list. Click **OK**.
9. Click **Close**.

CVE-Based IPS False Positive Analysis

Network Intrusion Prevention Sensors (IPS) trigger alerts based on network traffic. When an IPS sees traffic matching an attack signature, it generates an alert. Some of these attacks correspond to host vulnerabilities and have an associated CVE number. Most organizations run vulnerability scanning tools to scan their servers for vulnerabilities. If FortiSIEM is configured to collect this host vulnerability data, it can combine the IPS signature to CVE mapping, and Host to CVE mapping to detect if an IPS Alert is false positive.

Requirements

- Currently, FortiSIEM applies this logic on Incidents but not events. All important IPS events trigger some rule in FortiSIEM.
- FortiSIEM IPS rules must be written with a **Signature Id** and **Event Type** in the group by conditions. All built-in rules have been enhanced with this requirement starting with release 5.3.0.
- The primary source of IPS Signature to CVE mapping is FortiSIEM CMDB. These mappings are part of the FortiSIEM knowledge base and upgraded with every release. For FortiGate IPS signatures, FortiSIEM can also pull this information from FortiGuard Services via an API. The FortiGuard IOC license must be enabled in FortiSIEM.
- The source of Host to CVE mapping is Vulnerability scanners. FortiSIEM currently supports Qualys, Rapid7, Nessus and Tenable scanners. Make sure FortiSIEM is configured to collect this data at least once a day.

False Positive Detection Logic

Recall that for this detection logic to work, IPS-related incidents must have **Signature Id** and **Component Event Type** configured (for example, see the built-in **High Severity Outbound Permitted IPS Exploit** rule). The test is performed separately for both internal (for example, RFC-1918 address space) **Incident Source** and **Incident Target IPs**, as it does not make sense to perform tests for Internet addresses.

After the incident triggers, the associated CVEs for the Incident Event Type are first looked up. The primary source is the CMDB. If the CMDB does not have this information, then external websites are looked up. In the current release, only Fortinet IPS signatures are looked up using **Signature Id** in the FortiGuard database.

If associated CVEs are found, then another CMDB lookup is performed to see if the Host (in **Incident Source** or **Target**) is vulnerable to the CVEs. CMDB collects Host Vulnerability information from vulnerability scan data.

There are four detection outcomes:

- **Vulnerable** - this can result if ALL the following are true:
  a. IP is internal and,
  b. Event type to CVE mapping is found and,
  c. Host has been scanned for vulnerabilities in the last 2 weeks and,
  d. At least one CVE in (b) is found in the list of current vulnerabilities in (c).
- **Not Vulnerable** - this can result if ALL the following are true:
  a. IP is internal and,
  b. Event type to CVE mapping is found and,
  c. Host has been scanned for vulnerabilities in the last 2 weeks and,
  d. None of the CVEs in (b) are found in the list of current vulnerabilities in (c).
- **Insufficient Information** - this can result any of these cases:
  a. Even type to CVE mapping is not found or,
  b. Host has not been scanned in the last 2 weeks.
- **Not Needed** - this case is true if the IP is external.

An Incident is False positive if either of the following cases is true

- **Source Detection Status** is not **Not Needed** and Destination is **Not Vulnerable** or vice-versa
- Both **Source** and **Target** are **Not Vulnerable**

An Incident is True positive when either **Source** or **Destination** is **Vulnerable**.

Running an IPS False Positive Test

This test can be run on-demand or automatically when an Incident triggers. First you need to set up an Integration.

1. Go to **ADMIN > Settings > General > External Integration**.
2. Click **New**.
3. Set **Type = Incident**, **Direction = Outbound**, **Vendor = “FortiSIEM Attach CVE Check"**.
4. Click **Save**.

To Run the IPS False Positive Test On-Demand on an IPS Incident

1. Go to **INCIDENTS > List By Time**.
2. Select one incident. Make sure that the **Signature Id** and **Component Event Type** are configured in the **Incident Detail**.
3. Click **Action** and select **Run External Integration**.
4. Select the specific integration and click **OK**.

The IPS False positive test can be automated so that it runs automatically when the Incident triggers for the first time. To do this, create an **Incident Notification Policy**. The IPS Attack CVE Check will run as an **Incident Action**.

1. Go to **ADMIN > Settings > General > Notification Policy**.
2. Select an existing notification policy to edit, or click **New** to create one.
3. In the **Action** section, select **Invoke an Integration Policy**, then select the policy.
4. Save the policy.

Consequences of Running the IPS False Positive Test

When you run the integration policy, the following results can occur:

- The **Incident Comment** is updated with the detection status.
- The **Incident Status** is determined based on the following cases:
    a. False Positive Case: the **Incident Severity** is set to **Low** and the Incident is cleared.
    b. True Positive Case: the **Incident Severity** is set to **High** and a Case is opened.
    c. In all other cases, the **Incident Status** remains unchanged.

Executing a Playbook on an Incident

To execute a Playbook on an incident, take the following steps.

1. From the **INCIDENTS** page, select an incident.
   Note: You must be on the List by Time, List by Device, or List by Incident View.
2. Select **Execute Playbook** from the **Actions** menu.

3. From the **Execute Playbook** window, take the following steps.
    a. From the **Folders** column, expand any Playbook folder to view its content.
    b. From the **Items** column, select the Playbook you wish to execute and click **>**. The Playbook will appear in the **Selections** column. You may also search for Playbooks by using the Items **Search...** field.
    If you wish to remove a Playbook from the **Selections** column, select the Playbook you wish to remove and click **<**.
    c. When ready to execute your Playbook, click **Execute**. The **Playbook Execution Result** window appears, in the **Result** tab. This window provides a summary of result. Clicking **Details** will display additional information. Click on **View Output** to view any information related on a specific Playbook topic (Summary, Details, a specific attribute if applicable).
    d. Click on the **Actions** tab to perform any of the following actions.
    Note: All actions are optional.
        i. In the **Update Comment** field, enter any comments related to the Incident.
        ii. Click on **Add Summary** to add the Summary and Details from the Result tab into the **Update Comment** field.
        iii. To save the information added to the Update Comment field, click **Save**.
        iv. For **Resolve Incident**, select the one of the following resolutions: **Open**, **True Positive**, **False Positive**, or In **Progress**. When done, click **Apply**.
        v. Click on **Create Rule Exception** create icon to create a rule exception.
        vi. Click on the **Remediate Incident** create icon to run a remediation on the incident.
        vii. Click on **Set Incident Severity** drop-down list and select a severity level.
        viii. Click on the **Run External Integration** create icon to run an external integration.
    e. When done, click **Close**.

Under **Details**, the **Action History** column provides a log of all the actions taken, including comments from the **Update Comment** field.

Running a Connector on an Incident

To run a Connector on an incident, take the following steps.

1. From the **INCIDENTS** page, select an incident.
Note: You must be on the List by Time, List by Device, or List by Incident View.
2. Select **Run Connector** from the **Actions** menu.
3. From the **Run Connector** window, take the following steps.
    a. From the **Folders** column, select the Connector you want to run. When a Connector is selected, a list of actions for that Connector will populate under the **Items** column.
    b. From the **Items** column, select the Connector action you wish to run and click **>**. The Connector action will appear in the **Selections** column. You may also search for a Connector by using the Items **Search...** field.
    If you wish to remove a Connector from the **Selections** column, select the Connector you wish to remove and click **<**.
    c. Depending on the Connector action selected, a **Select Connector Parameters** section may appear. Enter and/or select the information necessary in the additional fields to continue.
    d. When ready to run your Connector, click **Execute**. The **Run Connector** window appears, in the **Result** tab. This window provides a summary of result. Clicking **Details** will display additional information.

Click on **View Output** to view any information related on a specific Connector topic (Summary, Details, a specific attribute if applicable).

e. Click on the **Actions** tab to perform any of the following actions.
   Note: All actions are optional.
   i. In the **Update Comment** field, enter any comments related to the Incident.
   ii. Click on **Add Summary** to add the Summary and Details from the Result tab into the **Update Comment** field.
   iii. To save the information added to the Update Comment field, click **Save**.
   iv. For **Resolve Incident**, select the one of the following resolutions: **Open**, **True Positive**, **False Positive**, or In **Progress**. When done, click **Apply**.
   v. Click on **Create Rule Exception** create icon to create a rule exception.
   vi. Click on the **Remediate Incident** create icon to run a remediation on the incident.
   vii. Click on **Set Incident Severity** drop-down list and select a severity level.
   viii. Click on the **Run External Integration** create icon to run an external integration.

f. When done, click **Close**.

Under **Details**, the **Action History** column provides a log of all the actions taken, including comments from the **Update Comment** field.

Troubleshooting Incident Trigger

An Incident may not trigger for one or more of the following reasons:

1. Rule filter conditions may not be satisfied, or events may be present. In this case, Fortinet recommends the following:
   - Test the rule with real events. If the rule does not trigger, then there may be some event attributes that are not parsed, or the rule is not written correctly.
   - View the rule and from the Filter condition page, and run the Rule as a Query for a previous time-period to see if there are matches.
2. The reporting device may be in maintenance mode, in which case, its events are ignored.
3. The Rule exception condition may be satisfied – this is expected behavior.
4. Events from Collector are delayed more than `dropping_time_threshold` when received by Worker. In this case, the log PH_DROP_EVENT_FROM_SHARED_BUFFER will be generated by the Rule Worker.
5. Rule Worker failed to upload packed aggregated result to Rule Master. This could be a networking issue. In this case, the log PH_RULEMOD_SUMMARY_UPLOAD_FAILED will be generated by the Rule Worker.
6. Rule Worker failed to pack summary events, before sending to Rule Master because of send buffer limit exceeded. This can happen if a rule is loosely written and the group by table size is very large at Rule Worker level. In this case, the log PH_REPORT_PACK_FAILED will be generated by the Rule Worker.
7. Rule Master failed to upload Incident to App Server. In this case, the log PH_UTIL_NOTIFICATION_ UPLOAD_FAILURE will be generated by the Rule Master.
8. Incident dropped because of too many incidents from the same rule, or too many incidents in general. In this case, the log PH_DROP_INCIDENT will be generated by the Rule Master. This is done to protect the system from getting flooded with Incidents. There are 6 parameters (in phoenix_config.txt) to control the incident rate:

   Short term Incident generation thresholds:
   - incident_rate_short_term_time_gap = 1 #unit: minute
   - incident_rate_short_term_per_rule_limit = 20

- incident_rate_short_term_all_rules_limit = 200;

Long term Incident generation thresholds:

- incident_rate_long_term_time_gap = 60 #uint: minute
- incident_rate_long_term_per_rule_limit = 300;
- incident_rate_long_term_all_rules_limit = 3000;

For the above parameters, if the following "too many incidents" condition is met, then incident generation pauses until the next hour boundary. For example, if this happens at 12:35PM, then Incident generation pauses from 12:35PM to 1:00PM.

Excessive Incident Generation Condition:

In 1 minute

- For one rule, more than 20 incidents fired OR
- For all rules, more than 200 incidents fired

OR in 60 minutes

- For one rule, more than 300 incidents fired OR
- For all rules, more than 3000 incidents fired

Working with Analytics Search

FortiSIEM search functionality includes real time and historical search of information that has been collected from your IT infrastructure. With real time search, you can see events as they happen, while historical search is based on information stored in the event database. Both types of search include simple keyword searching, and structured searches that let you search based on specific event attributes and values, and then group the results by attributes.

Note: If Data Obfuscation is turned on for a FortiSIEM user:

- The value for that object marked for data obfuscation is obfuscated. For example, if IP is marked for data obfuscation, the IP address is obfuscated. In earlier versions of FortiSIEM, raw events were completely obfuscated.
- CSV Export feature is disabled.

The following sections provide information about the operations under **ANALYTICS** tab:

Running a Built-in Search

FortiSIEM provides a number of built-in reports.

Complete these steps to run an built-in report:

1. Go to **ANALYTICS** tab.
2. From the folder drop-down list on the left, select **Shortcuts** or the **Reports** folder.
   - **Shortcuts** folder contains a few quick reports.
   - **Reports** folder contains the entire collection of built-in reports.
     You can search for a specific report in both of these collections by entering keywords in the Search box.
3. Select a specific report and click **>**.
4. If you are generating the report from **Shortcuts**, select whether you want to run the report in the currently selected tab or a new tab.
   Note: Running search in the currently selected tab discards the existing results displayed on that tab.

The query will run and display the results.
Note: You can also run the reports from **RESOURCES** > **Reports** folder. See here.

5. Click **Apply & Run**.

Search can be performed in two modes:

- Real time mode – from current time onwards. This mode runs only built-in searches that have no aggregation (for example, **Shortcuts** > **Raw Messages**). Note that every time you re-run this query, the displayed results will change.
- Historical mode – for previous time periods. Any query can be run in this mode. Note that the displayed search results will not change if you re-run this query for Absolute time range.

To run a real-time search

1. Click the **Edit Filters and Time Range** edit box.
   The filter conditions are displayed for the selected built-in query. See Understanding Search Components.
2. For **Time Range**, select **Real-time**.
3. Click **Apply & Run**.

To run a historical search

1. Click the **Edit Filters and Time Range** edit box.
   The filter conditions are displayed for the selected built-in query. See Understanding Search Components.
2. For **Time**, select **Relative** or **Absolute** option.
   a. For **Relative** option, the query will run for a duration in the past, starting from current time. Select the value and time scale in (**Minutes**/**Hours**/**Days**).
   b. For **Absolute** option, the query will run for a specific time window in the past. There are two ways to specify this:
      i. Using two explicitly defined time epochs.
      ii. Using **Always prior** option to define time-periods like last 1 week or last 2 months. If you are interested in re-running the same report on a daily basis, then you do not have to change the time period.
3. For **Event Source**, select **Online** or **Archive** option.
   a. For **Online** option, the query will check the configured online source.
   b. For **Archive** option, the query will check the configured archive source.
4. For **Trend Interval**, select **Auto**, **Hourly**, **Daily**, or **Weekly**. When you include a trend event attribute for a chart, such as **Event Receive Hour**, **Event Receive Daily**, or **Event Receive Weekly**, pick the appropriate configuration so your chart appears correctly.
5. Click **Apply & Run**.

Understanding Search Components

To perform a well-defined search, see the following sections:

- Query Functions - Functions available in 7.x FortiSIEM
- Specifying Search Filters – this specifies which data will be included in the Search.

- Specifying Search Time Window – only events that have been received by FortiSIEM within this time window will be part of the search.
- Specifying Trend Interval - specifies events that occur hourly, daily or weekly in trend charts.
- Specifying Event Search Source - only the selected source will be searched.
- Specifying Aggregations and Display Fields – this specifies how the data will be grouped and which fields will be displayed in the search result.
- Specifying Organizations for a Service Provider Deployment – only events belonging to this organization will be included in the Search.
- Run Multiple Searches Simultaneously – multiple real-time or historical searches can run simultaneously.
- Examples of Operators in Expressions

Specifying Search Filters

Complete these steps to specify search filters:

1. Click the **Edit Filters and Time Range** edit box.
2. Specify a filter condition:
   a. **Event Keyword** - Enter any related keyword for search.
   b. **Event Attribute** - Choose an event attribute from the drop-down list or build an expression using the expression builder. Only those event attributes based on the event type will be displayed.
      i. **Operator** - Choose the operator from the drop-down list.
      ii. **Value** - Enter a value in the edit box, or choose from CMDB, or build an expression using the expression builder, or select from Report.
   c. **CMDB Attribute** - Select a **Target** from the drop-down list. In the table, enter the CMDB attributes you want to search on.
      a. Select the **Attribute**.
      b. Select the **Operator**--the most common operators are IN and NOT IN.
      c. Click in the **Value** field and select **Select from Report** or **Select from CMDB**.
3. If more than one filter condition is needed, then click **+** under **Row**.
   a. Specify the AND/OR operator under **Next**.
   b. Specify the next filter condition. When you click in the **Attribute** field, FortiSIEM will display only those attributes that can be used with the previous attribute.
   c. Apply parenthesis if needed to prioritize filter evaluation by clicking **+** on the **Paren** icon.

   Note that the rows can be deleted by clicking the **-** under **Row** and the parenthesis can be deleted by clicking **-** under **Paren**.

Specifying Search Time Window

Complete these steps to specify search filters and time window:

1. Click the **Edit Filters and Time Range** edit box.
2. Specify the time window:
   a. **Real-time mode** – only from the current time onwards.
   b. **Historical mode** – for previous time periods that have already occurred. Select **Relative** or **Absolute** option.
      - For the **Relative** option, the query will run for a duration in the past, starting from current time. Choose the time scale (Minutes/Hours/Days) and the quantity.

- For the **Absolute** option, the query will run for a specific time window in the past. There are two ways to specify this:
  - Using two explicitly defined time epochs.
  - Using Always prior option to define time-periods such as the previous week or the previous two months. If you are interested in re-running the same report on a daily basis, then you do not have to change the time period.

The **ANALYTICS** view also provides a list of five time range buttons (15m 1h 1d 7d 30d) which appear to the left of the paginator. They allow you to filter data by the last 15 minutes, 1 hour, 1 day, 7 days, or 30 days.

Specifying Trend Interval

Complete these steps to specify the trend interval.

1. From the **Edit Filters and Time Range** edit box, specify the Trend Interval:
   a. **Auto** - (Default) Query is handled normally.
   b. **Hourly** - Select this configuration for proper chart display if you want to check the data hourly.
   c. **Daily** - Select this configuration for proper chart display if you want to check the data daily.
   d. **Weekly** - Select this configuration for proper chart display if you want to check the data weekly.

Specifying Event Search Source

Complete these steps to specify the event source for search:

1. Specify the source:
   a. **Online** - search online only.
   b. **Archive** - search archive only.

Specifying Aggregations and Display Fields

The following sections describe how to aggregate data using Group By fields and how to apply display conditions.

- Specifying Group By and Display Fields
- Specifying Display Conditions for Aggregated Search
- Saving Group By and Display Fields and Display Conditions
- Loading Group By and Display Fields and Display Conditions

Specifying Group By and Display Fields

If you want to specify an non-aggregated search (without Group By fields), then complete these steps:

1. Click the **Change Display Fields** drop-down list icon (☰▾) to create a display column.
2. Under the **Group By and Display Fields** section, enter an attribute:
   a. For a non-aggregated search, choose the event attribute from the drop-down list. If the attribute is not on the list, then enter a part of the attribute name to see some matches (for example, entering “IP” will display “Source IP” which is not on the list).

3. Optionally, select the **Order** of display as **ASC** (ascending) or **DESC** (descending) if the search result needs to show the results ordered by this column. Choose this order carefully. If multiple columns have **Order** specified, then the system will order the column that appears first and then go on to the other columns in order of appearance in the **Display Column** page.
4. If you want a column heading to display differently than the attribute, choose the desired name as **Display As**.
5. The search results are displayed in the order of the columns. You can alter the position of a column by clicking the **Move** up and down arrows.

If you want to specify an aggregated search (with Group By fields), then complete these steps:

1. Click the **Change Display Fields** drop-down list icon (☰▾) to create a display column.
2. Under the **Group By and Display Fields** section, enter an attribute:
   a. For aggregated search, enter an event attribute or create an expression using the Expression Builder, described below.
3. Optionally, select the **Order** of display as **ASC** (ascending) or **DESC** (descending) if the search result needs to show the results ordered by this column. Choose this order carefully. If multiple columns have **Order** specified, then the system will order the column that appears first and then go on to the other columns in order of appearance in the **Display Column** page.
4. If you want a column heading to display differently than the attribute, choose the desired name as **Display As**.
5. The search results are displayed in the order of the columns. You can alter the position of a column by clicking the **Move** up and down arrows.

Specifying Display Conditions for Aggregated Search

If you specified an aggregate search with Group By fields, then you can specify certain conditions. Only the events that match these display conditions will be displayed.

In the **Display Conditions** section of the **Group By and Display Fields** dialog box :

1. Choose an **Attribute** from the drop-down list.
2. Choose an **Operator** from the drop-down list.
3. Enter a **Value** for the operator.
4. If you require additional conditions, choose a value from the **Next** drop-down list and click the **+** icon under **Row**.
5. Click the **+** or **-** icons under **Paren** as needed, to add or remove parentheses on a row.

Saving Group By and Display Fields and Display Conditions

To save Group By and Display Fields and Display conditions, complete these steps:

1. Click **Save** in the **Group By and Display Fields** dialog box to save your configuration as a template.
2. Choose a **Scope** from the drop-down list in the **Save Group By and Display Fields as:** dialog box and enter a name for the template.

Loading Group By and Display Fields and Display Conditions

To load Group By and Display Fields and Display conditions, complete these steps:

1. Click **Load** in the **Group By and Display Fields** dialog box if you want to see a list of display fields that can be added to the template. The list can contain system-defined and user-defined display fields.

2. Click an item in the list, then click **Load**. The **Group By and Display Fields** dialog box closes and you will see the selected item in the list of **Attributes** in the **Group By and Display Fields** section.

Specifying Organizations for a Service Provider Deployment

To specify Organizations in a Service Provider deployment, select the organizations from the **Selection Organizations** drop-down icon (👤 ▾).

Run Multiple Searches Simultaneously

To run multiple real-time or historical searches simultaneously, follow these steps:

1. Click the **Edit Filters and Time Range** edit box.
2. Define the parameters required for the search. See Understanding Search Components.
3. Start the search.
4. Click the **+** button next to the search tab to define another search.
5. Define, then start, another real-time or historical search.

The additional search will appear as a tab next to the **+** button.

Note: real-time searches will pause as you switch between tabs.

Examples of Operators in Expressions

Operator	Argument	Example
COUNT	Matched Events	COUNT (Matched Events)
COUNT DISTINCT	Any non-numerical attribute that is not unique	COUNT DISTINCT (Host Name)
AVG, MAX, MIN, SUM, Pctile95, PctChange	Numerical attribute	AVG (CPU Util), MAX (CPU Util), MIN (CPU Util)
LAST, FIRST	Numerical attribute	LAST (System Uptime), FIRST (System Uptime)
HourOfDay, DayOfWeek	Time attribute	HourOfDay(Event Receive Time), DayOfWeek (Event Receive Time)
DeviceToCMDBAttr	Host name/IP	DeviceToCMDBAttr (Reporting IP : County/Region)
LookupTableGet	Event attribute **Format**: LookupTableGet(Lookup_Table_Name: Event_Attr_Key [:	LookupTableGet(TableName: EventAttrib1 : SearchColumn)

Operator	Argument	Example
	Event_Attr_Key_2: Event_Attr_Key_3...] : Column) • **Lookup Table** - The lookup table used in search. • **Key<*1-5*>** - Event Attribute used in search. • **Column Name** - The column that is searched.	
LookupTableHas	Event attribute **Format**: LookupTableHas(Lookup_Table_Name: Event_Attr_Key [: Event_Attr_Key_2: Event_Attr_key_3...]) • **Lookup Table** - The lookup table used in search. • **Key<*1-5*>** - Event Attribute used in search.	LookupTableHas(TableName: EventAttrib1)

Function	Function Type	Description	Syntax	Argument	Return Type	Elasticsearch		ClickHouse	
						Non-Agg	Agg	Non-Agg	Agg
LEN	String	Returns the length, in characters, of the input string.	LEN(X)	X: The source string that will be measured for string length.	Long	Yes	Yes	Yes	Yes
TO_LOWER	String	Converts input into lowercase.	TO_LOWER(X)	X: The source string that will be con-	String				

Function	Function Type	Description	Syntax	Argument	Return Type	Elasticsearch		ClickHouse	
						Non-Agg	Agg	Non-Agg	Agg
				verted to lower case					

String Functions	Argument	Example
LEN		
TO_LOWER		
TO_UPPER		
REPLACE		
TRIM		
LTRIM		
RTRIM		
SUB_STR		

Extraction Functions	Argument	Example
EXTRACT		

Conversion Functions	Argument	Example
TO_NUMBER		
TO_STRING		
LOG		

Aggregation Functions	Argument	Example
COUNT		
MEDIAN		
MODE		
STDDEV		

Aggregation Functions	Argument	Example
VARIANCE		
SUMSQ		
PCTILE		

Time Window Functions	Argument	Example
SMA		
EMA		

Conditional Functions	Argument	Example
IF		

Examples of Expressions

Operators with arguments can be combined with +, -, / and * with parenthesis to form an expression. For a good example, see the built in report “Top Devices By System Uptime Pct” which computes the System Uptime percentage using the expression

100 – (100*SUM(System Down Time)/SUM(Polling Interval)).

Example of using LookupTableHas and LookupTableGet

Lets say we want to create a rule to generate an alert when we see an event for users in the CritUsers table, where the user's role is either "Administrator" or "Manager".

User	MyRole	MyDepartment
user1	Administrator	IT
user2	Operator	Security
user3	Manager	Sales
user4	Analyst	IT

For our Filter, we would create the following rule:

(LookupTableGet(CritUsers: User : MyRole) = "Administrator"

OR

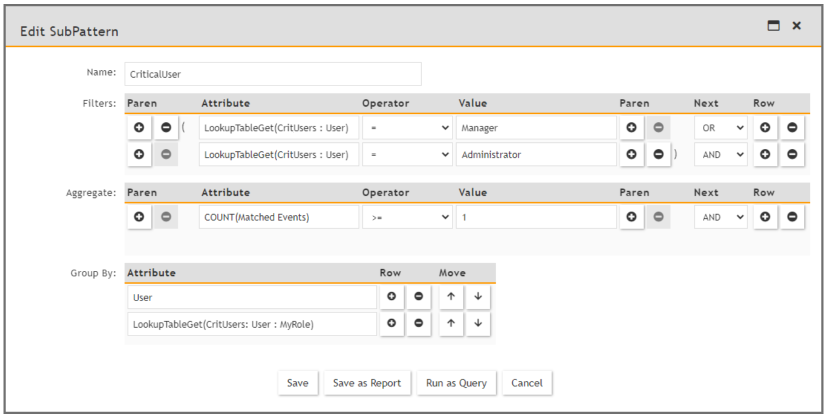
LookupTableGet(CritUsers : User : MyRole) = "Manager")

Group by:

User, LookupTableGet(CritUsers : user : MyRole)

Aggregate:

COUNT (Matched Events) >=1



Name: CriticalUser

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖ (	LookupTableGet(CritUsers : User)	=	Manager	⊕ ⊖	OR	⊕ ⊖
⊕ ⊖	LookupTableGet(CritUsers : User)	=	Administrator	⊕ ⊖)	AND	⊕ ⊖

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	COUNT(Matched Events)	>=	1	⊕ ⊖	AND	⊕ ⊖

Group By:

Attribute	Row	Move
User	⊕ ⊖	↑ ↓
LookupTableGet(CritUsers: User : MyRole)	⊕ ⊖	↑ ↓

Examples of Various Searches

- Non-aggregate search – see **Shortcut** > **Raw Messages**.
- Aggregate search:
  a. Basic – one attribute and one counting expression - **Shortcut** > **Top Event Types**.
  b. Intermediate – three attributes and one counting expression - **Shortcut** > **Top Reporting Devices** and **Event Types**
  c. Advanced – multiple attributes and complex expressions including Device to CMDB attributes:
     i. **Reports** > **Function** > **Performance** > **Top Network Interfaces By Util**
     ii. **Reports** > **Function** > **Availability** > **Top Devices By Business Hours Network Ping Uptime Pct**
     iii. **Reports** > **Incidents By Location and Category**

Query Functions

New query functions have been added for advanced analytics. Refer to the tables to see which functions are available for Elasticsearch and ClickHouse, and whether they work with aggregate and/or non-aggregate functions.

Functions are categorized as:

- Aggregate Functions
- Conditional Functions
- Conversion Functions
- Extraction Functions

- String Manipulation Functions
- Time Window Functions

Aggregate Functions

The following aggregate functions are available.

- COUNT
- MEDIAN
- MODE
- PCTILE
- STDDEV
- VARIANCE

Aggregate Function	Works with Elasticsearch Aggregate Functions	Works with Elasticsearch Non-Aggregate Functions	Works with ClickHouse Aggregate Functions	Works with ClickHouse Non-Aggregate Functions
COUNT	Yes	Yes	Yes	Yes
MEDIAN	Yes	No	Yes	No
MODE	Yes	No	Yes	No
PCTILE	No	No	Yes	No
STDDEV	Yes	No	Yes	No
VARIANCE	Yes	No	Yes	No

COUNT

The aggregate COUNT function returns the number of occurrences of a field.

Syntax	Argument	Returns	Return Type
COUNT (X)	X - The field whose number of occurrences need to be determined	How many times X occurred.	Long

COUNT Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
Elasticsearch Aggregate	Yes	No	Yes	Yes	Yes
Elasticsearch Non-Aggregate	Yes	No	No	No	No

COUNT Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
ClickHouse Aggregate	Yes	No	Yes	Yes	Yes
ClickHouse Non-Aggregate	Yes	No	No	No	No

EMA (N, X)	Exponential moving average over period N of field X	trueVal/falseVal

Elasticsearch Aggregate	No	Yes	Yes	Yes
Elasticsearch Non-Aggregate	No	No	No	No
ClickHouse Aggregate	No	Yes	No	No
ClickHouse Non-Aggregate	No	Yes	No	No

MEDIAN

The aggregate MEDIAN function returns the middle-most value of the field X.

Syntax	Argument	Returns	Return Type
MEDIAN(X)	X - a numerical field	Middle value of X within the time range of a query.	Double

MEDIAN Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
Elasticsearch Aggregate	Yes	No	Yes	Yes	Yes
Elasticsearch Non-Aggregate	No	No	No	No	No
ClickHouse Aggregate	Yes	No	Yes	Yes	Yes
ClickHouse Non-Aggregate	No	No	No	No	No

MODE

The aggregate MODE function returns the highest value of field X which has highest occurring frequency

Syntax	Argument	Returns	Return Type
MODE(X)	X - can be any field of type number,ip,string. Fields of type “text” are not allowed	Returns the most frequent value of the field X	The return type is similar to the type of field X

MODE Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested	With Trend
Elasticsearch Aggregate	Yes	No	Yes	Yes	Yes	No
Elasticsearch Non-Aggregate	No	No	No	No	No	No
ClickHouse Aggregate	Yes	No	Yes	Yes	Yes	No
ClickHouse Non-Aggregate	No	No	No	No	No	No

PCTILE

The aggregate PCTILE function

Syntax	Argument	Returns	Return Type
PCTILE(N,X)		Returns N percentile value of the numeric event attribute X.	N between 0 and 100.

PCTILE Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested	With Trend
Elasticsearch Aggregate	Yes	No	Yes	No	No	Yes
Elasticsearch Non-Aggregate	No	No	No	No	No	No
ClickHouse Aggregate	Yes	No	Yes	No	No	Yes
ClickHouse Non-Aggregate	No	No	No	No	No	No

SMA (N, X)	Simple moving average over period N of field X

Elasticsearch Aggregate	No	Yes	Yes	Yes
Elasticsearch Non-Aggregate	No	No	No	No
ClickHouse Aggregate	No	Yes	No	No
ClickHouse Non-Aggregate	No	Yes	No	No

STDDEV

The aggregate STDDEV function calculates the sample standard deviation of input field. Assumes data is normally distributed.

Syntax	Argument	Returns	Return Type
STDDEV(X)	X - a numerical field	Returns the sample standard deviation of the field X	Double

STDDEV Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested	With Trend
Elasticsearch Aggregate	Yes	No	Yes	Yes	Yes	Yes
Elasticsearch Non-Aggregate	No	No	No	No	No	No
ClickHouse Aggregate	Yes	No	Yes	Yes	Yes	No
ClickHouse Non-Aggregate	No	No	No	No	No	No

VARIANCE

The aggregate VARIANCE function returns the statistical sample variance of the input field.

Syntax	Argument	Returns	Return Type
VARIANCE(X)	X - a numerical field	Returns the variance of X	Double

VARIANCE Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested	With Trend
Elasticsearch Aggregate	Yes	No	Yes	Yes	Yes	Yes
Elasticsearch Non-Aggregate	No	No	No	No	No	No
ClickHouse Aggregate	Yes	No	Yes	Yes	Yes	No
ClickHouse Non-Aggregate	No	No	No	No	No	No

Conditional Functions

The following conditional function is available.

- IF

Conditional Function	Works with Elasticsearch Aggregate Functions	Works with Elasticsearch Non-Aggregate Functions	Works with ClickHouse Aggregate Functions	Works with ClickHouse Non-Aggregate Functions
IF	Yes	Yes	Yes	Yes

IF

The conditional function IF evaluates a Boolean expression and returns the user defined true/false values. Can run aggregations on top of IF function

Syntax	Argument	Returns	Return Type
IF(predicate, truVal, falseVal)	predicate – a valid boolean expression which evaluates to Boolean 'true'/'false' trueVal – value to be returned when predicate evaluates to 'true'. Can be 'string', 'int' falseVal -- value to be returned when predicate evaluates to 'true'. Can be 'string', 'int'	trueVal/falseVal based on what the predicate evaluates to	trueVal & falseVal are 'string' →string trueVal & falseVal are 'int' →int

IF Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested	With Trend
Elasticsearch Aggregate	Yes	No	Yes	No	Yes	Yes
Elasticsearch Non-Aggregate	Yes	Yes	Yes	No	No	No
ClickHouse Aggregate	Yes	Yes	Yes	No	Yes	No
ClickHouse Non-Aggregate	Yes	Yes	Yes	No	Yes	No

Conversion Functions

The following conversion manipulation functions are available.

- LOG
- TO_DOUBLE
- TO_INTEGER
- TO_STRING

Conversion Function	Works with Elasticsearch Aggregate Functions	Works with Elasticsearch Non-Aggregate Functions	Works with ClickHouse Aggregate Functions	Works with ClickHouse Non-Aggregate Functions
LOG	Yes	Yes	Yes	Yes
TO_DOUBLE	Yes	Yes	Yes	Yes
TO_INTEGER	Yes	Yes	Yes	Yes
TO_STRING	Yes	Yes	Yes	Yes

LOG

The conversion function LOG calculates the LOG of a number for its base.

Syntax	Argument	Returns	Return Type
LOG(X,<-base>)	X - a number whose logarithmic value needs to be calculated. X should be positive number greater than 0 <base> - (optional) base which needs to be used. Default value is 10. Only base 2, ‘e’ and 10 is allowed.	A numerical value which is equivalent to logY(X)	Double

LOG Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
Elasticsearch Aggregate	Yes	Yes	Yes	No	No
Elasticsearch Non-Aggregate	Yes	Yes	Yes	No	No
ClickHouse Aggregate	Yes	Yes	Yes	No	No
ClickHouse Non-Aggregate	Yes	Yes	Yes	No	No

TO_DOUBLE

The conversion function TO_DOUBLE converts the input string to a float64 number which can be a field name or a value.

Syntax	Argument	Returns	Return Type
TO_DOUBLE (X)	X - the string which needs to be converted to a number.	A string value representation of X	String

TO_DOUBLE Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
Elasticsearch Aggregate	Yes	Yes	No	No	No
Elasticsearch Non-Aggregate	Yes	Yes	Yes	No	No
ClickHouse Aggregate	Yes	Yes	Yes	No	Yes
ClickHouse Non-Aggregate	Yes	Yes	Yes	No	Yes

TO_INTEGER

The conversion function TO_INTEGER converts the input string to a number which can be a field name or a value. BASE is optional. The default is 10.

Syntax	Argument	Returns	Return Type
TO_INTEGER (X,<*base*>)	X - the string which needs to be converted to a number. <*base*> - optional parameter. Only base 2, 10 and 16 is allowed. Base 10 is default.	A string value representation of X <*base*>	String

TO_INTEGER Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
Elasticsearch Aggregate	Yes	Yes	No	No	No
Elasticsearch Non-Aggregate	Yes	Yes	Yes	No	No
ClickHouse Aggregate	Yes	Yes	Yes	No	Yes
ClickHouse Non-Aggregate	Yes	Yes	Yes	No	Yes

TO_STRING

The conversion function TO_STRING converts the input value to a string. If the input value is a number, it reformats it as a string. If the input value is a Boolean value, it returns the corresponding string value, "true" or "false".

Syntax	Argument	Returns	Return Type
TO_STRING (X)	X - can be a number or valid Boolean expression which evaluates to "true" or "false". .	X is a number - a string representation of X X is a Boolean expression – “true”/”false”	String

TO_STRING Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
Elasticsearch Aggregate	Yes	Yes	No	No	No
Elasticsearch Non-Aggregate	Yes	Yes	Yes	No	No
ClickHouse Aggregate	Yes	Yes	Yes	No	Yes
ClickHouse Non-Aggregate	Yes	Yes	Yes	No	Yes

Extraction Functions

The following extraction function is available.

- EXTRACT

Extraction Function	Works with Elasticsearch Aggregate Functions	Works with Elasticsearch Non-Aggregate Functions	Works with ClickHouse Aggregate Functions	Works with ClickHouse Non-Aggregate Functions
EXTRACT	Yes	Yes	Yes	Yes

EXTRACT

The extraction function EXTRACT retrieves a match for a regex from the source string. Only one capture group should be present in the regex.

Syntax	Argument	Returns	Return Type
EXTRACT (X,regex)	X - a string on which to search regex - regular expression .	match found: substring matched in the capture group match not found: null	Return type is ‘string’ by default

If EXTRACT is used to retrieve a value which is then enclosed in some aggregation function such as AVG, SUM, etc., then the return type will be ‘double’. Extracting a non-numerical value and enclosing it an aggregation function will result in query runtime error.

EXTRACT Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
Elasticsearch Aggregate	Yes	Yes	No	No	Yes
Elasticsearch Non-Aggregate	Yes	Yes	Yes	No	Yes

EXTRACT Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
ClickHouse Aggregate	Yes	Yes	Yes	No	Yes
ClickHouse Non-Aggregate	Yes	Yes	Yes	No	Yes

String Manipulation Functions

The following string manipulation functions are available.

- LEN
- LTRIM
- REPLACE
- RTRIM
- SUB_STR
- TRIM
- TO_LOWER
- TO_UPPER

String Manipulation Function	Works with Elasticsearch Aggregate Functions	Works with Elasticsearch Non-Aggregate Functions	Works with ClickHouse Aggregate Functions	Works with ClickHouse Non-Aggregate Functions
LEN	Yes	Yes	Yes	Yes
LTRIM	Yes	Yes	Yes	Yes
REPLACE	Yes	Yes	Yes	Yes
RTRIM	Yes	Yes	Yes	Yes
SUB_STR	Yes	Yes	Yes	Yes
TRIM	Yes	Yes	Yes	Yes
TO_LOWER	Yes	Yes	Yes	Yes
TO_UPPER	Yes	Yes	Yes	Yes

LEN

The string manipulation function LEN returns the length, in characters, of the input string.

Syntax	Argument	Returns	Return Type
LEN(X)	X - The source string that will be measured for	Returns the length, in characters, of the	Long

Syntax	Argument	Returns	Return Type
	string length.	input string	

LEN Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
Elasticsearch Aggregate	Yes	Yes	No	No	Yes
Elasticsearch Non-Aggregate	Yes	Yes	Yes	No	No
ClickHouse Aggregate	Yes	Yes	Yes	No	Yes
ClickHouse Non-Aggregate	Yes	Yes	Yes	No	Yes

LTRIM

The string manipulation function LTRIM removes the leading match of the specified regex. If no regex is provided, then it removes white spaces and tabs by default.

Syntax	Argument	Returns	Return Type
LTRIM (X,<*regex*>)	X – any string *<regex>* – String or regular expression to be trimmed from the beginning of source (optional)	Source after removing all leading matches of regex	String

LTRIM Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
Elasticsearch Aggregate	Yes	Yes	No	No	No
Elasticsearch Non-Aggregate	Yes	Yes	Yes	No	No
ClickHouse Aggregate	Yes	Yes	Yes	No	Yes
ClickHouse Non-Aggregate	Yes	Yes	Yes	No	Yes

REPLACE

The string manipulation function REPLACE replaces all string matches with another string.

Syntax	Argument	Returns	Return Type
REPLACE	X - original string	Returns a string formed by substituting string Z for every occur-	String

Syntax	Argument	Returns	Return Type
(X,Y,Z)	which needs to be modified Y - string to be replaced / regex Z - replacement string (optional)	rence of regex string Y in string X. If Z is not provided, then it is treated equal to empty string	

REPLACE Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
Elasticsearch Aggregate	Yes	Yes	No	No	No
Elasticsearch Non-Aggregate	Yes	Yes	Yes	No	No
ClickHouse Aggregate	Yes	Yes	Yes	No	Yes
ClickHouse Non-Aggregate	Yes	Yes	Yes	No	Yes

RTRIM

The string manipulation function RTRIM removes trailing matches of the specified regex. If no regex is provided, then it removes white spaces and tabs by default.

Syntax	Argument	Returns	Return Type
RTRIM (X,<*regex*>)	X – any string <*regex*> – String or regular expression to be trimmed from the end of source (optional)	source after removing all trailing matches of regex	String

RTRIM Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
Elasticsearch Aggregate	Yes	Yes	No	No	No
Elasticsearch Non-Aggregate	Yes	Yes	Yes	No	No
ClickHouse Aggregate	Yes	Yes	Yes	No	Yes
ClickHouse Non-Aggregate	Yes	Yes	Yes	No	Yes

SUB_STR

The string manipulation function SUB_STR extracts a substring of certain length from a source string starting from some index.

Note: ClickHouse index starts from 1. Elasticsearch starts from 0.

Syntax	Argument	Returns	Return Type
SUB_STR (X,Y,<Z>)	X - source string Y - start index. (0 <= Y <= len(X)) <Z> - number of characters to be retrieved from Y (optional)	substring of X, starting at the index specified by Y with the number of characters specified by Z. If Z is not provided, the function returns the rest of the string	String

LEN Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
Elasticsearch Aggregate	Yes	Yes	No	No	No
Elasticsearch Non-Aggregate	Yes	Yes	Yes	No	No
ClickHouse Aggregate	Yes	Yes	Yes	No	Yes
ClickHouse Non-Aggregate	Yes	Yes	Yes	No	Yes

TRIM

The string manipulation function TRIM removes all leading and trailing matches of the specified regex. If no regex is provided, then it removes white spaces and tabs by default.

Syntax	Argument	Returns	Return Type
TRIM (X,<*regex*>)	X - any string <*regex*> - String or regular expression to be trimmed from the beginning and end of source (optional) • <*regex*> with ',' not supported as of now	source after removing all leading and trailing matches of regex	String

TRIM Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
Elasticsearch Aggregate	Yes	Yes	No	No	No
Elasticsearch Non-Aggreg-	Yes	Yes	Yes	No	No

TRIM Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
ate					
ClickHouse Aggregate	Yes	Yes	Yes	No	Yes
ClickHouse Non-Aggregate	Yes	Yes	Yes	No	Yes

TO_LOWER

The string manipulation function TO_LOWER converts input into lowercase.

Note: TO_LOWER(User) can return empty strings, hence it will look like that it is returning NULL. For this reason, it is recommended to use attributes directly with IS NULL and IS NOT NULL.

Syntax	Argument	Returns	Return Type
TO_LOWER (X)	X - The source string that will be converted to lowercase	Returns the input string in lowercase	String

TO_LOWER Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
Elasticsearch Aggregate	Yes	Yes	No	No	No
Elasticsearch Non-Aggregate	Yes	Yes	Yes	No	No
ClickHouse Aggregate	Yes	Yes	No	No	Yes
ClickHouse Non-Aggregate	Yes	Yes	Yes	No	Yes

TO_UPPER

The string manipulation function TO_UPPER converts input into uppercase.

Note: TO_UPPER(User) can return empty strings, hence it will look like that it is returning NULL. For this reason, it is recommended to use attributes directly with IS NULL and IS NOT NULL.

Syntax	Argument	Returns	Return Type
TO_UPPER (X)	X - The source string that will be converted to uppercase	Returns the input string in uppercase	String

TO_UPPER Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested
Elasticsearch Aggregate	Yes	Yes	No	No	No
Elasticsearch Non-Aggregate	Yes	Yes	Yes	No	No
ClickHouse Aggregate	Yes	Yes	No	No	Yes
ClickHouse Non-Aggregate	Yes	Yes	Yes	No	Yes

Time Window Functions

The following Time Window functions are available.

- EMA
- SMA

Time Window Function	Works with Elasticsearch Aggregate Functions	Works with Elasticsearch Non-Aggregate Functions	Works with ClickHouse Aggregate Functions	Works with ClickHouse Non-Aggregate Functions
EMA	Yes	No	Yes	Yes
SMA	Yes	No	Yes	Yes

EMA

The time window EMA function computes the exponential moving average over the values of the input field for the determined time.

For EMA, older data points become exponentially less important. The speed at which the importance decays is controlled with a decay parameter represented with ∝ . The value of ∝ is internally calculated using the window size:

∝ =1-(1/2) 〖N 〗^( ) where ∝ is decay parameter and N is look back window size.

Syntax	Argument	Returns	Return Type
EMA (N,X)	N - the size of the look back window. (Integer) o If the time aggregate field included is phRecvHour, then window refers for last ‘N’ hours o If the time aggregate field included is phRecvDate, then window refers for last ‘N’ days, etc... X - The input field (Numerical attribute)	Exponential moving average over period N of field X	Double

EMA Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested	With Trend
Elasticsearch Aggregate	Yes	No	Yes	Yes	Yes	Yes
Elasticsearch Non-Aggregate	No	No	No	No	No	No
ClickHouse Aggregate	Yes	No	Yes	Yes	No	No
ClickHouse Non-Aggregate	Yes	No	Yes	No	No	No

SMA

The time window SMA function computes the simple moving average over the values of the input field for the determined time. It calculates the sum of all values in the window, then divides by the size of the window. It is effectively a simple arithmetic mean of the window.

Any query using SMA needs to have at least one of the time aggregation fields included. Supported time aggregation fields include

- phRecvHour
- phRecvDate
- phRecvWeek
- phRecvMonth

Syntax	Argument	Returns	Return Type
SMA (N,X)	N - the size of the window. (Integer) • If the time aggregate field included is phRecvHour, then window refers for last 'N' hours • If the time aggregate field included is phRecvDate, then window refers for last 'N' days etc X - The input field (Numerical attribute)	Simple moving average over period N of field X	Double

SMA Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested	With Trend
Elasticsearch Aggregate	Yes	No	Yes	Yes	Yes	Yes
Elasticsearch Non-Aggregate	No	No	No	No	No	No
ClickHouse Aggregate	Yes	No	Yes	Yes	No	No

SMA Function	Available	With Filter	With Orderby	With GroupEvtConstr	With Nested	With Trend
ClickHouse Non-Aggregate	Yes	No	Yes	No	No	No

Viewing Historical Search Results

Historical Search results are displayed in two panes:

- Bottom pane displays the results in tabular view following the definitions in the Display Fields.
- Top pane displays the trends over time:
  - For non-aggregated searches, the trend is for event occurrence and is displayed in a trending bar graph. Each bar captures the number of entries in the table during a particular time window.
  - For aggregated searches, the trend is for any of the (numerical) columns with aggregations. Trends are displayed for the Top 5 entries in the table. For integer values, such as COUNT (Matched Events), you will see a trend bar graph, while for continuous values such as AVG(CPU Utilization), you will see a line chart.

Both the bar and line charts show trends in a stacked manner, one for each row in the table. To see the trend for a specific row, disable all the other entries by deselecting the check box in the first column. To view the trend for a set of entries, you can select the check box corresponding to those entries.

For continuous values, you can toggle between a stacked view and a non-stacked view:

- To show the stacked view, click 📊 .
- To show the line chart view, click 📈 .

If there are multiple aggregate columns:

- Select a specific column in the **Chart for** in top right to see the Chart for that column.
- Select one column for **Chart for** and another column for **Lower Chart** to see the two charts at the same time – one on +ve Y-axis and one on –ve Y-axis. This generally makes sense when the values are of the same order. For example, AVG(CPU Utilization) and AVG(Memory Utilization) or AVG(Sent Bytes) and AVG(Recv Bytes).

You can visualize the results in other charts by clicking the 📊 ▾ drop-down. See FortiSIEM Charts and Views for descriptions of the available charts.

Events in FortiSIEM have an Event Type (like an unique ID) and an Event Name, a short description. When you choose to display Event Type, the Event Name is automatically displayed but Event type is hidden to make room to show other fields. To see the Event Types, click the **Show Event Type** check-box.

Raw events often take many lines to display in a search result. By default, Raw events are truncated and displayed in one line so that user can see many search results in one page. To see the full raw event, click the **Wrap Raw Event** check-box.

Using Search Result Tabs

A search result typically shows many rows. To drill down into a specific value for a specific column, hover over the specific cell and choose **Add to Filter** or **Add to Tab**. **Add to Filter** modifies the search on the current tab by including this constraint. **Add to Tab** on the other hand, gives you the option to keep the current tab intact and add the constraint to a new tab or to a tab of your choice. This enables you to see multiple search results side by side. Click **Add to Tab** and select the tab where the constraint needs to be added. The filter conditions and display columns are copied over to the new tab.

Zooming-in on a Specific Time Window

If you see an unusual pattern (for example, a spike) in the trend chart and want to drill down without providing an exact time range, do one of the following:

- Click the bar – a new search tab is created by duplicating the original search and adding the right time window as seen by hovering on the bar.
- Press and hold the **Shift** key and drag the mouse over a time window. This modifies the time window in the current tab. Click **Apply & Run** to see the results.

Viewing Parsed Raw Events

Hover over a **Raw Event Log** cell and click **Show Details**. The display shows how FortiSIEM parsed that event.

Adding an Attribute to the Filter Criteria in the Search

Complete these steps to add an attribute to the filter criteria in the search:

1. Check the **Filter** column.
2. Click **OK**.
   The Attribute is added to the filter condition.
3. Re-run the query to get the new results.

Adding an Attribute to the Search Display

Complete these steps to add an attribute to the search display:

1. Check the **Display** column.
2. Click **OK**.
   The Attribute is added to the display condition.
3. Re-run the query to get the new results.

Viewing Large Non-Aggregated Search Results

Non-aggregated search results without proper filtering conditions may return a large data set. Note the following while viewing such search results:

1. The table shows a maximum of 100K rows.
2. The trend data shows the entire data set.

Viewing Real-time Search Results

Real-time Search results display matching events that occur from the current time onwards.

The search results are displayed in two panes:

- Bottom pane displays the results in tabular form following the definitions in the **Display Fields**.
  Note that aggregations are not permitted in real-time search. Since results are coming in continuously, the results scroll and the latest events are displayed at the top.
- Top pane displays the counts of matched events over time.

The following actions are possible while viewing Real-time Search results:

- To pause the search, click **Pause**.
- To restart the real-time search from the point you left off, click **Resume** after **Pause**.
- To fast forward to the current time, click **Fast forward**.
- To clear the result table, click **Clear**.
- To restart the search all over again from the current time, click **Stop** and then **Run**.

In real-time search, only Event Type (like a unique ID) is displayed. Enable **Show Event Type** while running a real-time query. Note that Event Names are not displayed.

Raw events often take many lines to display in a search result. By default, Raw events are truncated and shown in one line so that user can see many search results in one page. To see the full raw event, click the **Wrap Raw Event** check-box.

Viewing Parsed Raw Events

Hover over a **Raw Event Log** cell and click **Show Details**. The display shows how FortiSIEM parses the event.

Adding an Attribute to the Filter Criteria in the Search

Complete these steps to add an attribute to the filter criteria in the search:

1. Check the **Filter** column.
2. Click **OK**.
   The Attribute is added to the filter condition.
3. Re-run the query to get the new results

Adding an Attribute to the Search Display

Complete these steps to add an attribute to the search display:

1. Check the **Display** column.
2. Click **OK**.
   The Attribute is added to the display condition.
3. Re-run the query to get the new results.

Zooming-in on a Specific Time Window

If you see an unusual pattern (for example, a spike) in the trend chart and want to drill down without entering the exact time range, do one of the following:

- Click the bar – a new search tab is created by duplicating the original search and adding the right time window as seen by hovering on the bar
- Press and hold **Shift** key and drag the mouse over a time window – this modifies the time window in the current tab.
  Click **Apply & Run** to see the results.
- When you run the Real-time search, a pop-up will appear asking if you want to stop the Real-time search before proceeding to the Historical Search.

Using Nested Queries

Nested Query functionality enables one query to refer to results from another query. This section describes how to set up and use nested queries for the three supported scenarios:

- Outer CMDB Query, Inner Event Query
- Outer Event Query, Inner Event Query
- Outer Event Query, Inner CMDB Query

Outer CMDB Query, Inner Event Query

The following generalized steps describe how to create a nested query where the outer query targets CMDB and the inner event query targets events.

If you want to reuse an existing query, then skip Step 1 and go to Step 2. Note that for a nested query to work correctly, the data type of the filter attribute in the outer query must "match up" with the data type of one certain display column in the inner query.

Step 1: Construct the Inner Event Query

1. Go to the **ANALYTICS** page.
2. Construct the query and make sure it produces the desired results.
   a. Click the **Edit Filter and Time Range** field and select **Event Attribute** in the query tab.
   b. Set the **Time Range**. For example, you can set it to the last 1 hour. This time period is not important if you use this query as an inner query.
   c. If it has the **Event Source**, then you can set it as Online.
   d. Click **Apply** to save your changes.
   e. Click the **Change Display Fields** icon and enter the attributes you want to display.
   f. Click **Apply & Run**.
3. Click **Action > Save as Report**.
4. Ensure **Save Definition** is checked.

Step 2: Construct the Outer CMDB Query by Referring to the Query in Step 1

1. Go to the **ANALYTICS** page.
2. Click in the Search bar--it will open the **Filter** dialog box.
3. Select **CMDB Attribute**.
4. Select the appropriate target from the drop-down list.

5. Set the query condition.
   a. Select the **Attribute**.
   b. Select the **Operator**--the most common operators are IN and NOT IN.
   c. Click in the **Value** field and select **Select from Report.**
   d. Select the **Report** name, saved in Step 1, Substep 4.
   e. Open the **Attribute** drop-down list and choose the attribute that matches the attribute in Step 2, Substep 5a.
   f. Click **OK**.
6. Choose the **Nested Time Range**: the inner report will be run for this time range.
7. Click the **Change Display Fields** icon and choose the attributes you want to display.
8. Click **Apply & Run**.
9. To save the report, click **Actions > Save as Report**. Enter the name of the nested query.

Outer Event Query, Inner Event Query

The following generalized steps describe how to set up and use nested queries for an outer event query and an inner event query.

Step 1: Construct the Inner Event Query

1. Go to the **ANALYTICS** page.
2. Click the **Edit Filter and Time Range** field.
   a. Select **Event Attribute** and create the **Filter Condition**.
   b. Set the **Time Range**.
      For example, you can set it to the last 1 hour. This time period is only useful to check if this query produces the desired results. If used as an inner query, time range would be set separately in Step 2 below.
   c. If it has the **Event Source**, then you can set it as Online.
   d. Click **Apply** to save your changes.
   e. Click the **Change Display Fields** icon and enter the attributes you want to display. This query needs to be an aggregate query to be used as an inner query. One of the Group By attributes must match (meaning compatible value sets) an attribute chosen in the outer query in Step 2, Substep 2.d.ii
   f. Click **Apply & Run**.
3. If you are happy with the result, then click **Actions > Save as Report**. Ensure **Save Definition** is checked.

Step 2: Construct the Outer Event Query

1. Go to the **ANALYTICS** page.
2. Click the Edit Filter and Time Range field.
   a. Select **Event Attribute** in the query tab.
   b. Choose an **Attribute**.
   c. Choose an **Operator**. The most common operators are IN and NOT IN.
   d. Click the **Value** field and select **Select from Reports**.
      i. Select the **Report** name, saved in Step 1, Substep 3.
      ii. Open the **Attribute** drop-down list and choose the attribute that matches the attribute in Step 1,

Substep 2e.

iii. Click **OK**.

3. Choose the time ranges.
   a. Choose the time range for outer query.
   b. Choose **Nested Time Range** for the inner query.
   c. If it has the **Event Source**, then you can set it as Online.
4. Click **Apply** to save your changes.
5. Click the **Change Display Fields** icon and enter the attributes you want to display.
6. Click **Apply & Run**.
7. You can save the results by clicking **Actions > Save as Report**. Ensure **Save Definition** is checked.

Outer Event Query, Inner CMDB Event Query

The following generalized steps describe how to set up and use nested queries for an outer event query and an inner CMDB query.

Step 1: Construct the Inner CMDB Query

1. Go to the **ANALYTICS** page.
2. Click the **Edit Filter and Time Range** field and select **CMDB Attribute** in the query tab.
   a. Select the appropriate **Target** from the drop-down list.
   b. Set the query condition.
      i. Select the **Attribute**.
      ii. Select the **Operator**
      iii. Click in the **Value** field. Do not select **Select from Report**.
   c. Click **Apply** to save your changes.
3. Click the **Change Display Fields** icon and enter the attributes you want to display.
4. Click **Apply & Run**.
5. If you are happy with the result, then click **Actions > Save as Report**. Ensure **Save Definition** is checked.

Step 2: Construct the Outer Event Query

1. Go to the **ANALYTICS** page.
2. Click the **Edit Filter and Time Range** field and select **Event Attribute** in the query tab.
   a. Choose an **Attribute**.
   b. Choose an **Operator** - the most common operators are IN and NOT IN.
   c. Click in the **Value** field and select **Select from Report**.
      i. Select the **Report** name, saved in Step 1 Substep 5.
      ii. Open the **Attribute** drop-down list and choose the attribute that matches the attribute in Step 1 Substep3.
      iii. Click **OK**.
3. Choose the **Time Range** for outer query.
4. If it has the **Event Source**, then you can set it as Online.
5. Click **Apply** to save your changes.
6. Click the **Change Display Fields** icon and enter the attributes you want to display.

7. Click **Apply & Run**.
8. You can save the results by clicking **Actions > Save as Report**. Ensure **Save Definition** is checked.

Searches Using Pre-computed Results

If you want to run the same search again and again, or you want to run certain pre-defined searches over a large time window, then the search time can be reduced by setting up pre-computation. See Known Issues in the latest What's New for any limitations with pre-computed results.

It is important that search filters, group by, and display parameters and display filters do not change. Otherwise, the pre-computation results will be invalid.

To use this feature, you must complete these steps:

1. Select a Report and turn on pre-computation.
2. Select the Pre-computed result option when running the search.

The following sections provide more information about the pre-computation feature and how to use it.

- Usage Notes
- Setting Up Pre-computation
- Impact of Organization and Roles
- Viewing Pre-computed Results
- Running a GUI Search on Pre-computed Results
- Scheduling a Report Based on Pre-computed Results
- Running a Report Bundle Based on Pre-computed Results
- Scheduling a Report Bundle Based on Pre-computed Results

Usage Notes

1. Currently, pre-computation only works with

- FortiSIEM EventDB
- Elasticsearch

1. Pre-computation is currently supported for Aggregated queries with COUNT, SUM, AVG, MAX, and MIN operators. Raw event queries and nested searches are not supported.
2. If you run a query with pre-computed results, but the search interval is wider than the available pre-computed results, then the results are returned for the pre-computed time interval only. Currently, FortiSIEM does not run a separate search for the missing time window and stitch together the two search results.
3. Pre-computation begins at hourly/daily boundaries. For example, if you set up hourly pre-computation at 2:34 PM, then the first pre-computation will begin at 3:10 PM for the time interval 2:00 PM – 3:00 PM.
4. FortiSIEM does not semantically compare search filters, group by, and display parameters and display filters for two searches. Thus, pre-computed results cannot be used for a cloned search.
5. Pre-computation is set up at a report level and not a report bundle level.
6. For the Service provider case, you must effectively have the same role in all Organizations to be able to use pre-computed results. Examples are

a. Full Admin for all Organizations.
b. Help desk user for one Organization and Read only user for another Organization. Note that both of these roles have empty data conditions and hence are effectively the same role from a pre-computation perspective.

Setting Up Pre-computation

Only a Super Global user having the Full Admin role can set up pre-computation. This is because only such a user can see all the roles. A Full Admin user for a specific organization cannot set up pre-computation. Follow these steps to set up pre-computation.

1. Log in to FortiSIEM as a Super Global Full Admin user.
2. Go to **RESOURCES > Reports**.
3. Select a **Report**, Click **More** and Select **Pre-compute**.
4. Enter the pre-compute options:
   a. Select the **Enable** option to enable pre-computation. If you do not select **Enable**, then the definition will be there, but pre-computation will stop and all older results will be deleted.
   b. Carefully select the **Organization** and the **Roles** for whom queries will be pre-computed. These selections determine when a user query can use pre-computed results. See Impact of Organization and Roles for more detail.
   Note: If duplicate roles with different names exist, only one role will appear for selection. For example, if you have "Full Admin" and "Full Admin2" with the same permissions, only "Full Admin" would appear for the pre-compute role selection.
   c. Select Pre-computation **Frequency**. A lower frequency provides more accuracy at the expense of more system load and storage. Choose the lowest frequency you can accept.
   d. Select the **Age** in number of days. Pre-computed results older than this age will be deleted.
   e. Check the **Pre-compute history** option if you want the system to automatically run and fill up data from earlier time intervals.
5. Click **OK**.

The system will begin pre-computation on the hour or day boundary. For example, if you set up hourly pre-computation at 2:34 PM, then the first pre-computation will begin at 3:10 PM for the time interval 2:00 PM – 3:00 PM. As another example, if you set up daily pre-computation at 10:00 PM, then the first pre-computation will begin slightly after 12:00 AM midnight for the previous day.

Impact of Organization and Roles

A query definition does not enforce Organization and Role restrictions. When you run a query, you are forced to choose one or more Organizations. The data conditions for your role definition are automatically applied. For example, if you run a Top Event Type query as a Full Admin user for Org1 and Org2, then you get All Event Types for Org1 and Org2. However if you run as a Network Admin for Org2 then you only get Network Event Types for Org2. Your Organization and Role assignments have an effect on the query results as they change the query filters.

If you set up pre-computation for an Organization and a set of Roles, then only the users belonging to the same Organization and having exactly the same Role can use pre-computed results. The only exception is for a Full Admin user who can use any pre-computed result in a query. The examples in the following table illustrate this point.

Pre-computation Definition			
Organization	Role	Who can use pre-computed results	Who cannot use pre-computed results
All Orgs Combined	Full Admin	Super-global users that are Full Admin for all Organizations or have roles without data conditions in some organizations.	Other users, for example, Super Global Network Admins for Org1 and Full Admin for Org2
All Orgs Combined	Network Admin	Super-global users that have the Network Admin role in All Organizations.	
All Orgs Combined	Network Admin, Server Admin	Super-global users that are both Network Admin and Server Admin in All Organizations.	If the user is a Network Admin for Org1 and Server Admin for Org2.
Org1	Full Admin	Full Admin or users with no data constraints belonging to Org1 can use pre-compute results.	Other users, for example, Org1 Network Admins cannot use these pre-computed results.
Org1	Network Admin	Network Admin users belonging to Org1 can use pre-compute results.	
Org1	Network Admin, Server Admin	Users belonging to BOTH Network Admin and Server Admin and belonging to Org1.	If the user belongs to only one role, for example Network Admin only, then the user cannot use pre-computed results.

Viewing Pre-computed Results

Once pre-computation is defined, FortiSIEM will pre-compute on the hour or day boundary.

To see the time slots of pre-computed results:

1. Select a Report.
2. Click **Pre-compute > Results**.
3. Click **Refresh** to get the latest results.
   a. **Time Range From** and **Time Range To** represent the Query Time Window.
   b. **Organization** and **Roles** relate to the query conditions.
   c. **Finish Time** specifies when the pre-computed query finished.

To see the content of a pre-computed result:

1. Select one row and click **View Results**.
2. You will be taken to the **ANALYTICS** tab with the query conditions already provided. You can see the results. The query name will display **(Pre-computed)** appended to the end of the name.
3. Note that because you are running a pre-computed query, you are allowed to perform only these two operations:

   a. Change the time range by clicking the **Query Filter** search bar and selecting a different **Time range**.
   b. Load another pre-computed (Organization, Role) combination for the same query by going to the **Query Filter** search bar and selecting a different (Organization, Role) from the **Pre-compute Settings** menu.

   All of the other possible choices, such as Query Filters, Organization Drip down, and Query Group By and Display Fields, are grayed out and unavailable.

4. If you want to stay in this page and change other conditions, click **Query Filter** search bar and deselect **Pre-compute Settings**.

Running a GUI Search on Pre-computed Results

You can run a search from the GUI on pre-computed results from the **ANALYTICS** page or the **RESOURCES** page.

- From the ANALYTICS Page
- From the RESOURCES Page

From the ANALYTICS Page

1. Load a **Report** and click **>**.
2. If the Report has been pre-computed, then the system will ask you to choose whether you want to use pre-computed results.
   a. If you do not want to use pre-computed results, then remove the check from **Use pre-compute for** and click **OK**. The query will run by searching the database.
   b. If you want to use pre-computed results, then check **Use pre-compute for** and select the Organization/Role combination from the drop-down list and click **OK**. The query will run based on pre-computed results.
3. Note that because you are running a pre-computed query, you are allowed to perform only these two operations:.
   a. Change the time range by clicking the **Query Filter** search bar and selecting a different **Time range**.
   b. Load another pre-computed (Organization, Role) combination for the same query by going to the **Query Filter** search bar and selecting a different (Organization, Role) from the **Pre-compute Settings** menu.

   All of the other possible choices, such as Query Filters, Organization Drip down, and Query Group By and Display Fields, are grayed out and unavailable.

4. If you want to stay in this page and change other conditions, click the **Query Filter** search bar and deselect **Pre-compute Settings**.

From the RESOURCES Page

1. Select a **Report** and click **Run**. A dialog box will open.
2. Select the **Organization** for which you want to run the report. The query result will contain the selected organizations. Note that based on the selected organizations, the pre-compute options below will change.
3. Select **Report Time Range**.
4. Select the pre-compute option if available from the menu.
5. Click **Run**.
6. You will be taken to the **ANALYTICS** tab with the query conditions already provided. You can see the results. The Query name will display **(Pre-computed)** appended at the end of the name.

7. Note that because you are running a pre-computed query, you are allowed to perform only these two operations:.
   a. Change the time range by clicking the **Query Filter** search bar and selecting a different **Time range**.
   b. Load another pre-computed (Organization, Role) combination for the same query by going to the **Query Filter** search bar and selecting a different (Organization, Role) from the **Pre-compute Settings** menu.

   All of the other possible choices, such as Query Filters, Organization Drip down, and Query Group By and Display Fields, are grayed out and unavailable.

8. If you want to stay in this page and change other conditions, click the **Query Filter** search bar and deselect **Pre-compute Settings**.

Scheduling a Report Based on Pre-computed Results

1. Go to the **RESOURCES** page.
2. Select a **Report** and click **More > Schedule**. A dialog box will open.
3. Select the **Organization** for which you want to run the report. Note that based on the selected organizations, the pre-compute options below will change.
   a. If you select **Combine all selected Organizations into one Report**, then the report will contain data from all organizations. You also have the option to select the organizations that you want to include. For pre-compute to work, you must select **All Organizations**.
   b. If you select **Generate separate Report for each selected Organization**, then a separate report will be sent out for each selected organization, Data between organizations will not be mixed in the same report. For pre-compute to work, you must select these Organizations to be pre-computed.
4. Select **Report Time Range**.
5. If you want data to be pre-computed, then select **Pre-compute settings** from the menu. You can select multiple entries for step 3b above.
6. Click **Next** and enter values for the rest of the options in the dialog box.
7. Click **OK**.

The system will run the report based on a schedule. If pre-compute settings are specified then the report results will be based on pre-computed data.

Running a Report Bundle Based on Pre-computed Results

A Report Bundle consists of one or more reports. One or more reports may be set to be pre-computed. If you run the Report Bundle, then the reports set up for pre-computation will have pre-computed results, while other reports will run normally (without pre-computation).

1. Go to **RESOURCES > Reports > Report Bundle**.
2. Select a **Report Bundle**.
3. On top left, select **Export Report Bundle**.
4. In **Pre-compute Settings**, select the Organization and Role combination. Each Report can be pre-computed for multiple Organization and Role combinations. When scheduling a report bundle, a common Organization and Role combination must be chosen that is applicable for ALL pre-computed reports. When Pre-Computation is defined, Filters cannot be selected.
5. Select other setting as usual.
6. Click **OK** to run the Report Bundle.

Scheduling a Report Bundle Based on Pre-computed Results

A **Report Bundle** consists of one or more reports. One or more reports may be set to be pre-computed. If you schedule the Report Bundle, then the reports set up for pre-computation will have pre-computed results, while other reports will run normally (without pre-computation).

1. Go to **RESOURCES > Reports > Report Bundle**.
2. Select a **Report Bundle**.
3. On top left, select **Schedule Report Bundle**.
4. Click **+** to create a schedule.
5. In **Pre-compute Settings**, select the Organization and Role combination. Each Report can be pre-computed for multiple Organization and Role combinations. When scheduling a report bundle, a common Organization and Role combination must be chosen that is applicable for ALL pre-computed reports. When Pre-Computation is defined, Filters cannot be selected.
6. Select other setting as usual.
7. Click **OK** to schedule the Report Bundle.

Saving Search Results

Sometimes you must save a search and/or the search results for later use. With the search result displayed in **ANALYTICS**, complete these steps:

1. From the **Actions** drop-down list, select **Save as Report**.
2. Specify the **Report Name**.
3. Specify whether the Report Definition must be saved. This will allow you to re-run the query at a later time. If you respond "yes", then:
    a. Check **Save Definition**.
    b. Select the report folder in **Save To** where the new report should be saved.
4. Enable **Save Results** if the Report results should be saved and then select the time duration.
   If this option is enabled, the results will be stored under the **Saved Results** folder under the **Folders** icon.
5. Enable **Save Template** if you want to apply a template to your results. Follow the instructions in Designing a PDF Report Template to design the cover page and add sections, subsections, attachments, and so on, to the report.

Viewing Saved Search Results, Loading Reports and Shortcuts

Complete these steps to view previously saved search results:

1. Go to the **Load Report/Saved Results** folder by clicking 📂 ▾ .
2. In the left column, select one of the following:
    - Saved Results
    - Shortcuts
    - Reports
    - CMDB Reports

3. Drill down if needed, and select the result, shortcut or report.
4. Hover over that object's **Name** cell, click on **>**, and choose **View Result** from the drop-down list. (To delete a saved search result, you can choose **Delete**.)
   The results will be displayed.
   Note: You may be prompted to view the selection in a new tab or current tab depending on what was selected.

Exporting Search Results

With the search results displayed under **ANALYTICS**, complete these steps to export:

1. From the **Actions** drop-down list, select **Export Result**.
2. Enter the **User Notes** (optional).
3. Specify the **Output Format** as **PDF**, **RTF**, or **CSV**.
   Files with a large number of rows should be exported in CSV format.
4. Select the **Time Zone** of the data from the drop-down list.
5. Select the Report **Template** if you select **PDF** or **RTF** format:
   - **Defined** - to use the template defined for this report defined under **RESOURCES** > **Reports** or use the system default template for ANALYTICS export.
   - **New** - to create a new custom report template for one-time use. The **Report Design** settings appear when you choose this option. Note that this template will not replace the template defined under **RESOURCES** > **Reports**.
     Refer to Designing a Report Template for the steps to design the **Cover Page** and **Table of Contents**.
6. Click **Generate** to generate the report.
7. Click **View** to download the report to the local disk.

Emailing Search Results

You must first configure email settings under **ADMIN** > **Settings** > **System** > **Email**. With the search result displayed in **ANALYTICS** tab, complete these steps to email search results:

1. Go to the **Actions** drop-down list and select **Email Result**.
2. Enter the receiver email address in the **To** field.
3. Enter the **Subject** of the email.
4. Enter any **Description** about the email.
5. Enter any **User Notes** about the search results (optional).
6. Choose the **Output Format** as **PDF**, **RTF**, or **CSV**.
7. Select the **Time Zone** of the data from the drop-down list.
8. Select the Report **Template** if you select **PDF** or **RTF** format:
   - **Defined** - to use the template defined for this report defined under **RESOURCES** > **Reports** or use the system default template for ANALYTICS export.
   - **New** - to create a new custom report template for one-time use. The **Report Design** settings appear when you choose this option. Note that this template will not replace the template defined under **RESOURCES** > **Reports**.
     Refer to Designing a Report Template for the steps to design the **Cover Page** and **Table of Contents**.
9. Click **Send**.

Creating a Rule from Search

With the search result displayed in Analytics, follow the steps below to create a rule:

1. From the **Actions** drop-down list, select **Create Rule**.
2. A rule template is automatically created by copying over important Search parameters:
   a. Rule Sub-pattern Filters contain Search Filter conditions
   b. Rule Sub-pattern Group By contain Search Display conditions
   c. Rule Aggregate Conditions are set to COUNT(Matched Events) >= 1
3. To complete the rule creation, configure the settings under the **Create Rule** window with reference to the following table:

Settings	Guidelines
Rule Name	Enter a name for the new Rule.
Description	Enter a description about the new Rule.
Event Type	The name you enter in the Rule Type field is replicated in the Event Type field.
Remediation Note	Enter the **Remediation** script. Make sure that the Remediation script for your scenario is defined. Check the existing Remediation scripts under **ADMIN** > **Settings** > **General** > **Notification Policy**, and check the **Action** column. If your device is not in the list, add the needed Remediation script.
Condition	Click **Condition** to create the rule conditions. See Defining Rule Conditions.
Severity	Select a **Severity** to associate with the incident triggered by the rule.
Category	Select the **Category** of incidents to be triggered by the rule.
Subcategory	Select the **Subcategory** from the available list based on the selected incident **Category**. To add custom subcategories, follow the steps under Setting Rule Subcategory.
Technqiue	Select any techniques from the available **Technique** list. You can choose to select zero, one, or multiple techniques. The Tactics row will update itself based on the techniques selected.
Action	Click the edit icon to define the incident (Incident Attributes and Triggered Attributes) that will be generated by this rule. You must have at least one incident defined before you can save your rule.
Exception	Click the edit icon to define any **Exceptions** for the rule. See Defining Rule Exceptions.
Tag	Click the drop-down list icon to view the tag list. If no tags appear, it means no tags have been created. From the drop-down list, select any tags you wish to associate with the rule. From Incidents View (by Time, by Device, by Incident), tags are displayed in

Settings	Guidelines
	the **Tag** column. See Tags for more information.
Update Status on Summary Dashboard	Select **Dashboard** to add this report under **DASHBOARD** tab.
Notification	Select a **Notification** frequency for how often you want notifications to be sent when an incident is triggered by this rule.
Impacts	Select the **Impacts** of the incident triggered by this rule from the drop-down.
Watch List	Click the edit icon to add the rule you want to add to the watch list. **Note:** The Type that you set for the watch list must match the Incident Attribute Types for the rule. For example, if your watch list Type is IP, and the Incident Attribute Type for the rule is string, you will not be able to associate the watch list to the rule.
Clear	Click the edit icon to define any **Clear** conditions for the rule. See Defining Clear Conditions.

1. Click **Save**.
   Your new rule will be saved to the group you selected in an inactive state. Before you activate the rule, you should test it.

Copying Filter and Time Range Tab Information

With a tab selected in **ANALYTICS**, take the following steps to copy the selected tab's filter and time range information to a new tab.

1. From the **Actions** drop-down list, select **Copy to New Tab**.
   A new tab is created that contains the filter and time range information of the selected tab.

Executing a Playbook

FortiSIEM allows you to execute existing FortiSOAR Playbooks on an event or incident.

- Executing a Playbook on an Event
- Executing a Playbook on an Incident

Executing Playbook on an Event

To execute a Playbook on an event, take the following steps.

1. From the **ANALYTICS** page, select an event.
2. Click **Execute Playbook**.

3. From the **Execute Playbook** window, take the following steps.
    a. From the **Folders** column, expand any Playbook folder to view its content.
    b. From the **Items** column, select the Playbook you wish to execute and click **>**. The Playbook will appear in the **Selections** column. You may also search for Playbooks by using the Items **Search...** field.
    If you wish to remove a Playbook from the **Selections** column, select the Playbook you wish to remove and click **<**.
    c. When ready to execute your Playbook, click **Execute**. The **Playbook Execution Result** window appears. This window provides a summary of result. Clicking **Details** will display additional information. Click on **View Output** to view any information related on a specific Playbook topic (Summary, Details, a specific attribute if applicable).
    d. When done, click **Close**.

Running a Connector

FortiSOAR Connectors are used to take a specific action on a third-party device.

- Running a Connector on an Event
- Running a Connector on an Incident

Running a Connector on an Event

To run a Connector on an event, take the following steps.

1. From the **ANALYTICS** page, select an event.
2. Click **Run Connector**.
3. From the **Run Connector** window, take the following steps.
    a. From the **Folders** column, select the Connector you want to run. When a Connector is selected, a list of available actions for that Connector will auto-populate under the **Items** column.
    b. From the **Items** column, select the desired Connector action and click **>** to add it to the **Selections** column. A **Select Connector Parameters** section may appear that is specific to the FortiSOAR Connector, if additional parameter information is needed. The parameters that appear will vary per Connector and specification type.
    Note: If you wish to remove a Connector action from the **Selections** column, select the Connector action you wish to remove and click **<**.
    c. If the **Select Connector Parameters** section appears based on the Connector action selected, populate the Connector parameters required to run the Connector action. Refer to FortiSOAR documentation for a given Connector for information regarding requirements.**Note**: The first parameter on nearly all Connectors is the Connector Config, which is essentially a descriptive name for a credential set for a given application, service, or device on FortiSOAR for that Connector type.
    An example is the Fortinet Fortigate Connector. Each Connector configuration is an binding of credential (API key) to a particular firewall. When you select this Connector configuration, the action will be executed on that firewall.
    d. When done, click **Execute**. FortiSIEM will call the given Connector using the parameters specified. The **Connector Result** window appears. This window provides a summary of result. Clicking **Details** will display additional information. Click on **View Output** to view any information related on a specific

Connector topic (Summary, Details, a specific attribute if applicable).

e. When done, click **Close**.

Machine Learning

The following sections provide information and procedures for Machine Learning:

Overview

FortiSIEM 7.0.0 introduces Machine Learning, which allows you to run various Machine Learning tasks on data collected by FortiSIEM.

Machine Learning Job Types

The following Machine Learning Tasks are supported:

- **Anomaly Detection** - The objective of an Anomaly Detection task is to learn what is normal in a dataset, and create an alert if the new values deviate from the normal dataset, by user specified threshold. Learning is done during the Training phase and alert creation is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.
- **Classification** – The objective of a Classification task to learn how to assign labels to items based on various fields in a dataset and then assign a label to a new item based on current values. This requires labels to be present in the dataset. Labels can be binary e.g. malware/not malware, spam/not-spam, or can belong to more than 2 classes as well. Learning the label assignment is done during the Training phase and assigning labels to new data is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.
- **Clustering** - The objective of a Clustering task is to group similar items based on a set of fields in a dataset, and then create an alert if an item belongs to a different group based on current values. Learning the groups is done during the Training phase and alert creation is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.
- **Forecasting** – The objective of a Forecasting task is to learn a time based trend of a field in a dataset and then predict future values of that field. Learning the time based trend is done during the Training phase and future prediction is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.
- **Regression** - The objective of a Regression task is to build a model for predicting a Target field based on other fields in a dataset, and then create an alert if the new values of the Target field exceeds the predicted value, by user specified threshold. Building the prediction model is done during the Training phase and alert creation is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.

Running Modes and Algorithms

The following Machine Learning running modes are supported:

- **Local** – In this mode, both Training and Inference phases run on the Supervisor and Worker cluster. During the Training phase, the user has to choose the Machine Learning Algorithm and its optimal parameters.
- **Local Auto** – In this mode, both Training and Inference phases run on the Supervisor and Worker cluster. FortiSIEM picks the best Machine Learning Algorithm with a tuned parameter set. In contrast to Local mode, the Training phase in Local Auto mode takes a significantly longer time to complete, since many algorithms are evaluated and the performance of each algorithm is optimized by tuning the parameter set.
- **AWS** - In this mode, both the Training and Inference stages take place on AWS. It is important to note that for regression, BinaryClassification, and MulticlassClassification, the algorithm parameters can be auto-tuned on AWS and the user can also define the Object Metric for Hyperparameter Tuning Job. However, for Anomaly Detection and Clustering, the user is required to configure the algorithm parameters themselves.
- **AWS Auto** - In this mode, Amazon SageMaker Autopilot helps you automatically build, train, and tune the best machine learning models without manual model selection and tuning. Although the training time might be longer (2 – 3 hours), using Autopilot can still be suitable when facing a dataset with a large number of features and complexity, Autopilot can automatically perform feature engineering and select the best model, helping you achieve good results in a short amount of time.

The following table shows the supported Machine Learning algorithms for each Task type and running mode.

Task	Running Mode	Supported Machine Learning Algorithms
Anomaly Detection	Local	Local Outlier Factor, Elliptic Envelope, Isolation Forest, Statistical Deviation, Bipartite Edge Anomaly Detection (Proprietary)
	AWS	Random Cut Forest
Classification	Local	Logistic Regression, Decision Tree Classifier, Random Forest Classifier, SGDClassifier, Support Vector Classifier (SVC)
	Local Auto	Decision Tree Classifier, Random Forest Classifier, SGDClassifier, Support Vector Classifier (SVC)
Binary Classification	AWS	Linear Learner
	AWS Auto	See https://docs.aws.amazon.com/sagemaker/latest/dg/autopilot-model-support-validation.html
Multiclass Classification	AWS	Linear Learner
	AWS Auto	See https://docs.aws.amazon.com/sagemaker/latest/dg/autopilot-model-support-validation.html
Clustering	Local	KMeans, GMeans, DBScan, BIRCH, Spectral Clustering
	Local Auto	BIRCH, DBSscan, KMeans
	AWS	KMeans

Task	Running Mode	Supported Machine Learning Algorithms
Forecasting	Local	ARIMA, State Space Dynamic factor MQ
Regression	Local	Linear Regression, Decision Tree Regressor, Random Forest Regressor, SGDRegressor, Support Vector Regression (SVR)
	Local Auto	Decision Tree Regressor, Random Forest Regressor, SGDRegressor, Support Vector Regression (SVR)
	AWS	Linear Learner
	AWS Auto	See https://docs.aws.amazon.com/sagemaker/latest/dg/autopilot-model-support-validation.html

A Machine Learning Job

The concept of a Machine Learning Job is introduced. It consists of the following attributes:

- **Job Id** – The unique ID for this job, assigned by FortiSIEM.
- **Scope** – System defined or User defined. System defined Jobs are provided by FortiSIEM. User defined jobs are created by the user. Note that System defined jobs are simply templates and must be trained.
- **Name** – Name of the job.
- **Description** – Description of the job.
- **Task** – One of the following Machine Learning Task Categories: Anomaly Detection, Regression, Clustering, Forecasting, Classification.
- **Machine Learning Algorithm** – A relevant algorithm for the Machine Learning Task.
- **Report** – The FortiSIEM Report that provides the data for training and inference.
- **Report Time Window** – The time window for which the report must be run. In other words, the fataset contains data during this Report Time Window.
- **Target** – The fields in the FortiSIEM Report that should be used as the target for the Machine Learning Task.
- **Features** – The fields in the FortiSIEM Report that should be used as the features for the Machine Learning Task.
- **Organization** (For FortiSIEM Service Provider deployments only) – The Organization for which the Report must be run. Currently the supported values are – All Organization data combined or a specific Organization at a time. In other words, if you want to run the machine learning task for 2 Organizations, then 2 separate Machine Learning jobs must be created.
- **Inference Schedule** – The frequency at which inference must be done. The purpose of Inference is to detect deviations from the model built during Training phase or to create future data for Forecasting.
- **Re-training Schedule** – The frequency at which training must be repeated. The purpose of retraining is to capture new patterns in the data.
- **Action** – Specifies the action to be taken after Inference is completed: whether to create an Alert or send an email containing the anomalies found.

System defined Machine Learning Job templates are provided in **Resources > Machine Learning Jobs**. Note that these are templates and cannot be run like Rules and Reports, since they are missing the Machine Learning model. A System defined Machine Learning Job does not set the following attributes:

1. Report Time Window
2. Organization

3. Inference Schedule
4. Re-training schedule
5. Action

These attributes must be provided by the user while training and scheduling a machine learning job.

Running a System Defined Machine Learning Job

To build a model and schedule a System defined job, the user must take the following steps:

1. Go to **Analytics > Machine Learning** and select the job.
2. Create an input dataset by running the report
   a. Choose Report Time Window
   b. Chose Organization for FortiSIEM Service Provider deployments
3. Train the dataset from **Analytics >Train**. A model will be built. You can tune the tune the algorithm parameters and Train again.
4. Once the model is ready, you can schedule the job to run for Inference from **Analytics >Schedule**.
5. A new job id will be assigned and will show in **Resources > Machine Learning Jobs** as an User defined job.
6. As part of Inference action, the alert will show up in Incidents or email will be sent.
7. You can edit the Inference and Re-training schedules by editing a job in **Resources > Machine Learning Jobs**.

Creating a Machine Learning Job From Scratch

A Machine Learning job can also be created from scratch. To do this, the user must take the following steps:

1. Navigate to **Analytics > Machine Learning** and Select a Report from the **Reports > Machine Learning Reports** folder. If the report is not present in that folder, then you can pre-built a report from **Analytics > Search** and save it in **Reports > Machine Learning Reports** before proceeding.
2. Create an input dataset by running the report
   a. Choose Report Time Window
   b. Chose Organization for FortiSIEM Service Provider deployments
3. Train the dataset from **Analytics >Train**.
   a. Choose **Run Mode**.
   b. Choose **Task**.
   c. Choose **Algorithm** and tune the parameters if needed.
   d. Choose **Training factor**.
   e. Click **Train**. You can tune the tune the algorithm parameters and Train again.
4. Once the model is ready, you can schedule the job to run for Inference from **Analytics >Schedule**.
5. A new job id will be assigned and will show in **Resources > Machine Learning Jobs** as an User defined job.
6. As part of Inference action, the alert will show up in Incidents or email will be sent.
7. You can edit the Inference and Re-training schedules by editing a job in **Resources > Machine Learning Jobs**.

Anomaly Detection

The objective of an Anomaly Detection Task is to learn what is normal in a dataset, and create an alert if the new values deviate from the normal dataset, by user specified threshold. Learning is done during the Training phase and alert creation is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.

- Anomaly Detection Algorithms for Local Mode
- Running Anomaly Detection Local Mode
- Anomaly Detection Algorithms for AWS Mode
- Running Anomaly Detection AWS Mode

Anomaly Detection Algorithms for Local Mode

In this mode, the following algorithms can run *locally* within the FortiSIEM Supervisor/Worker cluster.

Bipartite Graph Edge Anomaly Detection Algorithm

This is a proprietary machine learning algorithm that tries to detection login anomalies by learning the login patterns and forming dynamic user peer groups. A bipartite graph is a graph where the sets of nodes can be split into two disjoint sets such that there are no edges between the nodes within the same set. An example is Users and Workstations where the edge between a user and a Workstation represents a login, and the edge weight can be the number of logins. The anomaly detection algorithm works as follows. During the training phase, a similarity score between a user/workstation and another user/workstation is calculated. The principle behind similarity score calculation is as follows:

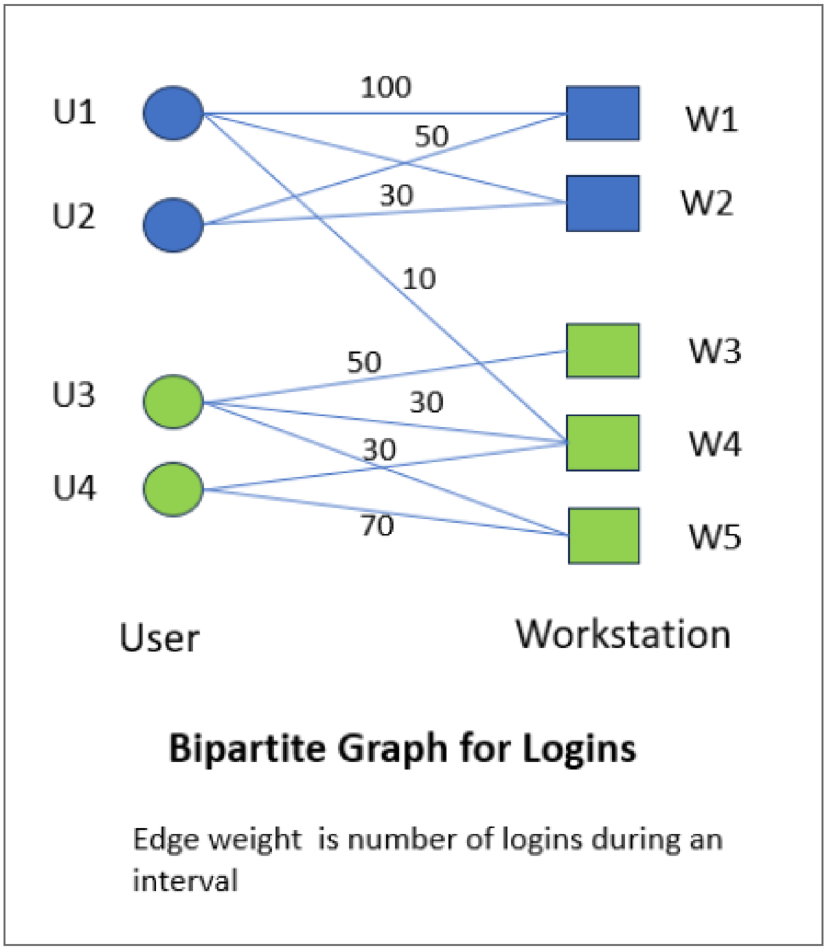
- The similarity score between a user and a workstation is high if the user accesses that workstation.
- The similarity score between two users is high if they access similar workstations.
- The similarity score between two workstations is high if they are accessed by a common set of users.

During testing and inference phases, a login from user (A) to a workstation (B) is considered anomalous if the similarity score between user A and the other users that typically access workstation B is lower than a user defined threshold. More specifically:

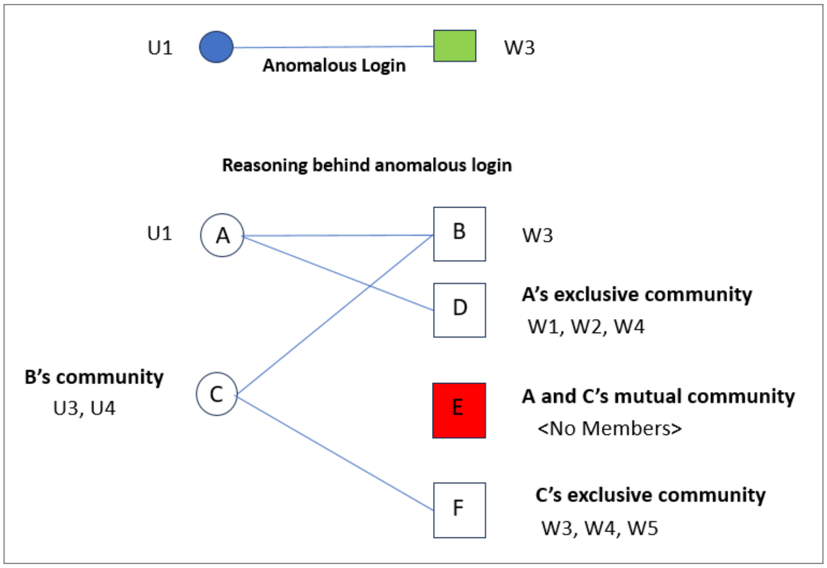
- C: The set of users that access workstation B during training phase. This is B’s community.
- E: The set of workstations that are accessed by both A and C during training phase. This is A and C’s mutual community.
- D: The set of workstations that are accessed by only A during training phase. This is A’s exclusive community.
- F: The set of workstations that are accessed by only C during training phase. This is C’s exclusive community.

For an anomaly to occur, the set of workstations E should be far fewer compared to set of Workstations D (A’s exclusive community) and F (C’s exclusive community). If this is not the case, then consider reducing the anomaly threshold.

As an example, consider the following login scenario between users U1, U2, U3, U4 and Workstations W1, W2, W3, W4. The login is modeled as a weighted Bipartite graph as shown below.


U1
U2
U3
U4
W1
W2
W3
W4
W5
100
50
30
10
50
30
30
70
User
Workstation
Bipartite Graph for Logins
Edge weight is number of logins during an interval

A login from user U1 to Workstation W3 is considered an anomaly because user U1 and W3's user community (namely U3 and U4) do not access common workstations.



There are 3 parameters for this algorithm:

- **Threshold** : Scores lower than this threshold is considered anomalous.
- **Max node degree**: Nodes with degree higher than this value will be ignored. In the User and Workstation case.
  - Users that access more than max node degree workstations will be ignored.
  - Workstations that are accessed by more than max node degree users will be ignored.
- **Convergence bound**: Bipartite Edge Anomaly Algorithm stops if the change in reward matrix is lower than this value. This is an internal parameter.

The following groups of users/workstations are eliminated during testing and inference phases, and they do not raise incidents:

1. Users that access many workstations (e.g., Domain Admins in Microsoft Active Directory environments).
2. Workstations that are accessed by many users (e.g., Microsoft Active Directory)
3. Users or Workstations that were never seen during the training phase and hence not part of the model. A periodic retraining would resolve this issue.

Elliptic Envelope Algorithm

An *unsupervised* anomaly detection algorithm which constructs an ellipsoid around the center of the data points. If a data point falls outside the Ellipsoid, then it is considered as an anomaly. This is suitable for Gaussian distributed data. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.covariance.EllipticEnvelope.html

Isolation Forest Algorithm

An *unsupervised* anomaly detection algorithm that builds a random tree by randomly selecting a feature and then randomly selecting a split value between the maximum and minimum values of that feature. If a data point has a small path from the root of the tree, then it is considered as an anomaly. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.IsolationForest.html

Local Outlier Factor Algorithm

An *unsupervised* anomaly detection algorithm which computes the local density deviation of a data point with respect to its neighbors. If a data point has substantially lower density than their neighbors, then it is considered as an anomaly. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.neighbors.LocalOutlierFactor.html

Statistical Deviation Algorithm

An *unsupervised* anomaly detection algorithm based on mean, median, standard deviation and absolute median deviation. A data point is considered an anomaly if the difference between current value and sample mean (or sample median) in a Window is more than a user specified multiplier times the standard deviation (respectively absolute median deviation) over the same window. This is a generalization of the Z-score based methods. The parameters for this algorithm are:

- *Mode*: Std (meaning Standard Deviation) or Median Absolute (meaning MedAbs)
- *Multiplier*: It will be used to calculate the lower/upper bound
- *Window*: Length of sliding window for calculating mean, median and standard deviation

Specially,

- For **Mode=Std**: a data point is anomalous if the absolute difference between current value and sample mean in the Window is more than Multiplier times the Standard Deviation over the same Window
- For **Mode= MedAbs**: a data point is anomalous if the absolute difference between current value and sample median in the Window is more than Multiplier times the Median Deviation over the same Window

Running Anomaly Detection Local Mode

Step 1: Design

First identify the following items:

- Fields to Analyze – these fields will be considered for anomaly detection. Currently each field must be a numerical field.
- Time field – this field is required for Statistical Deviation algorithms. It is optional for other algorithms.
- A FortiSIEM Report to get this data.

Requirements

1. Report must contain one or more numerical fields to use for anomaly detection. To provide several samples, you can provide a time field. This is optional.
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be columns other than the Fields to Analyze in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**, and click the Import Machine Learning Jobs (open folder) icon.
2. Select the data source in one of three ways:
   a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
   b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Jobs** folder
   c. To prepare data from a CSV file, choose **Import via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.

Step 3: Train

Train the Anomaly Detection task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import Via Jobs**, then make sure the Fields to Analyze are populated correctly.
3. If you chose **Import Via Report** or **Import Via CSV File**, then
    a. Set **Run Mode** to Local
    b. Set **Task** to Anomaly Detection
    c. Choose the **Algorithm**
    d. Choose the **Fields to Analyze** from the report fields.
4. Specify a *threshold* for detecting anomalies.
    - For **Local Outlier Factor**, **Elliptic Envelope**, **Isolation Forest** algorithms, the threshold is the **Contamination** parameter. Contamination is between 0 and 1 and specifies the proportion of the data that can be considered anomalous. If Contamination is 0.1, then roughly 10% of the data will be detected as anomalous during the training phase.
    - For **Statistical Deviation** algorithm, the threshold is the Multiplier parameter:
        - For **Statistical Deviation and Mode=Std**: a data point is anomalous if the absolute difference between current value and *sample mean* in the Window is more than *Multiplier* times the *Standard Deviation* over the same *Window*.
        - For **Statistical Deviation and Mode= MedAbs**: a data point is anomalous if the absolute difference between current value and *sample median* in the Window is more than *Multiplier* times the *Median Deviation* over the same *Window*.
    - For **Bipartite Graph Edge Anomaly Detection**, scores lower than the **threshold** is considered anomalous.
5. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
6. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab. For Anomaly detection, results includes **Model Quality** and **Anomalies found**.

Model Quality:

The following metrics show the quality of the anomaly detection algorithm.

- **Anomalies Found**: This shows the number of anomalies in the data.
- **Normal Results**: This shows the number of normal (or non-anomalous) results.

Anomaly Detection Results:

The Anomaly Detection Results table shows which results are anomalous (*isAnomaly* = 1).

- For **Statistical Deviation**: The columns avg, stddev, lower_bound, upper_bound are added to the table.
- For **Regression Deviation**: The columns avg, stddev, lower_bound, upper_bound are added to the table
- **Anomaly Details > Trend View**: For **Statistical Deviation**, this area shows a time trend and shows where anomaly occurs.

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**. Note the important tuning parameters are

- For **Local Outlier Factor**, **Elliptic Envelope**, **Isolation Forest** algorithms, the threshold is the **Contamination** parameter.
- For **Statistical Deviation** algorithm, the threshold is the **Multiplier** parameter.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.
  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when an anomaly is found during the Inference process.
  - Two choices are available – creating a FortiSIEM Incident or sending an email. Specify the emails if you want emails to be sent. Make sure that email server is specified in **Admin > Settings > Email**.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Anomaly Detection Algorithms for AWS Mode

In this mode, the following algorithm runs in AWS. The following algorithm is supported.

Random Cut Forest

Random Cut Forest is an *unsupervised* anomaly detection algorithm that builds a random tree by randomly selecting a feature and then randomly selecting a split value between the maximum and minimum values of that feature. If a new data point changes the tree structure, then it is considered as an anomaly. The parameters for this algorithm are described here:

Running Anomaly Detection AWS Mode

Step 0: Set Up AWS

Set up AWS SageMaker by following the instructions in Set Up AWS SageMaker.

Configure AWS in FortiSIEM by following the instructions in Configure FortiSIEM to use AWS SageMaker.

Step 1: Design

First identify the following items:

- Fields to Analyze – these fields will be considered for anomaly detection. Currently each field must be a numerical field.
- Time field – this field is required for Statistical Deviation algorithms. It is optional for other algorithms.
- A FortiSIEM Report to get this data.

Requirements

1. Report must contain one or more numerical fields to use for anomaly detection. To provide several samples, you can provide a time field. This is optional.
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be columns other than the Fields to Analyze in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**, and click the Import Machine Learning Jobs (open folder) icon.
2. Select the data source in one of three ways:
    a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
    b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Jobs** folder
    c. To prepare data from a CSV file, choose **Import via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report Time Interval and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.

Step 3: Train

Train the Anomaly Detection task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the Fields to Analyze are populated correctly.
3. If you chose **Import via Report** or **Import Via CSV File**, then
    a. Set **Run Mode** to AWS
    b. Set **Task** to Anomaly Detection
    c. Choose the **Algorithm**
    d. Choose the **Fields to Analyze** from the report fields.

4. Specify the parameters for Random Cut Forest.
5. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
6. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.
  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when an anomaly is found during the Inference process.
  - Two choices are available – creating a FortiSIEM Incident or sending an email. Specify the emails if you want emails to be sent. Make sure that email server is specified in **Admin > Settings > Email**.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Classification

The objective of a Classification Task to learn how to assign labels to items based on various fields in the dataset and then assign a label to new item based on current values. This requires labels to be present in the dataset. Labels can be binary e.g. malware/not malware, spam/not-spam or can belong to more than 2 classes as well. Learning the label assignment is done during the Training phase and assigning labels to new data is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.

Classification Algorithms for Local Mode

In this mode, the following algorithms can run *locally* within the FortiSIEM Supervisor/Worker cluster.

- **Decision Tree Classifier**: A *supervised* classification algorithm that uses a Decision Tree constructed using the feature variables to classify new data points. It requires a set of pre-labelled data points during the training process to construct the tree.
- **Logistic Regression**: A *supervised binary* classification algorithm that can classify data points into two classes based on sigmoid function using a set of features. It requires a set of pre-labelled data points during the training process.
- **Random Forest Classifier**: A *supervised* classification algorithm that uses Ensemble learning and Bootstrapping techniques to improve the accuracy of Decision Tree based classification algorithms. Ensemble learning uses multiple models and Bootstrapping randomly samples datasets and then averages the results of each model to improve accuracy. It requires a set of pre-labelled data points during the training process to construct the trees.
- **SGDClassifier**: A *supervised* classification algorithm that uses Stochastic Gradient Descent (SGD) update techniques for existing classifiers and is computationally efficient for large datasets. It requires a set of pre-labelled data points during the training process.
- **Support Vector Classifier**: Support Vector Classifier (SVC), also called Linear Support Vector Machine (SVM), is a *supervised* classification algorithm that separates data points using a hyperplane with specified margins (support vector). It requires a set of pre-labelled data points during the training process.

Running Classification Local Mode

Step 1: Design

First identify the following items:

- **Fields to use for Classification**: Each field must be a numerical field.
- **Class Label**: The class to which the data corresponds to.
- A **FortiSIEM Report** to get this data.

To provide several samples of the data, you can choose one of the following time attributes as a report column

- Event Receive Hour
- Event Receive Date

Requirements

1. Report must contain
    - A Class Label
    - One or more numerical fields to use for classification

    To provide several samples, you can provide a time field. This is optional.
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be additional columns in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**, and click the Import Machine Learning Jobs (open folder) icon.
2. Select the data source in one of three ways:
    1. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
    2. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Job** folder
    3. To prepare data from a CSV file, choose **Import Via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.

Step 3: Train

Train the Classification task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the **Class Label** and **Fields to use for Classification** are populated correctly.
3. If you chose **Import via Report** or **Import via CSV File**, then
    1. Set **Run Mode** to Local
    2. Set **Task** to Classification
    3. Choose the **Algorithm**
    4. Choose the **Class Label** and **Fields to use for Classification** from the report fields.
4. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
5. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

Model Quality:

The following metrics show the quality of the clusters found.

- **True Positives (TP)**: Correct classification for label = 0, i.e. actual = 0 and predicted = 0
- **True Negative (TN)**: Correct classification for label = 1, i.e. actual = 1 and predicted = 1
- **False Positive (FP)**: Incorrect classification for label = 0, i.e. actual = 0 and predicted = 1
- **False Negative (FN)**: Incorrect classification for label = 1, i.e. actual = 1 and predicted = 0
- **Accuracy**: Accuracy is the total number of correct classification divided by the total number of attempted classification, i.e. ((TP+TN)/(TP+TN+FP+FN)). It is between 0 and 1. A score close to 1 means accurate classification.
- **Recall**: Recall is calculated by dividing the True Positives by anything that should have been predicted as Positive. So Recall is FP/(FP+TN).
- **Precision**: Precision is calculated by dividing the True Positives by anything that was classified as a Positive. So Precision is TP/(TP+FP).
- **F1 Score**: F1 Score combines Precision and Recall into a single metric by taking their harmonic mean. F1 Score = 2 / ((1/Precision)+(1/Recall)). It ranges from 0-1, and a higher F1 score denotes a better quality classifier.
- **ROC AUC**: It measures the entire two-dimensional area underneath the entire ROC curve (think integral calculus) from (0,0) to (1,1). It tells how much the model is capable of distinguishing between classes. Higher ROC AUC values indicate that the model is better at predicting 0 classes as 0 and 1 classes as 1.
- **Confusion Matrix**: presents TP, TN, FP and FN in a matrix

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.
  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when an anomaly is found during the Inference process.
  - Two choices are available – creating a FortiSIEM Incident or sending an email. Specify the emails if you want emails to be sent. Make sure that email server is specified in **Admin > Settings > Email**.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Classification Algorithms for Local Auto Mode

In this mode, FortiSIEM picks the best algorithm from the following:

- Decision Tree Classifier
- Random Forest Classifier
- SGDClassifier
- Support Vector Classifier (SVC)

Note: The **Max Run Time** parameter is used to limit the amount of time this job runs. By default it is set to 5 minutes. The longer this job runs, potentially better result can be generated.

Running Classification Local Auto Mode

To run, follow the Classification steps in Algorithms for Local Mode, but in Step 3, 3a, select **Run Mode** as **Local Auto**.

Classification Algorithms for AWS Mode

In this mode, the following algorithms runs in AWS. The following algorithms are supported.

- **Linear Learner Algorithms**: Linear models are supervised learning algorithms used for solving either classification or regression problems. For more information, see https://docs.aws.amazon.com/sagemaker/latest/dg/linear-learner.html

Running Classification AWS Mode

Step 0: Set Up AWS

Set up AWS SageMaker by following the instructions in Set Up AWS SageMaker.

Configure AWS in FortiSIEM by following the instructions in Configure FortiSIEM to use AWS SageMaker.

Step 1: Design

First identify the following items:

- **Fields to use for Classification**: Each field must be a numerical field.
- **Class Label**: The class to which the data corresponds to.
- A **FortiSIEM Report** to get this data.

To provide several samples of the data, you can choose one of the following time attributes as a report column

- Event Receive Hour
- Event Receive Date

Requirements

1. Report must contain
   - A Class Label
   - One or more numerical fields to use for classification

   To provide several samples, you can provide a time field. This is optional.
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be additional columns in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**, and click the Import Machine Learning Jobs (open folder) icon.
2. Select the data source in one of three ways:
   a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
   b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Job** folder
   c. To prepare data from a CSV file, choose **Import Via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.

Step 3: Train

Train the Classification task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the **Class Label** and **Fields to use for Classification** are populated correctly.
3. If you chose **Import via Report** or **Import via CSV File**, then
   a. Set **Run Mode** to AWS
   b. Set **Task** to Classification
   c. Choose the **Algorithm**
   d. Choose the **Class Label** and **Fields to use for Classification** from the report fields.
4. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
5. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

Model Quality:

The following metrics show the quality of the clusters found.

Binary Classification

- **True Positives (TP)**: Correct classification for label = 0, i.e. actual = 0 and predicted = 0
- **True Negative (TN)**: Correct classification for label = 1, i.e. actual = 1 and predicted = 1
- **False Positive (FP)**: Incorrect classification for label = 0, i.e. actual = 0 and predicted = 1
- **False Negative (FN)**: Incorrect classification for label = 1, i.e. actual = 1 and predicted = 0

- **Precision**: The precision of the final model on the validation dataset. If you choose this metric as the objective, we recommend setting a target recall by setting the binary_classifier_model_selection hyperparameter to precision_at_target_recall and setting the value for the target_recall hyperparameter. This objective metric is only valid for binary classification.
- **Recall**: The recall of the final model on the validation dataset. If you choose this metric as the objective, we recommend setting a target precision by setting the binary_classifier_model_selection hyperparameter to recall_at_target_precision and setting the value for the target_precision hyperparameter. This objective metric is only valid for binary classification.
- **roc_auc_score**: The area under receiving operating characteristic curve (ROC curve) of the final model on the validation dataset. This objective metric is only valid for binary classification.
- **binary_classification_accuracy**: The accuracy of the final model on the validation dataset. This objective metric is only valid for binary classification.
- **binary_f_beta**: The F-beta score of the final model on the validation dataset. By default, the F-beta score is the F1 score, which is the harmonic mean of the validation:precision and validation:recall metrics. This objective metric is only valid for binary classification.
- **Confusion Matrix**: Presents TP, TN, FP and FN in a matrix

Multiclass Classification

- **Dcg**: The discounted cumulative gain of the final model on the validation dataset. This objective metric is only valid for multiclass classification.
- **multiclass_accuracy**: The accuracy of the final model on the validation dataset. This objective metric is only valid for multiclass classification.
- **multiclass_top_k_accuracy**: The accuracy among the top k labels predicted on the validation dataset. If you choose this metric as the objective, we recommend setting the value of k using the accuracy_top_k hyperparameter. This objective metric is only valid for multiclass classification.

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.

  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.
  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when an anomaly is found during the Inference process.
  - Two choices are available – creating a FortiSIEM Incident or sending an email. Specify the emails if you want emails to be sent. Make sure that email server is specified in **Admin > Settings > Email**.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Classification Algorithms for AWS Auto Mode

In this mode, FortiSIEM automatically chooses the best algorithm with the optimal parameters. Depending on the size of your dataset (whether is it greater or smaller than 100MB), algorithms from HPO mode or from ensembling mode will be considered. For more information, see https://docs.aws.amazon.com/sagemaker/latest/dg/autopilot-model-support-validation.html. Definitions below taken from Amazon SageMaker Developer Guide.

HPO mode (Dataset > 100MB)

- **Linear learner**: A supervised learning algorithm that can solve either classification or regression problems.
- **XGBoost**: A supervised learning algorithm that attempts to accurately predict a target variable by combining an ensemble of estimates from a set of simpler and weaker models.
- **Deep learning algorithm**: A multilayer perceptron (MLP) and feedforward artificial neural network. This algorithm can handle data that is not linearly separable.

Ensembling mode (Dataset <=100MB)

- **LightGBM**: An optimized framework that uses tree-based algorithms with gradient boosting. This algorithm uses trees that grow in breadth, rather than depth, and is highly optimized for speed.
- **CatBoost**: A framework that uses tree-based algorithms with gradient boosting. Optimized for handling categorical variables.
- **XGBoost**: A framework that uses tree-based algorithms with gradient boosting that grows in depth, rather than breadth.
- **Random Forest**: A tree-based algorithm that uses several decision trees on random sub-samples of the data with replacement. The trees are split into optimal nodes at each level. The decisions of each tree are averaged together to prevent overfitting and improve predictions.
- **Extra Trees**: A tree-based algorithm that uses several decision trees on the entire dataset. The trees are split randomly at each level. The decisions of each tree are averaged to prevent overfitting and to improve predictions. Extra trees add a degree of randomization in comparison to the random forest algorithm.
- **Linear Models**: A framework that uses a linear equation to model the relationship between two variables in observed data.
- **Neural network torch**: A neural network model that is implemented using Pytorch.
- **Neural network fast.ai**: A neural network model that is implemented using fast.ai.

Note: The Max Run Time parameter is used to limit the amount of time this job runs. By default it is set to 225 minutes.

The longer this job runs, potentially better results can be generated.

Running Classification AWS Auto Mode

To run, follow the Regression steps in Algorithm for AWS Mode, but in Step 3, 3a, select **Run Mode** as **AWS Auto**.

For Step 3, the following model quality information pertains.

Model Quality:

The following metrics show the quality of the clusters found.

Binary Classification

- **True Positives (TP)**: Correct classification for label = 0, i.e. actual = 0 and predicted = 0
- **True Negative (TN)**: Correct classification for label = 1, i.e. actual = 1 and predicted = 1
- **False Positive (FP)**: Incorrect classification for label = 0, i.e. actual = 0 and predicted = 1
- **False Negative (FN)**: Incorrect classification for label = 1, i.e. actual = 1 and predicted = 0
- **F1**: The F1 score is the harmonic mean of the *precision* and *recall*, defined as follows: F1 = 2 * (*precision* * *recall*) / (*precision* + *recall*). It is used for binary classification into classes traditionally referred to as positive and negative. Predictions are said to be true when they match their actual (correct) class, and false when they do not.
Precision is the ratio of the true positive predictions to all positive predictions, and it includes the false positives in a dataset. *Precision* measures the quality of the prediction when it predicts the positive class.
Recall (or sensitivity) is the ratio of the true positive predictions to all actual positive instances. *Recall* measures how completely a model predicts the actual class members in a dataset.
F1 scores vary between 0 and 1. A score of 1 indicates the best possible performance, and 0 indicates the worst.
- **LogLoss**: Log loss, also known as cross-entropy loss, is a metric used to evaluate the quality of the probability outputs, rather than the outputs themselves. It is used in both binary and multiclass classification and in neural nets. It is also the cost function for logistic regression. Log loss is an important metric to indicate when a model makes incorrect predictions with high probabilities. Values range from 0 to infinity. A value of 0 represents a model that perfectly predicts the data.
- **Recall**: Recall measures how well an algorithm correctly predicts all of the true positives (TP) in a dataset. A true positive is a positive prediction that is also an actual positive value in the data. Recall is defined as follows: Recall = TP/(TP+FN), with values ranging from 0 to 1. Higher scores reflect a better ability of the model to predict true positives (TP) in the data. It is used in binary classification.
Recall is important when testing for cancer because it's used to find all of the true positives. A false positive (FP) reflects a positive prediction that is actually negative in the data. It is often insufficient to measure only recall, because predicting every output as a true positive yields a perfect recall score.
- **Precision**: Precision measures how well an algorithm predicts the true positives (TP) out of all of the positives that it identifies. It is defined as follows: Precision = TP/(TP+FP), with values ranging from zero (0) to one (1), and is used in binary classification. Precision is an important metric when the cost of a false positive is high. For example, the cost of a false positive is very high if an airplane safety system is falsely deemed safe to fly. A false positive (FP) reflects a positive prediction that is actually negative in the data.
- **AUC**: The area under the curve (AUC) metric is used to compare and evaluate binary classification by algorithms that return probabilities, such as logistic regression. To map the probabilities into classifications, these are compared against a threshold value.
The relevant curve is the receiver operating characteristic curve (ROC curve). The ROC curve plots the true positive rate (TPR) of predictions (or recall) against the false positive rate (FPR) as a function of the threshold value, above which a prediction is considered positive. Increasing the threshold results in fewer false positives, but more

false negatives.
AUC is the area under this ROC curve. Therefore, AUC provides an aggregated measure of the model performance across all possible classification thresholds. AUC scores vary between 0 and 1. A score of 1 indicates perfect accuracy, and a score of one half (0.5) indicates that the prediction is not better than a random classifier.

- **Accuracy**: The ratio of the number of correctly classified items to the total number of (correctly and incorrectly) classified items. It is used for both binary and multiclass classification. Accuracy measures how close the predicted class values are to the actual values. Values for accuracy metrics vary between zero (0) and one (1). A value of 1 indicates perfect accuracy, and 0 indicates perfect inaccuracy.
- **BalancedAccuracy**: BalancedAccuracy is a metric that measures the ratio of accurate predictions to all predictions. This ratio is calculated after normalizing true positives (TP) and true negatives (TN) by the total number of positive (P) and negative (N) values. It is used in both binary and multiclass classification and is defined as follows: 0.5*((TP/P)+(TN/N)), with values ranging from 0 to 1. BalancedAccuracy gives a better measure of accuracy when the number of positives or negatives differ greatly from each other in an imbalanced dataset, such as when only 1% of email is spam.

Multiclass Classification:

- **F1macro**: The F1macro score applies F1 scoring to multiclass classification problems. It does this by calculating the precision and recall, and then taking their harmonic mean to calculate the F1 score for each class. Lastly, the F1macro averages the individual scores to obtain the F1macro score. F1macroscores vary between 0 and 1. A score of 1 indicates the best possible performance, and 0 indicates the worst.
- **PrecisionMacro**: The precision macro computes precision for multiclass classification problems. It does this by calculating precision for each class and averaging scores to obtain precision for several classes. PrecisionMacro scores range from zero (0) to one (1). Higher scores reflect the model's ability to predict true positives (TP) out of all of the positives that it identifies, averaged across multiple classes.
- **Accuracy**: The ratio of the number of correctly classified items to the total number of (correctly and incorrectly) classified items. It is used for both binary and multiclass classification. Accuracy measures how close the predicted class values are to the actual values. Values for accuracy metrics vary between zero (0) and one (1). A value of 1 indicates perfect accuracy, and 0 indicates perfect inaccuracy.
- **BalancedAccuracy**: BalancedAccuracy is a metric that measures the ratio of accurate predictions to all predictions. This ratio is calculated after normalizing true positives (TP) and true negatives (TN) by the total number of positive (P) and negative (N) values. It is used in both binary and multiclass classification and is defined as follows: 0.5*((TP/P)+(TN/N)), with values ranging from 0 to 1. BalancedAccuracy gives a better measure of accuracy when the number of positives or negatives differ greatly from each other in an imbalanced dataset, such as when only 1% of email is spam.
- **LogLoss**: Log loss, also known as cross-entropy loss, is a metric used to evaluate the quality of the probability outputs, rather than the outputs themselves. It is used in both binary and multiclass classification and in neural nets. It is also the cost function for logistic regression. Log loss is an important metric to indicate when a model makes incorrect predictions with high probabilities. Values range from 0 to infinity. A value of 0 represents a model that perfectly predicts the data.
- **RecallMacro**: The RecallMacro computes recall for multiclass classification problems by calculating recall for each class and averaging scores to obtain recall for several classes. RecallMacro scores range from 0 to 1. Higher scores reflect the model's ability to predict true positives (TP) in a dataset, whereas a true positive reflects a positive prediction that is also an actual positive value in the data. It is often insufficient to measure only recall, because predicting every output as a true positive will yield a perfect recall score.

Clustering

The objective of a Clustering Task is to group similar items based on a set of fields in a dataset, and then create an alert if an item belongs to a different group based on current values. Learning the groups is done during the Training phase and alert creation is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.

Clustering Algorithm for Local Mode

In this mode, the following algorithms can run *locally* within the FortiSIEM Supervisor/Worker cluster.

- **BIRCH**: Balanced Iterative Reducing and Clustering using Hierarchies (BIRCH) is an *unsupervised* clustering algorithm for grouping particularly large data-sets. It takes a hierarchical approach by first summarizing large data-sets into smaller, dense regions called Clustering Feature (CF) entries and then clustering the smaller data set. It only works for numerical entries. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.cluster.Birch.html
- **DBScan**: Density-Based Spatial Clustering of Applications with Noise (DBSCAN) is an *unsupervised* clustering algorithm that groups together points that are closely packed together (points with many nearby neighbors) and discarding data points that lie alone in low-density regions (whose nearest neighbors are too far away). The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.cluster.DBSCAN.html
- **GMeans**: An *unsupervised* clustering algorithm for grouping data points. It extends K-means by trying to *automatically determine the number of clusters* by Gaussian normality test. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.cluster.KMeans.html
- **KMeans**: An *unsupervised* clustering algorithm that groups data points into user specified K groups so that each data point belongs to one group. It tries to iteratively minimize intra-cluster distance and maximize inter-cluster distance. Note that user needs to specify the number of clusters based on user’s knowledge of data. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.cluster.KMeans.html
- **Spectral Clustering**: An *unsupervised* graph-based clustering algorithm for grouping data points. It first constructs a similarity graph, then embeds the data points in a lower dimensional space and then applying classical algorithms like KMeans to partition the data points. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.cluster.SpectralClustering.html

Running Clustering Local Mode

Step 1: Design

First identify the following items:

- **Fields to use for Clustering**: Each field must be a numerical field.
- **Id field**: The identity of a row of data, typically the host name or host IP.
- A **FortiSIEM Report** to get this data.

The Time field is not recommended for a Clustering task since an item may belong to different clusters at different point in time.

Requirements

1. Report must contain
    - an Id field
    - One or more numerical fields to use for clustering
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be additional columns in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the data-set exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**.
2. Select the data source in one of three ways:
    a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
    b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Job** folder
    c. To prepare data from a CSV file, choose **Import Via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.

Step 3: Train

Train the Clustering task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the **Id Field** and **Fields to use for Clustering** are populated correctly.
3. If you chose **Import via Report** or **Import via CSV File**, then
    a. Set **Run Mode** to Local
    b. Set **Task** to Clustering
    c. Choose the **Algorithm**

   d. Check the algorithm parameters, e.g. for KMeans choose the cluster size as a guess.
   e. Choose the **Id Field** and **Fields to use for Clustering** from the report fields.
4. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
5. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

Model Quality:

The following metrics show the quality of the clusters found.

- **Calinski Marabasz Score**: Calinski Marabasz Score (also known as the Variance Ratio Criterion) is calculated as a ratio of the sum of inter-cluster dispersion and the sum of intra-cluster dispersion for all clusters (where the dispersion is the sum of squared distances). *A high Calinski-Harabasz Score means better clustering* since observations in each cluster are closer together (more dense), while clusters themselves are further away from each other (well separated).
- **Davies Bouldin Score**: This is calculated as the average similarity of each cluster with a cluster most similar to it. *Low Davies Bouldin Score means clusters are well separated.*
- **Silhouette Score**: This is calculated using the mean intra-cluster distance and the mean nearest-cluster distance for each sample. *Silhouette Score of 1 means clusters are well apart from each other and clearly distinguished.* Silhouette Score of 0 means that clusters are indifferent, or we can say that the distance between clusters is not significant. Silhouette Score of -1 means clusters are assigned in the wrong way.

The actual and predicted values and the errors are shown in 3 ways:

- **Clustering Result table**: this shows which entity is in which cluster
- **Clustering Membership > Heatmap View**: this shows entity-cluster membership along with the values. Entities in the same cluster should have the same color.

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.

  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when cluster changes during the Inference process.
  - Two choices are available – creating a FortiSIEM Incident or sending an email. Specify the emails if you want emails to be sent. Make sure that email server is specified in **Admin > Settings > Email**.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Clustering Algorithms for Local Auto Mode

In this mode, FortiSIEM picks the best algorithm from the following:

- BIRCH
- DBSCAN
- KMeans

Note: The **Max Run Time** parameter is used to limit the amount of time this job runs. By default it is set to 10 minutes. The longer this job runs, potentially better result can be generated.

Running Clustering Local Auto Mode

To run, follow the Clustering steps in Algorithms for Local Mode, but in Step 3, 3a, select **Run Mode** as **Local Auto**.

Clustering Algorithm for AWS Mode

In this mode, the following algorithm runs in AWS.

- KMeans

Running Clustering AWS Mode

Step 0: Set Up AWS

Set up AWS SageMaker by following the instructions in Set Up AWS SageMaker.

Configure AWS in FortiSIEM by following the instructions in Configure FortiSIEM to use AWS SageMaker.

Step 1: Design

First identify the following items:

- **Fields to use for Clustering**: Each field must be a numerical field.
- **Id field**: The identity of a row of data, typically the host name or host IP.
- A **FortiSIEM Report** to get this data.

The Time field is not recommended for a Clustering task since an item may belong to different clusters at different point in time.

Requirements

1. Report must contain
   - an Id field
   - One or more numerical fields to use for clustering
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be additional columns in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**.
2. Select the data source in one of three ways:
   a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
   b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Job** folder
   c. To prepare data from a CSV file, choose **Import Via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.

Step 3: Train

Train the Clustering task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the **Id Field** and **Fields to use for Clustering** are populated correctly.
3. If you chose **Import via Report** or **Import via CSV File**, then
   a. Set **Run Mode** to AWS
   b. Set **Task** to Clustering
   c. Choose the **Algorithm**
   d. Check the algorithm parameters, e.g. for KMeans choose the cluster size as a guess.
   e. Choose the **Id Field** and **Fields to use for Clustering** from the report fields.
4. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
5. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

Model Quality:

The following metrics show the quality of the clusters found.

- **Calinski Marabasz Score**: Calinski Marabasz Score (also known as the Variance Ratio Criterion) is calculated as a ratio of the sum of inter-cluster dispersion and the sum of intra-cluster dispersion for all clusters (where the dispersion is the sum of squared distances). *A high Calinski-Harabasz Score means better clustering* since observations in each cluster are closer together (more dense), while clusters themselves are further away from each other (well separated).
- **Davies Bouldin Score**: This is calculated as the average similarity of each cluster with a cluster most similar to it. *Low Davies Bouldin Score means clusters are well separated.*
- **Silhouette Score**: This is calculated using the mean intra-cluster distance and the mean nearest-cluster distance for each sample. *Silhouette Score of 1 means clusters are well apart from each other and clearly distinguished.* Silhouette Score of 0 means that clusters are indifferent, or we can say that the distance between clusters is not significant. Silhouette Score of -1 means clusters are assigned in the wrong way.
- **'msd' (Mean Squared Distance)**: This metric is the average of the squared distances between each data point and its assigned cluster center. The mean squared distance is used to assess the overall quality of the clustering, where lower values indicate better clustering performance.
- **'ssd' (Sum of Squared Distances)**: This metric is the sum of the squared distances between each data point and its assigned cluster center. It is also known as the within-cluster sum of squares (WCSS) and is commonly used to evaluate the compactness of the clusters.

The actual and predicted values and the errors are shown in the following ways:

- **Clustering Result table**: this shows which entity is in which cluster
- **Clustering Membership > Heatmap View**: this shows entity-cluster membership along with the values. Entities in the same cluster should have the same color.

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.

  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when cluster changes during the Inference process.
  - Two choices are available – creating a FortiSIEM Incident or sending an email. Specify the emails if you want emails to be sent. Make sure that email server is specified in **Admin > Settings > Email**.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Forecasting

- Forecasting Algorithms for Local Mode
- Running Forecasting Local Mode

The objective of a Forecasting Task is to learn a time based trend of a field in a dataset and then predict future values of that field. Learning the time based trend is done during the Training phase and future prediction is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.

Forecasting Algorithms for Local Mode

In this mode, the following algorithms can run locally within the FortiSIEM Super/Worker cluster.

- **ARIMA (AutoRegressive Integrated Moving Average)**: A statistical analysis model that uses time series data to predict future values. Descriptions of the parameters are here: https://analyticsindiamag.com/quick-way-to-find-p-d-and-q-values-for-arima/ and https://www.sciencedirect.com/topics/mathematics/arima
- **State Space Dynamic MQ**: A forecasting method that can be used to predict future values. Descriptions of the parameters are here: https://www.statsmodels.org/devel/generated/statsmodels.tsa.statespace.dynamic_factor_mq.DynamicFactorMQ.html#statsmodels.tsa.statespace.dynamic_factor_mq.DynamicFactorMQ

Running Forecasting Local Mode

Step 1: Design

First identify the following items:

- **Field to Forecast**: Each field must be a numerical field.
- **Fields to use for Forecasting**: Each field must be a numerical field. Field to forecast could be the same as field to use for forecasting; meaning that previous values of a field is used to forecast future values of the same field.
- **Id Field**: Identifies who the data is for.
  Note: The Id Field is optional.
- **Date Field**: Can be hourly or daily.
- A **FortiSIEM Report** to get this data.

To provide several samples of the data, you can choose one of the following time attributes as a report column

- Event Receive Hour
- Event Receive Date

Requirements

1. Report must contain
   - Date Field - Event Receive Hour or Event Receive Date
   - One numerical field to forecast
   - (Optional) Other fields to use for forecasting
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be additional columns in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**, and click the Import Machine Learning Jobs (open folder) icon.
2. Select the data source in one of three ways:
   a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
   b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Job** folder
   c. To prepare data from a CSV file, choose **Import Via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.

Step 3: Train

Train the Forecasting task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the **Date Field**, **Field(s) to use for Forecasting**, and **Id Field** are populated correctly.
3. If you chose **Import via Report** or **Import via CSV File**, then
   a. Set **Run Mode** to Local
   b. Set **Task** to Forecasting
   c. Choose the **Algorithm**
   d. Choose **Id Field**
   e. If the **Algorithm** is ARIMA:
      i. Choose the **Field to Forecast** from the report fields. Current ARIMA implementation uses previous values of a field to forecast the future values of the same field.

        ii. Choose the **Steps** parameter to specify how many time steps to be forecasted. The default value is 5 and can be found by clicking the Settings icon next to the Algorithm.

    f. If the Algorithm is **State Space Dynamic Factor MQ**:

        i. Choose the **Field to Forecast** and **Fields to use for Forecasting** from the report fields.

        ii. Choose the **Steps** parameter to specify how many time steps to be forecasted. The default value is 5 and can be found by clicking the Settings icon next to the Algorithm.

4. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
5. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

Model Quality:

This shows how accurately the algorithm is able to predict the field. The following metrics are calculated:

- **Max Error**: Mmaximum of the error between predicted value and actual value over all data points. *Lower value means that regression is a better fit.*
- **Mean Absolute Error**: Average of Absolute difference between predicted and actual values over all data points. *Lower value means that regression is a better fit.*
- **Mean Squared Error**: Average of Square of difference between predicted and actual values over all data points. *Lower value means that regression is a better fit.*
- **R2 score**: a statistical measure of how well the regression predictions approximate the real data points. *An R2 of 1 indicates that the regression predictions perfectly fit the data.* R-square value of 0.8 means that 80% of the variation in the predicted attribute is explained by the feature attributes.
- **Root Mean Squared Error (RMSE)**: Square root of the average of Square of difference between predicted and actual values over all data points. *Lower value means that regression is a better fit.* RMSE is affected by the scale of the data. RMSE can be heavily affected by a few predictions which are much worse than the rest.

Forecasting Result is shown in two ways

- **Tabular form**: The predicted values are shown in the first few rows.
- **Trend form**: Shows how the algorithm learns the values over time and is able to forecast future values

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
    - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
    - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.

   - **Job Description**: Description of the job.
   - **Inference schedule**: The frequency at which Inference job will be run
   - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.
   - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
   - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when an anomaly is found during the Inference process.
   - One choice is available – Send email(s) by entering the email address(es) in the **Send email to** field. Make sure that the email server is specified in **Admin > Settings > Email**.
   - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Regression

The objective for Regression Task is to build a model for predicting a Target field based on other fields in a dataset, and then create an alert if the new values of the Target field exceeds the predicted value, by user specified threshold. Building the prediction model is done during the Training phase and alert creation is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.

- Regression Algorithms for Local Mode
- Running Regression Local Mode
- Regression Algorithms for Local Auto Mode
- Running Regression Local Auto Mode
- Regression Algorithms for AWS Mode
- Running Regression AWS Mode
- Regression Algorithms for AWS Auto Mode
- Running Regression AWS Auto Mode

Regression Algorithms for Local Mode

The following Machine Learning Algorithms are available:

In this mode, the following algorithms can run *locally* within the FortiSIEM Supervisor/Worker cluster.

- **Decision Tree Regressor**: A supervised regression algorithm that uses a Decision Tree to predict a Target variable based on Feature variables. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.tree.DecisionTreeRegressor.html
- **Linear Regression**: A supervised regression algorithm that predicts a Target variable based on a linear combination of Feature variables. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.linear_model.LinearRegression.html
- **Random Forest Regressor**: A supervised regression algorithm that uses Ensemble learning and Bootstrapping techniques to improve the accuracy of Decision Tree based prediction algorithms. Ensemble learning uses multiple models and Bootstrapping randomly samples datasets and then averages the results of each model to

improve accuracy. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestRegressor.html

- **SGDRegressor**: A supervised regression algorithm that uses Stochastic Gradient Descent (SGD) method to minimize a user specified loss function for the Linear Regression algorithm. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.linear_model.SGDRegressor.html
- **SVR**: A supervised regression algorithm that finds a linear function representing the data within a margin of error Support Vector Regression (SVR) error function for prediction. SVR is more robust to outliers than most other regression methods, since it does not care much about the data outside the margin. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.svm.SVR.html

Running Regression Local Mode

Step 1: Design

First identify the following items:

- **Field to Predict**: Must be a numerical field.
- **Fields to use for Prediction**: Each field must be a numerical field.
- A **FortiSIEM Report** to get this data.

There must be several samples of the data. This can be accomplished by choosing one of the following time attributes as a report column

- Event Receive Time
- Event Receive Hour
- Event Receive Date

Requirements

1. Report must contain
   - A time attribute
   - One numerical **Field to Predict**
   - One or more numerical **Fields to use for Prediction**
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be additional columns in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**.
2. Select the data source in one of three ways:
   a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
   b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Job** folder
   c. To prepare data from a CSV file, choose **Import Via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.

Step 3: Train

Train the Regression task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the **Fields to use for Prediction** and **Fields to Predict** are populated correctly.
3. If you chose **Import via Report** or **Import Via CSV File**, then
   a. Set **Run Mode** to Local
   b. Set **Task** to Regression
   c. Choose the **Algorithm**
   d. Choose the **Fields to use for Prediction** and **Fields to Predict** from the report fields.
4. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
5. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

Model Quality:

This shows how accurately the algorithm is able to predict the field. The following metrics are calculated:

- **Max Error**: Maximum of the error between predicted value and actual value over all data points. *Lower value means that regression is a better fit.*
- **R2 score**: A statistical measure of how well the regression predictions approximate the real data points. *An R2 of 1 indicates that the regression predictions perfectly fit the data.* R-square value of 0.8 means that 80% of the variation in the predicted attribute is explained by the feature attributes.
- **Mean Absolute Error**: Average of Absolute difference between predicted and actual values over all data points. *Lower value means that regression is a better fit.*
- **Mean Squared Error**: Average of Square of difference between predicted and actual values over all data points. *Lower value means that regression is a better fit.*
- **Root Mean Squared Error (RMSE)**: Square root of the verage of Square of difference between predicted and actual values over all data points. *Lower value means that regression is a better fit.* RMSE is affected by the scale of the data. RMSE can be heavily affected by a few predictions which are much worse than the rest.

The actual and predicted values and the errors are shown in 3 ways:

- **Regression Result table**: If the model did well, then the error column should have small values.
- **Scatter plot**: If the model did well, then this chart must be centered along the y=x line.
- **Error histogram**: If the model did well, then the chart should be clustered around the x=0 line.

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.
  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when an anomaly is found during the Inference process.
  - Only one choice is available – Creating an incident when Error is #. Enter a number in the **Create an Incident when Error is great than** field.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Regression Algorithms for Local Auto Mode

In this mode, FortiSIEM automatically chooses the best algorithm with the optimal parameters. The following algorithms are considered:

- **Decision Tree Regressor**
- **Random Forest Regressor**
- **SGDRegressor**
- **SVR**

Note: The **Max Run Time** parameter is used to limit the amount of time this job runs. By default it is set to 5 minutes. The longer this job runs, potentially better results can be generated.

Running Regression Local Auto Mode

To run, follow the Regression steps in Algorithms for Local Mode, but in Step 3, 3a, select **Run Mode** as **Local Auto**.

Regression Algorithms for AWS Mode

The following algorithm runs in AWS mode.

- **Linear- Learner Algorithem-for-Regression**: Linear models are supervised learning algorithms used for solving either classification or regression problems. See https://docs.aws.amazon.com/sagemaker/latest/dg/linear-learner.html for more information.

Running Regression AWS Mode

Step 0: Set Up AWS

Set up AWS SageMaker by following the instructions in Set Up AWS SageMaker.

Configure AWS in FortiSIEM by following the instructions in Configure FortiSIEM to use AWS SageMaker.

Step 1: Design

First identify the following items:

- **Field to Predict**: Must be a numerical field.
- **Fields to use for Prediction**: Each field must be a numerical field.
- A **FortiSIEM Report** to get this data.

There must be several samples of the data. This can be accomplished by choosing one of the following time attributes as a report column

- Event Receive Time
- Event Receive Hour
- Event Receive Date

Requirements

1. Report must contain
   - A time attribute
   - One numerical **Field to Predict**
   - One or more numerical **Fields to use for Prediction**
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be additional columns in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the data-set exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**.
2. Select the data source in one of three ways:
    a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
    b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Job** folder
    c. To prepare data from a CSV file, choose **Import Via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.

Step 3: Train

Train the Regression task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the **Fields to use for Prediction** and **Fields to Predict** are populated correctly.
3. If you chose **Import via Report** or **Import Via CSV File**, then
    a. Set **Run Mode** to AWS
    b. Set **Task** to Regression
    c. Choose the **Algorithm**
    d. Choose the **Fields to use for Prediction** and **Fields to Predict** from the report fields.
4. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
5. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

Model Quality:

This shows how accurately the algorithm is able to predict the field. The following metrics are calculated:

- **Mean Absolute Error (MAE)**: Average of Absolute difference between predicted and actual values over all data points. *Lower value means that regression is a better fit.*
- **Mean Squared Error (MSE)**: The mean square error of the final model on the validation dataset. This objective metric is only valid for regression.
- **R2 score**: A statistical measure of how well the regression predictions approximate the real data points. *An R2 of 1 indicates that the regression predictions perfectly fit the data.* R-square value of 0.8 means that 80% of the variation in the predicted attribute is explained by the feature attributes.
- **Root Mean Squared Error (RMSE)**: The root mean square error of the final model on the validation dataset. This objective metric is only valid for regression.

The actual and predicted values and the errors are shown in 3 ways:

- **Regression Result table**: If the model did well, then the error column should have small values.
- **Scatter plot**: If the model did well, then this chart must be centered along the y=x line.
- **Error histogram**: If the model did well, then the chart should be clustered around the x=0 line.

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.
  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when an anomaly is found during the Inference process.
  - Only one choice is available – Creating an incident when Error is #. Enter a number in the **Create an Incident when Error is great than** field.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Regression Algorithms for AWS Auto Mode

In this mode, FortiSIEM automatically chooses the best algorithm with the optimal parameters. Depending on the size of your dataset (whether is it greater or smaller than 100MB), algorithms from HPO mode or from ensembling mode will be considered. For more information, see https://docs.aws.amazon.com/sagemaker/latest/dg/autopilot-model-support-validation.html. Definitions below taken from Amazon SageMaker Developer Guide.

HPO mode (Dataset > 100MB)

- **Linear learner**: A supervised learning algorithm that can solve either classification or regression problems.
- **XGBoost**: A supervised learning algorithm that attempts to accurately predict a target variable by combining an ensemble of estimates from a set of simpler and weaker models.

- **Deep learning algorithm**: A multilayer perceptron (MLP) and feedforward artificial neural network. This algorithm can handle data that is not linearly separable.

Ensembling mode (Dataset <=100MB)

- **LightGBM**: An optimized framework that uses tree-based algorithms with gradient boosting. This algorithm uses trees that grow in breadth, rather than depth, and is highly optimized for speed.
- **CatBoost**: A framework that uses tree-based algorithms with gradient boosting. Optimized for handling categorical variables.
- **XGBoost**: A framework that uses tree-based algorithms with gradient boosting that grows in depth, rather than breadth.
- **Random Forest**: A tree-based algorithm that uses several decision trees on random sub-samples of the data with replacement. The trees are split into optimal nodes at each level. The decisions of each tree are averaged together to prevent overfitting and improve predictions.
- **Extra Trees**: A tree-based algorithm that uses several decision trees on the entire dataset. The trees are split randomly at each level. The decisions of each tree are averaged to prevent overfitting and to improve predictions. Extra trees add a degree of randomization in comparison to the random forest algorithm.
- **Linear Models**: A framework that uses a linear equation to model the relationship between two variables in observed data.
- **Neural network torch**: A neural network model that is implemented using Pytorch.
- **Neural network fast.ai**: A neural network model that is implemented using fast.ai.

Note: The **Max Run Time** parameter is used to limit the amount of time this job runs. By default it is set to 225 minutes. The longer this job runs, potentially better results can be generated.

Running Regression AWS Auto Mode

To run, follow the Regression steps in Algorithms for AWS Mode, but in Step 3, 3a, select **Run Mode** as **AWS Auto**.

For Step 3, the following model quality information pertains.

Model Quality:

This shows how accurately the algorithm is able to predict the field. The following metrics are calculated:

- **MAE**: The mean absolute error (MAE) is a measure of how different the predicted and actual values are, when they're averaged over all values. MAE is commonly used in regression analysis to understand model prediction error. If there is linear regression, MAE represents the average distance from a predicted line to the actual value. MAE is defined as the sum of absolute errors divided by the number of observations. Values range from 0 to infinity, with smaller numbers indicating a better model fit to the data.
- **RMSE**: Root mean squared error (RMSE) measures the square root of the squared difference between predicted and actual values, and is averaged over all values. It is used in regression analysis to understand model prediction error. It's an important metric to indicate the presence of large model errors and outliers. Values range from zero (0) to infinity, with smaller numbers indicating a better model fit to the data. RMSE is dependent on scale, and should not be used to compare datasets of different sizes.
  MSE: The mean squared error (MSE) is the average of the squared differences between the predicted and actual values. It is used for regression. MSE values are always positive. The better a model is at predicting the actual values, the smaller the MSE value is.
- **R2**: R2, also known as the coefficient of determination, is used in regression to quantify how much a model can explain the variance of a dependent variable. Values range from one (1) to negative one (-1). Higher numbers indicate a higher fraction of explained variability. R2 values close to zero (0) indicate that very little of the dependent

variable can be explained by the model. Negative values indicate a poor fit and that the model is outperformed by a constant function. For linear regression, this is a horizontal line.

Investigating Incidents

You can examine an incident in-depth through the following methods.

1. From the **Incidents** page, select an incident and choose **Investigate** from the **Action** drop-down list.
   or
2. On the **Analytics > Investigation** page, enter the Incident ID number of the incident you wish to examine, or select it from the top 10 incidents that appear initially on a new tab, and click **Load**.

When an incident number has been provided, the Analytics Investigation page will show an undirected graph of the incident and involved entities (host/ip, user, process, file) as nodes. The latest top 10 incidents appear initially on a new tab on the **Analytics > Investigation** page.

A **Time From** and **To** field are available to set the time span you wish to investigate for the selected incident.

A left vertical bar offers the following functions.

Icon	Description
Investigation History	Click to view investigation actions that have taken place for the incident.
Timeline	Click to view information on when the incident occurred. Incidents are ordered by when they occurred in the timeline. Hover your mouse cursor over an incident in the Timeline panel to see the incident and its affected entities in the undirected graph. A Play icon can be clicked to illustrate when the incident occurred for the selected time span. The information icon can be clicked to get more detailed information. Check the **Auto** checkbox to play the next node automatically without having to click it. The Recenter icon moves the current incident in the timeline sequence to the center
Root Incident Comments	Click to view any comments made related to the incident.

Examining an Incident and Related Entities

After an incident has been loaded into Analytics, you can take the following actions. A node will either be an incident or an entity (host/ip, user, process, file). An incident can be recognized by a colored border that also indicates the severity of the incident.

- Hover over a node to bring up a quick overview on the incident/entity object.
- Click on a incident node to access a left pane that provides detailed information on the incident and various actions that you can take.

Button	Description
Details	Click to view detailed information on the incident.
Events	Click to view the triggering events that led to the incident. Click > to go to the next triggering event, if applicable.
Context	Click to get information about all the IPs and hosts in the incident. Device type, presence in Malware lists and watch lists is also provided.
Comments	Click to view and add/edit comments related to the incident.
...	Click to view additional actions available to take on the incident. See Acting on Incidents for more information. In addition to the actions that can be taken listed in Acting on Incidents, the user also has access to **Action History**. Clicking on **Action History** displays all the actions that the user has taken on the incident in the current session, including the date/time each action was taken. The user can expand and get more details on a particular action by clicking on the caret icon.

- Click on a node that is an entity to access a left pane that shows entity information. See Pane Information on the Risk Page for more information.

Button	Description
Details	Click to view detailed information on the entity.
External Lookup	If the entity is a device, click to run an external lookup (VirusTotal, RiskIQ, and/or FortiGuard) for the entity. First, select the IP address from the **External Lookup Target** drop-down list, select the external lookup from the **Check from Website** drop-down list, then click **Lookup**.
Run Report	If the entity is a host or IP node, Run Report is available. From the **Report** drop-down list, select a report. Next, use the **Quick Filters** or **Custom Filters** if needed, then click **Run**. From the **Result Summary**, click **Show** to get a more detailed table.
Context	Click to get IP and host information.

- Additionally, when a node is selected from the undirected graph, related objects can be added to the undirected graph. See the following table for further information on the actions you can take.
  Note: Actions that are available are determined by the object you selected.

Action	Description
Related Entities	Click to view additional identified related entities for the incident

Action	Description
	you selected.
Related Incidents	Click to view additional identified related incidents for the entity you selected.
Related Incidents and Entities	Click to view additional identified related incidents and entities for the entity you selected.
Remove Node	Click to remove the selected node.

Working with the Undirected Graph

- Adding an Undirected Graph
- Clearing an Undirected Graph
- Fitting the Undirected Graph in Panel
- Repositioning a Node
- Repositioning the Undirected Graph
- Zooming In/Out of the Undirected Graph

Adding an Undirected Graph

Click on **+**, enter the Incident ID that you wish to view an undirected graph of, and click **Load**.

Clearing an Undirected Graph

To clear an undirected graph, click the trash icon in the lower right corner.

Fitting the Undirected Graph in Panel

To fit the undirected graph in the existing panel, click the "fit in frame" icon.

Repositioning a Node

To reposition a node, click and hold the left mouse button over a node. Next, move the mouse to reposition the node, and release the mouse button when done.

Repositioning the Undirected Graph

To reposition the undirected graph, click and hold the left mouse button over a location that isn't a node. Next, move the mouse to reposition the undirected graph, and release the mouse button when done.

To recenter the undirected graph, click the Center icon, located in the lower right corner.

Zooming In/Out of the Undirected Graph

To zoom in or out of a graph, click the **+** or **-** icons.

Working with Dashboards

FortiSIEM collects logs and performance metrics and create Incidents by event correlation and other means. This data can be summarized in Reports. A Dashboard provides a graphical view of these reports. FortiSIEM Dashboards are organized into a two-level hierarchy: Dashboard folders with each folder containing multiple Dashboards.

You can perform various operations from FortiSIEM Dashboards:

- General Operations

A Dashboard can be one of the following six built-in dashboard types:

- Widget Dashboard
- Summary Dashboard
- Business Service Dashboard
- Identity and Location Dashboard
- Interface Usage Dashboard
- PCI Logging Status Dashboard

General Operations

FortiSIEM Dashboard can be used to perform various operations:

- Viewing Built-in Dashboard Folders
- Displaying Only Dashboard Folders of Interest
- Setting a Home Dashboard Folder
- Creating a New Dashboard Folder
- Creating a New Dashboard Under a Folder
- Sharing Dashboard Folders
- Deleting a Dashboard
- Deleting a Dashboard Folder
- Starting Dashboard Slideshow

Viewing Built-in Dashboard Folders

FortiSIEM provides several built-in dashboard folders:

Folder	Dashboard	Type	Description
Amazon Web Services Dashboard	Summary	Summary Dashboard	
	Performance	Widget Dashboard	

Folder	Dashboard	Type	Description
	Login	Widget Dashboard	
	Cloud Trail	Widget Dashboard	
	Elastic Load Balancer	Widget Dashboard	
Application Server Dashboard	JBoss	Widget Dashboard	
	WebSphere	Widget Dashboard	
	WebLogic	Widget Dashboard	
	Tomcat	Widget Dashboard	
	GlassFish	Widget Dashboard	
Database Dashboard	Logon	Widget Dashboard	
	System Perf	Widget Dashboard	
	Oracle Performance	Widget Dashboard	
	SQL Server Performance	Widget Dashboard	
	MySQL Performance	Widget Dashboard	
FortiSIEM Dashboard	Event	Widget Dashboard	
	Audit	Widget Dashboard	
	Incidents	Widget Dashboard	
	Incidents/Cases	Widget Dashboard	
Fortinet Security Fabric	FortiGate Threat	Widget Dashboard	
	FortiGate Traffic	Widget Dashboard	
	FortiMail	Widget Dashboard	

Folder	Dashboard	Type	Description
	FortiSandbox	Widget Dashboard	
	FortiDeceptor	Widget Dashboard	
	FortiEDR	Widget Dashboard	
	FortiClient	Widget Dashboard	
	FortiADC	Widget Dashboard	
	FortiNDR (FortiAI)	Widget Dashboard	
	FortiProxy	Widget Dashboard	
Global FortiSIEM Dashboard	Event	Widget Dashboard	After upgrading, super users in global mode can access the Global FortiSIEM Dashboard. **Note**: This is the same as the FortiSIEM Dashboard.
	Audit	Widget Dashboard	
	Incidents	Widget Dashboard	
GCP Dashboard	Google Cloud Audit	Widget Dashboard	
Google Apps Dashboard	Summary	Widget Dashboard	
	Audit	Widget Dashboard	
Identity and Location Dashboard	Identity and Location	Summary Dashboard	
NetApp Dashboard	Overall	Widget Dashboard	
	NFS Perf	Widget Dashboard	
	CISF Perf	Widget Dashboard	
	ISCSI Perf	Widget Dashboard	

Folder	Dashboard	Type	Description
Network Dashboard	Summary	Summary Dashboard	
	Hardware	Summary Dashboard	
	Availability	Widget Dashboard	
	Performance	Widget Dashboard	
	Login/Change	Widget Dashboard	
	Netflow	Widget Dashboard	
	IPSLA	Widget Dashboard	
	VoIP	Widget Dashboard	
	CBQoS	Widget Dashboard	
Nutanix Dashboard	Nutanix Audit	Widget Dashboard	
Office365 Dashboard	Logon	Widget Dashboard	
	Audit	Widget Dashboard	
Oracle Cloud Dashboard	Oracle Cloud Audit	Widget Dashboard	
Salesforce Dashboard	Login	Widget Dashboard	
	Activity	Widget Dashboard	
	Performance	Widget Dashboard	
Security Dashboard	Perimeter	Widget Dashboard	
	Access	Widget Dashboard	
	Malware	Widget Dashboard	
	Vulnerability	Widget Dashboard	
	Exploits	Widget Dashboard	

Folder	Dashboard	Type	Description
	Policy Violation	Widget Dashboard	
	UEBA AI Alerts	Widget Dashboard	
	UEBA Events	Widget Dashboard	
	OT/IoT	Widget Dashboard	
Server Dashboard	Summary	Summary Dashboard	
	Hardware	Summary Dashboard	
	Availability	Widget Dashboard	
	Performance	Widget Dashboard	
	Login	Widget Dashboard	
VMWare Dashboard	VM	Widget Dashboard	
	ESX	Widget Dashboard	
	Cluster	Widget Dashboard	
	Resource Pool	Widget Dashboard	
	Datastore	Widget Dashboard	
	Environment	Widget Dashboard	
	Events	Widget Dashboard	
VNX Dashboard	Processor	Widget Dashboard	
	Ports	Widget Dashboard	
	LUNs	Widget Dashboard	
	Storage Pool	Widget Dashboard	
Web Server Dashboard	System Performance	Widget Dashboard	

Folder	Dashboard	Type	Description
	IIS Performance	Widget Dashboard	
	Apache Performance	Widget Dashboard	
	Access	Widget Dashboard	

Displaying Only Dashboard Folders of Interest

Complete these steps to see only the dashboards folders that are of interest to you:

1. Click the **User Profile** icon () in the upper right corner of the UI.
2. Click the **UI Settings** tab.
3. Click the Edit icon for **Dashboard Settings**.
4. Select the currently **Visible Dashboards** that you want to hide and click **<**.
5. Click **Save**.

The dashboard folder drop-down list under the **DASHBOARD** tab will display only the selected dashboard folders.

Setting a Home Dashboard Folder

Complete these steps to see a specific dashboard folder when you navigate to the **DASHBOARD** tab:

1. Click the **User Profile** icon () in the upper right corner of the UI.
2. Click the **UI Settings** tab.
3. Select a **Dashboard Home** from the drop-down list.
4. Click **Save**. Refresh the Web page if it doesn’t reload automatically.

Creating a New Dashboard Folder

Complete these steps to create a new dashboard folder:

1. Go to **DASHBOARD** and select **New** from the Dashboard drop-down list.
2. Enter a dashboard **Name**.
3. Select whether you want to share the dashboard.
4. Click **Save**.

Creating a New Dashboard Under a Folder

Note: You can add a dashboard to a built-in dashboard folder.

To create a new dashboard under a dashboard folder:

1. Go to **DASHBOARD** tab.
2. Select the dashboard from the folder drop-down list. The dashboards belonging to the folder will display on the top menu.
3. Click **+** to the right.
4. Enter a dashboard **Name**, select a dashboard **Type**, and add any related **Description** about this dashboard.
5. Click **Save**.

Sharing Dashboard Folders

When you create a new dashboard folder, FortiSIEM gives you the option of sharing the folder, and all of the dashboards in it, with other users.

Note the following rules and restrictions on shared dashboards:

Rules for creating and using shared dashboard folders:

- A user can share only with other users in the same organization.
  - A Super user can share only with other Super users, even if that Super user is in Global mode.
  - Org users can share only with (the same) Org users.
- If a Global/Super user shares a dashboard with another user, the other user can see only this dashboard in Global/Super mode.
- If a Local/Super user shares a dashboard with another user, the other user can see only this dashboard in Local/Super mode.
- If you share with all users in the current Org, then above rules also apply.

Restrictions on shared dashboards:

- Only the user who created the dashboard has Write permission to it, including setting the list of shareable users. The users with whom the dashboards are shared have only Read permission.
- Shared users can view the reports and perform Search and drill down operations on them. If shared users try to change the dashboard in any way, they will be asked to clone the dashboard with a new name. Cloning the dashboard breaks the link with the original dashboard. If the user wants access to the original dashboard, then the user who created the dashboard must share it again.
- For shared dashboards, run the report once, so that all users see the same data.
- A shared dashboard cannot be hidden from view.

Advantages of a shared dashboard folder:

- The dashboard owner can seamlessly propagate changes to the users with whom the dashboard is shared.
- An organization can quickly standardize on a set of dashboards created by experts.
- The report to populate the dashboard is run once if the report is run in inline mode. This uses less system resources

Creating a Shared Dashboard

Complete these steps to create a shared dashboard folder:

1. Go to **DASHBOARD** and click **New** to create a dashboard folder.
2. In the **Create Dashboard Folder** dialog box, enter a **Name** for the dashboard folder.

3. Select the **Everyone in current org** checkbox to share the dashboard folder with everyone in the current organization.
   a. To share with selected users/groups, click the edit icon. Select **Users** (CMDB Users) and/or **AD Groups** from the left column, then select individual users from the middle column and shuttle them to the **Selections** column.
   b. Click **Continue**. The selected users and groups will be able to access the shared dashboard and its contents.
4. Click the edit icon next to **Exclude** to exclude sharing with selected users.
   a. Select **Users** (CMDB Users) and/or **AD Groups** from the left column, then select individual users from the middle column and shuttle them to the **Selections** column.
   b. Click **Continue**. The excluded users will not be able to see or access the shared dashboard folder.
5. Click **Save**. The dashboard folder will have a icon – this indicates that it is a shared folder. At this point, you can create dashboards for the shared dashboard folder. See Creating a new dashboard under a folder.

Cloning a Shared Dashboard Folder

In shared dashboard, you can perform the refresh, drill down, and search operations. If you want to make any other changes, such as add a dashboard, change display settings, or delete the dashboard, then you must clone the shared dashboard folder. Once cloned, the link between the original shared dashboard and the cloned dashboard will be broken. This means that changes to the original shared dashboard will not be reflected in the cloned dashboard.

Complete these steps to clone a dashboard folder.

1. Log in to FortiSIEM.
2. Go to **Dashboard** and select the dashboard folder that has been shared with you from the drop-down list.
3. Any changes you attempt to make, such as add a dashboard, change display settings, or delete the dashboard, will open the **Clone Dashboard Folder** dialog box.
4. Enter a new **Folder Name** in the **Clone Dashboard Folder** dialog box.
5. Click **Save**.

You can now make your own changes to the dashboards in the cloned dashboard folder.

Deleting a Dashboard

Note: Built-in dashboards cannot be deleted.

Complete these steps to delete a user-created dashboard:

1. Go to **DASHBOARD** tab.
2. Select the dashboard folder drop-down list. The dashboards belonging to that folder will display.
3. Select the dashboard to delete from the top menu and click the **x**.

Deleting a Dashboard Folder

Note: Built-in dashboard folders cannot be deleted.

Complete these steps to delete a user-created dashboard folder:

1. Go to **DASHBOARD** tab.
2. Select the dashboard folder from the folder drop-down list and click the **x**.

Starting Dashboard Slideshow

Make sure that you have created the slideshow templates before starting a slideshow. See Dashboard Slideshow Settings.

Complete these steps to start a dashboard slideshow:

1. Go to **DASHBOARD** tab.
2. Click the dashboard folder drop-down list and click **Start Slideshow** to select the configured slideshow. The slideshow starts in full screen mode. To exit full screen mode, click the **Exit Full Screen (Esc)** button.
3. To return to the dashboard page, click ➡ button on the top-right.

Widget Dashboard

A Widget Dashboard displays a graphical view of FortiSIEM reports. The reports can be from CMDB data or Event data. The reports can be Top N type aggregated reports or non-aggregated reports, likely displaying raw messages. Aggregated reports can be displayed in various forms: gadgets, bar, donuts, tables, line, stacked line, scatter plot, heat maps, tree maps, and geo-maps.

- Creating a Widget Dashboard
- Data Source
- Populating a Widget Dashboard
- Modifying Widget Dashboard Layout
- Modifying Widget Information Display
- Searching in a Widget Dashboard
- Drill-down into a Widget
- Exporting Widget Dashboard Definition
- Importing Widget Dashboard
- Forcing a Refresh

Creating a Widget Dashboard

When you create a new dashboard, choose Widget Dashboard as the **Type**.

Data Source

All Event data and CMDB Data can be used to populate a Widget Dashboard.

Populating a Widget Dashboard

You can add up to a maximum of 20 event reports or CMDB reports to a Widget Dashboard. Complete these steps to add a report to a Widget Dashboard:

1. Make sure the report of your choice exists. CMDB Reports can be found in **CMDB** > **CMDB Reports**. Event Reports can be found in **RESOURCES** > **Reports**.

- If the report exists, then run the report to make sure that data is accurate and the fields you want to see are present. Do not choose too many columns in a dashboard view, as may clutter the dashboard.
- If the report does not exist, then create the report and **Save** it. You can save it in a folder for easy navigation.

2. Go to **DASHBOARD** tab. Select the dashboard folder from the drop-down list.
3. Click **+** below the dashboard folder drop-down list. Select the report from the menu and click **>** to display it on the dashboard.
   The report will run and the results will be displayed in the Widget Dashboard.

Modifying Widget Dashboard Layout

You can select one of two Widget Dashboard layouts from the **Layout** drop-down list on top-right menu of dashboard:

- **Tile view** - widgets can be of non-uniform size and can be dragged around the dashboard space.
- **Column view** - widgets are arranged in a fixed number of columns (1 or 3) in the dashboard space.

Modifying Widget Information Display

1. Click the tools icon on the top-right of the widget to open the **Settings** page.
   a. To change the title, enter a new **Title**.
   b. To change the chart format, choose a new **Display** from the available choices, only if it is relevant for the report. FortiSIEM Charts and Views describes the available charts.
   c. To change the time duration of the report, choose a different **Time**.
   d. To modify the size of the widget, choose a different **Width** and **Height**. Widgets displayed in tabular formats typically take more width and height compared to Single Line view.
   e. To display more or fewer entries, choose the appropriate **Result Limit**. Note that a larger result limit may require more width and height.
   f. For a Service Provider installed in a Super/Global view, choose the **Organizations** to run the report for. This option is available if you run reports from the Super/Global view.
   g. To change the chart refresh interval, select the appropriate **Refresh Interval**. Reports will be re-run periodically at specified refresh intervals.
   h. To change the **Trend Interval**, select one of the following from the drop-down list:
   Auto - (Default) Query is handled normally.
   Hourly - Select this configuration for proper chart display if you want to check the data hourly.
   Daily - Select this configuration for proper chart display if you want to check the data daily.
   Weekly - Select this configuration for proper chart display if you want to check the data weekly.
   i. Select **Display Settings** for the specific **Display** chosen before. FortiSIEM Charts and Views describes the required settings for each of the charts.
   j. If the report contains nested query report, select a time range from “Nested Time” drop-down list for the inner query.
2. Click **Save**.

Searching in a Widget Dashboard

You can search data for specific event attributes simultaneously in all the widgets in a dashboard. To do this, click the Filter button on left and select the values. You can search on any field that appears in at least one widget on a dashboard.

For example, if you choose to Filter on IP = 10.1.1.1, then only the entries for Source IP or Destination IP or Host IP = 10.1.1.1 are shown on all the widgets.

Note the following:

- The values you can search are pre-populated by searching through the data in various widgets. You can only search for a value if it is present in any widget on the dashboard.
- Without filters, a dashboard shows pre-computed results – so they load quickly. However, when you search, all the reports in the Widget Dashboard are run in an ad hoc mode. Subsequently, search results may return relatively slowly.

Drill-down into a Widget

To analyze the results shown in a widget further, click the magnifying glass icon on the top-right of the widget. This will take you to the **ANALYTICS** tab. The same query will be re-run slightly differently:

- Time conditions are maintained
- Filter conditions are maintained
- Aggregation conditions are removed and the field values and the raw messages are shown directly

This enables users to better understand the widget results. For example, if a column like AVG(CPU) is high over a time duration, then drill down shows all the individual CPU values over the time duration so that you can quickly go to the time when CPU spiked.

Exporting Widget Dashboard Definition

If you want to create the same dashboard in another FortiSIEM, or share with another user, or create the same dashboard for another Organization in a Service Provider FortiSIEM instance, use the export/import feature.

To export the dashboard definition, click the export button on top-right. The definition will be saved in a file, which then can be imported into another FortiSIEM Widget Dashboard.

Importing a Widget Dashboard

To import a dashboard widget, click the import button on top-right and select the file. The imported file must be exported from another FortiSIEM Widget Dashboard.

Forcing a Refresh

To update the whole dashboard, click the refresh icon on the top-right menu.

Summary Dashboard

A Summary Dashboard displays the metrics for many devices in a spreadsheet format. Unlike the widget dashboard that shows a few metrics in one widget, a Summary Dashboard can simultaneously show many more metrics. This often allows rapid diagnostics. FortiSIEM calculates and maintains these metrics in an in-memory database inside Query Master module.

Note: RBAC for Summary dashboard is controlled by hiding by Device Group and not by Data Condition. If you want to hide a group of devices in Summary dashboard for a role, hide the Device Group in the role. The user should not be able to choose the devices from the Device Group.

- Creating a Summary Dashboard
- Data Source
- Managing Devices in a Summary Dashboard
- Changing Display Columns
- Changing Refresh Interval
- Forcing a Refresh
- Searching a Summary Dashboard

Creating a Summary Dashboard

When you create a new dashboard, choose Summary Dashboard as **Type**.

Data Source

The source of data in a Summary Dashboard is the performance and availability monitoring metrics and incidents. To see the metrics that can be displayed, click the column icon. The left table shows the event types and the middle table shows the available metrics for the selected event type. These metrics can be displayed in a Summary Dashboard. Custom attributes from custom monitoring may also be displayed after they are defined.

In addition to metrics, the following are shown:

- Performance, Availability and Security incident counts
- Performance, Availability and Security Status each derived from respective incident severities

Managing Devices in a Summary Dashboard

When you create a Summary Dashboard for the first time, no devices are displayed.

Complete these steps to add devices to the dashboard:

1. Click the device icon.
2. Choose devices to display from the **Available Devices** list and click the right arrow button.
3. Click **OK**.

If the devices do not display in the dashboard, check the pre-defined filters for **Severity**. You may want to set Severity to **All Severities** to see the device recently added. When there are a large number of devices being monitored, you may want to show only the devices with **Critical + Warning** severity, as they would need attention.

Complete these steps to remove a device from the dashboard:

1. Click the device icon.
2. Choose devices to display from the **Selected Devices** list and click the left arrow button.
3. Click **OK**.

Changing Display Columns

Complete these steps to change the pre-defined set of display columns in the Summary Dashboard:

1. Click the columns icon.
2. To remove a column, choose the column from the **Selected Columns** list and click the left arrow button.
3. To add a new column:
    a. Select an **Event Types** on the left-most tab
    b. Choose the **Columns** from the middle tab corresponding to the selected **Event Types**.
    c. Click right arrow.
4. Click **OK**.

Changing Refresh Interval

Select the refresh interval from the drop-down menu on the top-right menu.

Forcing a Refresh

To update the whole dashboard click the refresh icon on top-right menu.

Searching a Summary Dashboard

You can search for specific devices by entering values in the search field.

1. Select the fields to search by clicking the search icon.
2. Enter the search string in the search field.

You can also filter from the three pre-defined drop-down lists:

- Severity
- Organizations
- Locations

You can set the location property for devices from **ADMIN** > **Settings** > **Discovery** > **Location**.

Business Service Dashboard

In FortiSIEM, you can define a Business Service as a container of Devices (Go to **CMDB** > **Business Services**, then click **New**). A Business Service Dashboard provides an overview of the health of the business service by showing the related Incidents and impacted devices.

- Creating a Business Service Dashboard
- Data Source
- Adding/Removing Business Service to the Dashboard
- Summary View
- Drilldown View
- Filtering Summary View
- Filtering Drilldown View
- Changing Refresh Interval
- Forcing a Refresh

Creating a Business Service Dashboard

When you create a new dashboard, choose Business Service Dashboard as **Type**.

Data Source

The only source of data for this dashboard is incidents triggering for the devices belonging to a Business Service.

Adding/Removing Business Services to the Dashboard

When you create a Business Service Dashboard for the first time, no Business Services are shown.

Complete these steps to add a Business Service to the dashboard:

1. Click the devices icon.
2. Select the Business Services from the **Available Services** Business Service list.
3. Click right arrow to move them to the **Selected Services** list.
4. Click **Save**.

Complete these steps to remove a Business Service from the dashboard:

1. Click the devices icon.
2. Select the Business Services to remove from the **Selected Services** list.
3. Click left arrow to move them back to the **Available Services** list.
4. Click **Save**.

Summary View

Business Service Dashboard has two views: Summary view and Drilldown view. The Summary view is the default view when you access the Dashboard.

The first level Summary view displays:

- Incident Counts By Severity and Top Impacted Devices across all Business Services.
- High and Medium Severity Incident Counts for each Business Service.

Click a specific Business Service in the first level to see the second level Summary view. This displays:

- Devices belonging to the Business Service that has triggered incidents.
- For each device:
  - Device Name
  - Device Type
  - Availability Status
  - Incidents and counts – you can click an Incident to see more details in a pop up. From there, you can take action on an incident (for example, drill down the incident on Incident page).

Drilldown View

Click the **Drilldown** button to display the Drilldown view of Business Services.

The first level Drilldown view displays the Incidents of each Business Service.

Click a specific Business Service in the first level to display the second level Drilldown view. It displays the Summary dashboard view of each device belonging to the selected Business Service.

Click the **Overview** button to get back to the Summary view.

Filtering Summary View

In the first level Summary view, you can filter the information displayed by Incident Severity and Organizations (for Service Provider deployments). Choose the values from the respective drop-down lists.

In the second level Summary view, you can filter the information by Device name and type.

Filtering Drilldown View

In the first level Drilldown view, you can filter the information by Organizations (for Service Provider deployments). Simply choose the values from the drop-down list.

In the second level Drilldown view, you can filter the information by Device name and type.

Changing Refresh Interval

Select the refresh interval from the drop-down menu on top-right.

Forcing a Refresh

To update the whole dashboard, select **Refresh Now** on top-right.

Identity and Location Dashboard

In many situations, you would like to know which user is using an IP address and where the user connected from. The Identity and Location Dashboard provides you an audit trail of this information by providing the linkage between:

- Network Identity - IP address, or MAC address
- User identity - user name, host name, or domain
- Location - a wired switch port, a wireless LAN controller, or VPN gateway

The following sections provide more information about Identity and Location Dashboard:

- Data Source
- Adding to the Data Source
- Viewing Identity and Location Dashboard
- Searching for Specific Information

Data Source

This association is built over time by combining information from the following events:

- **Active Directory logon events** – such as Win-Security-540 and Win-Security-4624 that provide IP Address, User, and Domain information
- **DHCP events** – these provide IP, MAC address, and sometimes host name information. Events include:
  - WIN-DHCP-IP-LEASE-RENEW
  - WIN-DHCP-IP-ASSIGN
  - FortiGate-event-DHCP-response-Request
  - FortiGate-event-DHCP-response-Ack
  - AO-WUA-DHCP-IP-LEASE-RENEW
  - AO-WUA-DHCP-IP-ASSIGN
  - Linux_DHCPACK
  - Generic_DHCPACK
  - Cradlepoint-dhcp-updated
- **VPN logon events** – these provide IP and user information. Events include:
  - ASA-713228
  - Juniper-SecureAccess-Session-Start
  - Cisco-VPN3K-IKE/25
  - ASA-722022
  - ASA-713049-Client-VPN-Logon-success
  - FortiGate-ssl-vpn-session-tunnel-up
  - ASA-113019
- **WLAN logon events** – these provide IP and user information. Events include:
  - Aruba-1014-wlsxNUserEntryCreated,
  - FortiGate-Wireless-Client-IP-Assigned
  - Cisco-WLC-53-bsnDot11StationAssociate
- **Cloud Service logon events** – these provide IP and user information. Events include:
  - AWS-CloudTrail-SIGNIN-ConsoleLogin-Success
  - Google_Apps_login_login_success
  - Salesforce_Login_Success
  - OKTA-USER-AUTH-LOGIN-SUCCESS
  - MS_OFFICE365_UserLoggedIn_Succeeded
- **AAA Authentication events** - these provide IP and user information. Events include:
  - Win-IAS-PassedAuth
  - CisACS_01_PassedAuth
- **FortiSIEM Discovery events** – these provide IP, user, and location information. Events include:
  - PH_DISCOV_HOST_LOCATION
  - PH_DISCOV_CISCO_WLAN_HOST_LOCATION
  - PH_DISCOV_ARUBA_WLAN_HOST_LOCATION
  - PH_DISCOV_GEN_WLAN_HOST_LOCATION

Adding to the Data Source

You can modify the file `/opt/phoenix/config/identityDef.xml` file to add new events. Remember to restart the `phIdentityMaster` and `phIdentityWorker` modules on all nodes after the changes are done.

Viewing Identity and Location Dashboard

Identity and Location Dashboard is a spreadsheed style tabular dashboard that displays the following information:

- **IP Address** - IP address of a host whose identity and location is recorded in this result. You can view IP addresses with country flags in a map by clicking **Locations**.
- **MAC Address** - MAC address of the host
- **User Name** - User associated with this IP Address. Obtained from one of these event types in the Data Source section.
- **Host Name** - Host Name from which IP Address was used. Obtained from one of these event types in the Data Source section.
- **Domain** - Provides context for the User. The Information displayed here depends on the logon event type it was obtained from:
  - Windows Domain Logon: Domain name
  - VPN Logon: reporting IP address of the VPN gateway
  - WLAN Logon: reporting IP address of the WLAN controller
  - AAA Logon: reporting IP of the AAA server
- **VLAN ID** - For hosts directly attached to a switch, this is the VLAN ID of the switch port,
- **Connected to** - For hosts attached to a switch port, this is the switch name, reporting IP address, and interface name,
- **First Seen** - The time at which this entry was first created in the AccelOps Identity and Location database,
- **Last Seen** - The time at which some attribute of this entry was last updated. If there is a conflict, for example, a host acquiring a new IP address because of DHCP, then the original entry is closed and a new entry is created. A closed entry will never be updated.
- **Organization** - Displays the Organization to which the IP address belongs for Service Provider installations in a Super/Global View.

Searching for Specific Information

You can search in two ways:

- **Search single field** - use the search box.
  - For Time Range, choose the time ranges in the time range field on the top right
  - For other fields, select the fields in the Search area and enter the value to be searched
- **Search multiple fields at the same time** – use the Filter area
  - Select the field, enter the searched value and click **OK**. The condition will diaplay on the top
  - Select another field and so on.
  - You can clear a condition by clicking the **x** button.

Interface Usage Dashboard

This dashboard provides an overview of the usage of individual interfaces of Router and Firewall devices. The dashboard has three levels:

- The Top view displays device level metrics in a tabular form.
- Once you select a device in the Top view, the middle table shows the basic interface level metrics such as received and sent bytes.
- You can drill-down and get Application level usage and QoS metrics for a specific device interface. To do this, select a device in the Top view and a specific interface in the middle view.

The following sections provide more information about the Interface Usage Dashboard:

- Data Source
- Adding/Removing Devices and Interfaces to the Dashboard
- Viewing Device Level Metrics
- Viewing Interface Level Metrics
- Viewing Application Usage
- Viewing QoS Statistics
- Drill-down from Widgets
- Modifying Widget Information Display
- Changing Refresh Interval
- Forcing a Refresh

Data Source

This dashboard applies to network devices: Routers/Switches and Firewalls.

- Top View - Device level metrics are sourced from Ping monitoring and SNMP.
- Middle View – Basic interface level metrics are also sourced from SNMP.
  - The sent and receive metrics are available for all network devices implementing MIB2 (RFC 1213).
  - Latency, Jitter, and Loss are available for FortiGate Firewalls/UTM devices via SNMP – see FORTINET-FORTIGATE-MIB: `fgSystem.fgLinkMonitor` (see note below on configuration restriction).
- Bottom View
  - Application Usage is available from Netflow
  - QoS values are available for FortiGate Firewalls/UTM devices via SNMP – see FORTINET-FORTIGATE-MIB: `fgIntf.fgIntfBcs.fgIntfBcInTable.fgIntfBcInEntry` for ingress and `fgIntf.fgIntfBcs.fgIntfBcTable.fgIntfBcEntry` for egress.

Configuring Latency, Jitter and Loss

FortiGate SNMP metrics report Latency, Jitter. and Loss by link ID, which is different from SNMP interface ID. FortiSIEM requires that the user configures the link ID to be identical to SNMP interface ID.

SNMP interface IDs are available by running the SNMP walk command: `snmpwalk -v2c -c<cred> <ip> ifName`. In the output, the integer after `ifName` is the interface ID.

```
#snmpwalk -v2c -cpwd 10.1.1.1 ifName
IF-MIB::ifName.1 = STRING: port1
IF-MIB::ifName.2 = STRING: port2
IF-MIB::ifName.3 = STRING: port3
```

Here the SNMP interface ID of port1 is 1, SNMP interface ID of port2 is 2 and so on.

Use the SNMP interface ID in the `config system virtual-wan-link` command – see the examples below:

This is a basic example where the port, health check members and SNMP index can align naturally, however this is not likely to be the case with all configurations.

```
#config system virtual-wan-link
  set status enable
  config members
    edit 1
      set interface port1
    next
    edit 2
      set interface port2
    next
  end

#config health-check
    edit "HC_Backoffice"
                set server "8.8.8.8"
                set update-static-route disable
                set members 1 2
     next
```

As mentioned, to ensure that the Interface SNMP Index ID corresponds to that of the virtual WAN link and the health check, it is required that SNMP index must align. This example and description shows how to configure a FortiGate for SDWAN monitoring with FortiSIEM.

1. The interface should specify the SNMP index, for example, `105` (`set snmp-index 105`):

```
config system interface
   edit "port4"
      set vdom "root"
      set ip 10.1.31.10 255.255.255.240
      set allowaccess ping https ssh
      set type physical
      set netflow-sampler both
      set inbandwidth 50192
      set outbandwidth 50192
      set ingress-shaping-profile "test_Internal"
      set egress-shaping-profile "test_Internal"
      set alias "MPLS"
       set snmp-index 105
      set preserve-session-route enable
   next
end
```

2. The member ID in the virtual WAN link must be same as the SNMP index associated with the Interface, for example, `105`.

```
config system virtual-wan-link
   set status enable
      config members
         edit 105
            set interface "ha"
            set gateway 10.1.31.1
            set comment "MPLS"
            next
```

```
                        ......
                        ......
                  end
            end
```

3. The member ID should be added to a health check, again in this example it is `105`.

```
            config health-check
               edit "TEST_Backoffice"
                     set server "10.10.33.240" "10.10.1.240"
                     set interval 5
                     set update-cascade-interface disable
                     set update-static-route disable
                     set members 1 2 105
               next
            end
```

4. When monitoring Latency, Jitter and Loss via SNMP it is now possible to identify the Interface it is associated with the health check.

```
            [snmpwalk -v2c -c {password} {HostIp} 1.3.6.1.4.1.12356.101.4.9.2.1
            SNMPv2-SMI::enterprises.12356.101.4.9.2.1.3.7 = Gauge32: 105
            SNMPv2-SMI::enterprises.12356.101.4.9.2.1.5.7 = STRING: "20.078" (latency)
            SNMPv2-SMI::enterprises.12356.101.4.9.2.1.6.7 = STRING: "0.736" (Jitter)
            SNMPv2-SMI::enterprises.12356.101.4.9.2.1.9.7 = STRING: "0.000" (Loss)
```

Adding/Removing Devices and Interfaces to the Dashboard

When you create an Interface Usage Dashboard for the first time, no devices are displayed.

Complete these steps to add a device to the dashboard:

1. Click the devices icon.
2. Select the Organization and then click the **Firewall** or **Router Switch** folder.
3. Select a device and its interface of interest.
4. Click the right arrow.
5. Click **Save**.

Complete these steps to remove a device from the dashboard:

1. Click the devices icon.
2. Select the **Device/Interface** pair from the selected list.
3. Click the left arrow.
4. Click **Save**.

This dashboard is data driven. That means the dashboard will be populated only if the metrics are present. First, create a Summary dashboard and see if the devices are present in that dashboard and display values. Then, you will see them in this dashboard.

Viewing Device Level Metrics

The Top view displays Device level metrics. The metrics are averaged over three minute intervals. To see the trend, click the trend icon next to the numbers.

Viewing Interface Level Metrics

Once you select a device in the Top view, the middle table displays the interface level metrics for that device. The metrics are averaged over three minute intervals. To see the trend, click the trend icon next to the numbers.

Viewing Application Usage

Complete these steps to see the Application Usage for an interface:

1. Select a device in the Top view.
2. Select an interface in the Middle view.
3. Click the **Application Usage** tab.

Viewing QoS Statistics

Complete these steps to see the QoS Statistics for an interface:

1. Select a device in the Top view.
2. Select an interface for the selected device in the Middle view.
3. Click the **QoS Statistics** tab.

Drill-down from Widgets

Click the magnifying glass icon on a widget. This will take you to the **ANALYTICS** tab with the values populated. From there, you can analyze the data in more depth.

Modifying Widget Information Display

Follow the steps in Widget Dashboard > Modifying widget information display.

Changing Refresh Interval

Select the refresh interval from the drop-down menu on top-right.

Forcing a Refresh

To update the whole dashboard, select the refresh icon on the top-right menu.

PCI Logging Status Dashboard

A PCI Logging Status dashboard provides an overview of which devices in PCI are logging and logging correctly. The devices are displayed by CMDB Device Groups (for example Windows, Linux, Firewalls, and so on) and by Business Units.

- Setting Up Data Source
- Creating a Dashboard
- Analyzing Dashboard Data
- Searching Dashboard Data

Setting Up Data Source

Data source setup includes the following steps:

1. Creating CMDB Devices
2. Assigning Devices to Business Units
3. Assigning Devices to PCI Business Service
4. Specifying the Criteria for Logging Correctly
5. Specifying the Violation Time Limits

Creating CMDB Devices

The devices must be available in CMDB for displaying in the dashboard. This can be done in any of the following ways:

- Manually:
    a. Go to **CMDB** > select the Device Group > click **New**.
- Discovery:
    a. Create the credentials in **ADMIN** > **Setup** > **Credentials**.
    b. Discover in **ADMIN** > **Setup** > **Discovery**.
- Device Import:
    a. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
    b. Click **New** and choose **Type** as "Device" and **Direction** as "Inbound".
    c. Choose the **File Path** on the Supervisor node and place the CSV file there.
    d. For **Content Mapping**, click the edit icon.
        I. For **Column Mapping**, click **+** and enter the mapping between columns in the **Source** CSV file and the **Destination** CMDB.
            i. Enter Source CSV column Name for **Source Column**.
            ii. Check **Create Property if it Does not Exist** to create the new attribute in FortiSIEM if it does not exist.
                A. Enter a name for the **Destination Column** of the property from the drop-down list.
                B. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite it's current value.
            iii. If the property exists in the CMDB, select FortiSIEM CMDB attribute for **Destination Column**.
            iv. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite its current value.
            v. Click **OK**.
        II. For **Data Mapping**, click **+** and enter the mapping between data values in the external system and the destination CMDB.
    e. Click **Save**.
    f. Select the Instance and click **Run**.

Assigning Devices to Business Units

For the PCI Logging dashboard to display the devices logging and logging correctly by business units, the Business Unit property needs to be set for a device. This can be done in any of the following ways:

- Manually:
  a. Go to **CMDB** > select one or more devices > click **Edit** and set the Business Unit.
  b. Click **Save**.
- Device Import:
  a. Prepare a CSV file containing Device Host Names and Business Unit as two columns. Note that the Device host names must match the host names in CMDB, if they are present.
  b. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
  c. Click **New** and choose **Type** as "Device" and **Direction** as "Inbound".
  d. Choose the **File Path** on the Supervisor node and place the CSV file there.
  e. For **Content Mapping**, click the edit icon.
     I. For **Column Mapping**, click **+** and enter the mapping between columns in the **Source** CSV file and the **Destination** CMDB.
        i. Enter Source CSV column Name for **Source Column**
        ii. Check **Create Property if it Does not Exist** to create the new attribute in FortiSIEM if it does not exist
            A. Enter a name for the **Destination Column** of the property from the drop-down list.
            B. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite it's current value.
        iii. If the property exists in the CMDB, select FortiSIEM CMDB attribute for **Destination Column**.
        iv. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite its current value.
        v. Click **OK**.
     II. For **Data Mapping**, click **+** and enter the mapping between data values in the external system and the destination CMDB.
  f. Click **Save**.
  g. Select the instance and click **Run**.

Assigning Devices to PCI Service

Devices in the PCI Logging Status Dashboard belong to the PCI Business Service. Assigning Devices to the PCI Service can be done in any of the following ways:

- Manually:
  a. Go to **CMDB** > **Business Services** > **Compliance** > select the PCI Service > click **Edit** and add **Devices**.
  b. Click **Save**.
- Device Import:
  a. Prepare a CSV file containing Device Host Names and isPCI property. Host names must match the host names in CMDB. The **isPCI Device Property** takes TRUE or FALSE values.
  b. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
  c. Click **New** and choose **Type** as "Device" and **Direction** as "Inbound".
  d. Choose the **File Path** on the Supervisor node and place the CSV file there.
  e. For **Content Mapping**, click the edit icon.
     I. For **Column Mapping**, click **+** and enter the mapping between columns in the **Source** CSV file and the **Destination** CMDB.

i. Enter Source CSV column Name for **Source Column**
ii. Check **Create Property if it Does not Exist** to create the new attribute in FortiSIEM if it does not exist
A. Enter a name for the **Destination Column** of the property from the drop-down list.
B. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite it's current value.
iii. If the property exists in the CMDB, select FortiSIEM CMDB attribute for **Destination Column**.
iv. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite its current value.
v. Click **OK**.
II. For **Data Mapping**, click **+** and enter the mapping between data values in the external system and the destination CMDB.
f. Click **Save**.
g. Select the instance and click **Run**.

Note: Device Import options in Assigning Devices to Business Units and Assigning Devices to PCI Service can be combined. So it is possible to have a single file with three columns: Host Name, Business Unit, and isPCI.

Specifying Criteria for Logging Correctly

To specify a criteria for logging correctly, define the following:

- **Correctly Logging Reports** – these specify the criteria for devices in a device group to be correctly logging Authentication, FIM, and Change events. Reports must be defined separately for each CMDB device group and each functional category: Authentication, FIM, and Change. Several Correctly Logging Reports are pre-defined in **RESOURCES** > **Reports** > **Function** > **Compliance** > **Compliance Logging Policy**.
- **PCI Logging Policy** – these specify whether a CMDB Device Group needs to correctly send logs in the various functional categories: Authentication, FIM, and Change. Currently, these three functional categories are fixed. PCI Logging Policies can be specified in **ADMIN** > **Settings** > **Compliance** > **PCI**. Several PCI Logging Policies are pre-defined.

Complete these steps to customize correctly logging criteria:

1. Define a report in **RESOURCES** > **Reports** > **Function** > **Compliance** > **Compliance Logging Policy**.
2. Create a PCI Logging Policy in **ADMIN** > **Settings** > **Compliance** > **PCI** and specify the new report.

If you create your own correctly logging report, then it must have the following well-defined structure:

- **Group By Criteria** must have Customer ID and Reporting Device Name.
- **Select Clause** must have Customer ID, Reporting Device Name, and Last Event Receive Time.
- **Filtering Criteria** must be specific to the CMDB Device Group (for example: Firewalls, Routers, Windows Server, and so on) and functional logging category (for example: Authentication, FIM, and Change).

Note: It is highly recommended to clone an existing correctly logging report and modify the Filtering Criteria.

Specifying Violation Time Limits

Specify the time duration after which a device is reported to be not logging or not logging correctly. Four properties are defined in **ADMIN** > **Device Support** > **Custom Properties**:

- **lastAuthTimeLimit** - time limit for authentication logs (default 1 day)
- **lastFIMTimeLimit** - time limit for FIM logs (default 1 day)
- **lastChangeTimeLimit** - time limit for authentication log (default 1 day)
- **lastLogTimeLimit** - time limit for sending any log (default 1 day)

Similar to any other device property, you can change the global defaults and set them on a per-device basis.

Creating a Dashboard

Once you setup the data sources following the steps described in Setting up data source, the dashboard must be created manually.

The dashboard is updated nightly at 12:00 am (Supervisor time). At that time, the Supervisor:

- Runs the reports specified in **ADMIN** > **Settings** > **Compliance** > **PCI**.
- Updates the last reporting times.
- Calculates violations using the thresholds defined in **ADMIN** > **Device Support** > **Custom Properties**.

When you open the PCI Logging Status dashboard, the results are displayed from the daily run of previous night.

Analyzing Dashboard Data

The PCI Logging Status Dashboard displays:

- **Logging** - Percentage of PCI devices logging within the time period lastLogTimeLimit (default 1 day).
- **Logging Correctly** - Percentage of PCI devices logging correctly.
- **Logging By Group** - Percentage of PCI devices logging correctly broken down by Device Group.
- **Logging Correctly By Group** - Percentage of PCI devices logging correctly broken down by Device Group.
- **Logging Correctly By Business Unit, Group** - Percentage of PCI devices logging correctly broken down by Device Group.

The displays are color coded as Red, Yellow, and Green according to the tunable thresholds defined in **Dashboard** > **Threshold Setting**. By default:

- Red – less than 50%
- Yellow – between 50% and 80%
- Green – higher than 80%

If you click the entries, the devices in violation are shown in a tabular format along with the last time they reported events in each category.

Searching Dashboard Data

The Dashboard data can be searched by any Device Property, for example a Business Unit defined in **ADMIN** > **Device Support** > **Custom Properties** with Search (check-box) enabled. Click the search field under a specific category and enter the property values. Matches are exact and case sensitive.

Managing Tasks

FortiSIEM supports Data Anonymization to hide Personally Identifiable Information including IP addresses, host names, user names and email addresses in external and internal logs, Incidents, and CMDB records based on the user role for a specific period of time.

After assigning the user to anonymize a role and creating a Data Anonymization approver, the work-flow is as follows:

a. The user creates a de-anonymization request and sends to the approver.
b. The approver receives an email notification.
c. The approver then verifies and accepts the request for a specific period by setting a validity date. (An approver may also reject a request specifying a valid reason.)
d. If approved, the user can see the de-anonymized data until the validity period.
e. After the validity period, the data is hidden again. To de-anonymize the data, create a new request.

The following procedures describe how a user can submit a task request and the Data Anonymization approver approves or rejects.

- Requesting a De-anonymization Request
- Approving a De-anonymization Request

Requesting a De-anonymization Request

You can send a de-anonymization request with justification, to a Data Anonymization approver, to de-anonymize the requested data for a specific period of time.

1. Go to **TASKS** > **Request** tab.
2. Click **New** to create a de-anonymization request.
3. Select the **Approver** from the drop-down to send this request.
4. Select the **Type** of de-anonymization request.
5. Enter the **Justification** for viewing the data.
6. Click **Save** to send the request to the Data Anonymization approver.

Approving a De-anonymization Request

When a user sends a de-anonymization request, the Data Anonymization approver receives an email notification. The approver can see the list of de-anonymization requests under the **Approval** tab on login. The approver then verifies the justification and provides approval.

1. Go to **TASKS** > **Approval** tab.
2. Select the request from the list or search using the search bar and choose the following options from the drop-down list on the right:
   - **Approve** to allow de-anonymization for a specific time period under **Valid Till** or **For** the date and time listed in the time stamp field. You can click the time stamp field to choose a different date and time. The

default time is two days, if no date/time is selected.
- **Reject** to reject the de-anonymization request specifying a valid **Reason**.

3. Click **OK** to send the approval/rejection.
The user can see the **Status** of this request under the **Request** tab on login.

Note: Fortinet understands that multiple approvers can be selected in a request. Fortinet's behavior in these situations is to acknowledge the approver who first provides approval (or rejection), and ignore any further responses. Furthermore, any approval or rejection is final, meaning it cannot be updated or changed.

If there is an approval for a task, but the another new request for the same task is sent again and another approval is granted, the approval with the shortest expiration takes precedence in this situation.

FortiSIEM Manager

FortiSIEM Manager can be used to monitor and manage multiple FortiSIEM instances. The FortiSIEM Manager needs to be installed on a separate Virtual Machine and requires a separate license.

Note: Only FortiSIEM Manager and FortiSIEM Supervisor instances 6.5.0+ are supported.

FortiSIEM Manager provides the following functionalities:

- Each FortiSIEM Instance needs to register to the FortiSIEM Manager. After successful registration, a 2-way HTTP (S) communication channel is set up between each Instance and the Manager.
- Incidents, License and Health information will be forwarded from each FortiSIEM instance to the FortiSIEM Manager. Incidents are forwarded in near-real time, Health information forwarded once every minute, and License information forwarded once every hour.
- FortiSIEM Manager retains Health information for the last 1 day. FortiSIEM Manager also stores Incidents and the latest License information in local PostGreSQL database. The number of incidents stored depends on the size of the local PostGreSQL database. Raw events are not stored in FortiSIEM Manager. When the user visits the **Triggering Event** tab on the **INCIDENTS** page, raw events are fetched on demand from the FortiSIEM Instance.
- All Incident status changes in each FortiSIEM instance are forwarded to the FortiSIEM Manager. If you create a new rule or make changes to a rule in a FortiSIEM instance, the changes are forwarded to the FortiSIEM Manager.
- From FortiSIEM Manager, you can do the following operations and the changes are propagated to the right FortiSIEM instance(s) with the right FortiSIEM Manager logged-in-user context:
  - Clear, Resolve and Add Comments to one or more Incidents
  - Disable one or more rules and change their severity.
  - Change the severity of an incident
  - Run FortiSOAR Playbooks and Connectors and update Incident Status and Comments
  - A one-click operation to log you into the appropriate FortiSIEM instance where an Incident occurred. This enables you quickly to investigate an Incident in depth.

Communication between FortiSIEM Manager and instances is via REST APIs over HTTP(S).

You have to upgrade FortiSIEM Manager first before upgrading all FortiSIEM Instances - this applies to both Content Update and Software Image Update.

For details in installing FortiSIEM Manager, see the VM or Hardware Installation Guides here.

For details on registering a FortiSIEM instance to the FortiSIEM Manager, see here.

For viewing health and license information in FortiSIEM Manager, see here.

The FortiSIEM Manager provides the following tools.

FortiSIEM Manager Incidents

When a correlation rule triggers, an incident is created in FortiSIEM. This section describes how to view and manage Incidents in FortiSIEM. There are 2 primary views:

- **Overview**: This view provides a "top down" view of the various types of Incidents and impacted hosts.
- **List View**: This tabular view enables the user to search incidents and take actions. (List by Time, Device, Incident)

To interact with an incident, see Acting on Incidents.

FortiSIEM can cross-correlate incident data and perform lookups on selected external ticketing/work flow systems. See Lookups Via External Websites.

FortiSIEM Manager Incidents Overview View

The Overview view provides a "top down" view of various types of Incidents and impacted hosts. Go to **INCIDENTS** > **Overview** to see this view. Overview can set as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list and **Overview** from the **Incident Home** drop-down list.

The panel is divided into four sections:

- **Top Instances by Incident** - displays Incident Counts by Instances and their Severity.
- **Incidents by Category** – displays Incident Counts By Function and Severity.
- **Top Incidents** – displays the Top Incidents sorted first by Severity and then Count.
- **Top Impacted Hosts** – displays Top impacted hosts by Severity or Risk Score.

To change the incident time range, choose the **Time Range** option on the top right. For Service provider installations, choose the appropriate Organizations on top right. By default, the data combined for all Organizations and the Organization is shown next to each host. This view will automatically refresh every minute by default. The refresh menu on top bar allows the user to disable the automatic refresh or choose a different refresh interval.

Incidents by Category

This pane shows the number of unique Security, Performance, Availability, and Change incidents that have triggered in the specified time range.

To drill into a specific category, click the number and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described inIncidents List View.

Top Incidents

This pane shows the Top Incidents, first by Severity and then by Count.

- Each box represents an Incident.
- The color of the box title reflects the Incident Severity.
- The number reflects the unique incidents that has triggered in the chosen time window.
- The entries inside the box represent the IP address and host names appearing in either the Incident Source or Incident Target.
- Boxes are ordered left to right by Incident Severity and then unique incident count. That means that Red colored boxes (High Severity) appear first, then Yellow (Medium Severity), and finally Green (Low Severity). Within boxes of the same color, boxes with a higher number of Incident counts appear first. You can scroll to the right.

To drill down, click the number in the left side bar or each host and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described in Incidents List View.

Top Impacted Hosts by Severity

This pane shows the Top Impacted Hosts, first by Severity and then by Count.

- Each box represents an impacted host (where an Incident has occurred during the specified time window).
- The color of the box title reflects the maximum of Severity over all Incidents.
- The number on the left of the box reflects the unique incidents that have triggered on the host in the chosen time window.
- The entries inside the box represent the incidents that have triggered for that host.
- Boxes are ordered left to right by Incident Severity and then unique incident count. That means that the Red colored boxes (High Severity) appear first, then Yellow (Medium Severity), and finally Green (Low Severity). Within boxes of the same color, boxes with a higher number of Incident counts appear first. You can scroll to the right.

To drill down, click the number in the left side bar or each incident and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described in Incidents List View.

Top Impacted Hosts by Risk Score

This pane shows the Top Impacted Hosts, first by Risk Score.

- Each Box represents an impacted host (where an Incident has occurred during the specified time window).
- The color of the box title reflects the Risk Score (80 and above is Red, 50-79 is Yellow, and less than 50 is Green).
- The number on the left of the box reflects the risk score.
- The entries inside the box represent the incidents that have triggered for that host.
- Boxes are ordered left to right by Risk Score. That means that Red colored boxes (High Risk) appear first, then Yellow colored boxes (Medium Risk), and Green colored boxes (Low Risk).
- You can scroll to the right.

To drill down, click the number in the left side bar or each incident and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described in Incidents List View.

FortiSIEM Manager Incidents - List View

This tabular view enables the user to search incidents and take actions.

- Viewing Incidents
- Acting on Incidents

Viewing Incidents

To see this view, click **INCIDENTS** in the FortiSIEM header. By default, the **List by Time** view opens. The **INCIDENTS** view also allows you to filter data by device and by incident.

You can set **INCIDENTS** as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list. You can filter the **INCIDENTS** view further by choosing **List – by Time**, **List – by Device**, or **List – by Incident** from the **Incident Home** drop down list.

An incident's status can be one of the following:

- **Active**: An ongoing incident.
- **Manually Cleared**: Cleared manually by a user - the incident is no longer active.
- **Auto Cleared**: Automatically cleared by the system when the rule clearing condition is met. Rule clearance logic can be set in the rule definition.
- **System Cleared**: Cleared by the system. All non-security related incidents are cleared from the system every night at midnight local time, and will show a status of **System Cleared**.
- **Externally Cleared**: Cleared in the external ticketing system.

The resolution for an incident can be:

- **Open**
- **True Positive**, or
- **False Positive**

When an **Incident Status** is **Active**, Incident Resolution is **Open**. When an Incident is **Cleared**, then the user can set the **Incident Resolution** to be **True Positive** or **False Positive**. If you are changing the **Incident Resolution** to be **True Positive** or **False Positive**, then you must **Clear** the Incident.

The following sections describe the three views that are available through the **INCIDENTS** view:

- List by Time View
- List by Device View
- List by Incident View

List by Time View

The **List by Time** view displays a table of the incidents which have been active in the last 2 hours. The **Last Occurred** column contains the incidents sorted by time, with the most recent first. By default, the view refreshes automatically every minute. The refresh menu on the top bar allows the user to disable automatic refresh or choose a different refresh interval.

Unique to the **List by Time** view is a list of five time range buttons (15m 1h 1d 7d 30d) which appear above the paginator. They allow you to filter data by the last 15 minutes, 1 hour, 1 day, 7 days, or 30 days.

The following attributes are shown for each incident:

- Severity - High (Red), MEDIUM (Yellow), or LOW (Green).
- Last Occurred - last time this incident occurred.
- Instance - location where the incident occurred.
- Incident - name of the incident.
- Tactics - name of the tactic involved with the incident.
- Technique - name of the technique involved with the incident.
- Reporting - set of devices that is reporting the incident.
- Source - source of the incident (host name or IP address).
- Target - target of the incident (host name or IP address or user).
- Detail - other incident details, for example, Counts, Average CPU utilization, file name, and so on.

To see the incident details, click the incident. A bottom panel appears that shows more details about the incident:

- **Details** - includes the full list of incident attributes that are not shown in the top pane.

Column	Description
Biz Service	Impacted biz services to which either the incident source or target belongs.
Category	Category of incidents triggered.
Cleared Reason	For manually cleared incidents, this displays the reason the incident was cleared.
Cleared Time	Time when the incident was cleared.
Cleared User	User who cleared the incident.
Count	Number of times this incident has occurred with the same incident source and target criteria.
Detail	Event attributes that triggered the incident.
Event Type	Event type associated with this incident. All incidents with the same name have the same Incident Type.
External Cleared Time	Time when the incident was resolved in an external ticketing system.
External Resolve Time	Resolution time in an external ticketing system.
External Ticket ID	ID of a ticket in an external ticketing system such as ServiceNow, ConnectWise, etc.
External Ticket State	State of a ticket in an external ticketing system.
External Ticket Type	Type of the external ticketing system (ServiceNow, ConnectWise, Salesforce, Remedy).
External User	External user assigned to a ticket in an external ticketing system.
First Occurred	The first time that the incident was triggered.
Incident	Name of the rule that triggered the incident. Use the drop-down list near the Incident if you must add this incident to filter.
Incident Comments	Comments added by the user.
Incident ID	Unique ID of the incident in the Incident database.
Incident Status	An incident's status can be one of the following: • **Active**: An ongoing incident.

Column	Description
	• **Manually Cleared**: Cleared manually by a user - the incident is no longer active. • **Auto Cleared**: Automatically cleared by the system when the rule clearing condition is met. Rule clearance logic can be set in the rule definition. • **System Cleared**: Cleared by the system. All non-security related incidents are cleared from the system every night at midnight local time, and will show a status of **System Cleared**. • **Externally Cleared**: Cleared in the external ticketing system.
Incident Title	A system default title or a user-defined title for an incident.
Last Occurred	The last time when the incident was triggered.
Manager Incident ID	The ID of the incident from FortiSIEM Manager.
Notification Recipients	User who was notified about the incident.
Notification Status	Status of the Notification: Success or Fail.
Organization	Organization of the reporting device (for Service Provider installations).
Reporting	Reporting device.
Reporting Device Status	Status of the device: Approved or Pending. You must approve devices for the incidents to trigger, but they will still be monitored.
Reporting IP	IP addresses of the devices reporting the incident.
Resolution	The resolution for an incident can be: • **Open** (not defined or not known whether the incident is True Positive or False Positive) • **True Positive**, or • **False Positive** When an **Incident Status** is **Active**, Incident Resolution is **Open**. When an Incident is **Cleared**, then the user can set the **Incident Resolution** to be **True Positive** or **False Positive**. If you are changing the **Incident Resolution** to be **True Positive** or **False Positive**, then you must **Clear** the Incident.
Severity	Incident Severity is an integer in the range 0-10 (0-4 is set as Low, 5-8 as Medium, and 9-10 as High).
Severity Category	Incident Severity Category: High, Medium or Low.
Source	Source IP or host name that triggered the incident.

Column	Description
Subcategory	Subcategory of the triggered incident. To add custom subcategories to an incident category, see here.
Tactics	Name of the tactics involved with the incident.
Tag	Name of the tag involved with the rule that triggered the incident.
Target	IP or host name where the incident occurred.
Technique	Name of the technique involved with the incident.
Ticket ID	ID of the ticket if created in FortiSIEM.
Ticket Status	Status of any tickets associated with the incident.
Ticket User	User assigned to a ticket if created in FortiSIEM.
View Status	Whether the Incident has been Read or Not.

- **Events** - this displays the set of events that triggered the incident. If an incident involves multiple sub-patterns, select the sub-pattern to see the events belonging to that sub-pattern. For **Raw Event Log** column, click **Show Details** from the drop-down to see the parsed fields for that event.
- **Rule** - this displays the **Definition of Rule that Triggered the Incident** and the **Triggered Event Attributes**.

To close the incident details pane, click the highlighted incident.

List by Device View

The upper pane of the **List by Device** view lists the devices that are experiencing incidents. In the list, the device can be identified by either an IP or a host name. The name of the device is followed by the number of incidents in parentheses. Click the device name to see the incidents associated with the device. The lower portion of the view contains the same features and functionality as the **List by Time** view.

List by Incident View

The upper pane of the **List by Incident** view lists the incidents detected by FortiSIEM. The name of the incident is followed by the number of incidents in parentheses. Click the incident name to see the incidents associated with the device. The lower portion of the view contains the same features and functionality as the **List by Time** view.

Acting on Incidents

The **Actions** menu provides a list of actions that can be taken on incidents. To see a Location View of the incidents, select **Locations** from the **Actions** menu. FortiSIEM has a built in database of locations of public IP addresses. Private IP address locations can be defined in **ADMIN** > **Settings** > **Discovery** > **Location**.

To change the incident attribute display columns in the List View, select **Change Display Columns** from the **Actions** menu, select the desired attributes and click **Close**.

You can perform the following operations using the **Actions** menu:

- Changing the Severity of an Incident
- Searching Incidents
- Clearing One or More Incidents
- Clearing All Incidents from the Incident View
- Disabling One or More Rules
- Adding or Editing Comments for One or More Incidents
- Exporting One or More Incidents into a PDF, RTF, or CSV File
- Emailing Incidents
- Executing a Playbook
- Running a Connector
- Resolve Incident
- Running an External Integration
- Show in Instance

Changing the Severity of an Incident

1. Select the incident.
2. Select **Change Severity** from the **Actions** menu.
3. Select **Change to HIGH**, **MEDIUM**, or **LOW**.

Searching Incidents

1. Select **Search** from the **Actions** menu.
2. In the left pane, click an Incident attribute (for example, Function). All possible values of the selected attribute with a count next to it is shown (for example, Security, Availability and Performance for Function).
   Note: FortiSIEM Manager adds Manager Incident ID as a search parameter.
3. Select any value (for example, Performance) and the right pane updates with the relevant incidents.
4. Click and select other Incident Attributes to refine the Search or click **X** to cancel the selection.

Changing the Time Range for the Search

1. Select **Search** from the **Actions** menu.
2. Near the top of the left panel, click the time value.
3. Click **Relative** or **Absolute**:
   - If you click **Relative**, adjust the time value in the **Last** field.
   - If you click **Absolute** enter a time range. If you select **Always Prior**, enter a time period prior to the current time.

Saving the Search Criteria

Once you have performed your search, follow these steps to save the search criteria:

1. Click the **Save** icon (💾)which appears above the list of incident attributes, and to the right of **Search**.
2. In the **Save Search Filter under by Time as** dialog box, enter a name for the filter or accept the default. The default will be a time stamp value such as `Search Filters - 12/17/2019 17:04:59`.

The filter will appear in the **Search** (🔍 Search ▾) drop-down list, for example:

- When saving a filter based on the List by Time View, it displays in the **Search** drop-down list.
- When saving a filter based on the List by Device View, it displays in the **Search** drop-down list.
- When saving a filter based on the List by Incident View, it displays in the **Search** drop-down list.

Clearing One or More Incidents

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold the **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Clear Incident** from the **Actions** menu.
5. Select whether the **Resolution** is **True Positive** or **False Positive**.
6. Enter a **Reason** for clearing.
7. Click **OK**.

Clearing All Incidents from the Incident View

You can remove all occurrences of selected incidents from the Incident View. This action can potentially span multiple pages.

1. Search for specific incidents and move them into the right pane.
2. Select **Clear All Incidents in View** from the **Actions** menu.
3. Select whether the **Resolution** is **True Positive** or **False Positive**.
4. Enter a **Reason** for clearing.
5. Click **OK**.

Disabling One or More Rules

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold the **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Disable Rule** from the **Actions** menu.
5. For Service Provider installations, select the Organizations for which to disable the rule.
6. Click **OK**.

Adding or Editing Comments for One or More Incidents

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold the **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Edit Comment** from the **Actions** menu.
5. Enter or edit the comment in the edit box.
6. Click **OK**.

Exporting One or More Incidents into a PDF, RTF or CSV File

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold the **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Export** from the **Actions** menu.
5. Enter or edit the comment in the edit box.
6. Select the **Output Format** and **Maximum Rows**.
7. Click **Generate**.
   A file will be downloaded in your browser.

Emailing Incidents

Incidents can be emailed to one or more recipients. Make sure that Email settings are defined in **ADMIN** > **Settings** > **System** > **Email**. Note that email notification from the Incident page is somewhat ad hoc and must be manually setup by the user after the incident has triggered. To define an automatic notification, create an Incident Notification Policy in **ADMIN** > **Settings** > **Notification Policy**. To email one or more incidents on demand:

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Notify via Email** from the **Actions** menu and enter the following information:
   a. Send To – a list of receiver email addresses, separated by commas.
   b. Email template – Choose an email template. You can use the default email template, or create your own in **ADMIN** > **Settings** > **System** > **Email** > **Incident Email Template**.

Resolve Incident

You can directly resolve an incident by taking the following actions.

1. Select the incident.
2. From the **Actions** drop-down list, select **Resolve Incident**.
3. Select the resolution (Open, In Progress, True Positive, False Positive).
4. Click **OK**.

Running an External Integration

Incidents can be handled by an existing external integration policy configured through FortiSIEM.

To create an external integration policy, navigate to **ADMIN > Settings > General > External Settings**. Click **New** to begin creating an external integration. For more information, see Configuring External Integration.

To run an external integration policy, take the following steps:

1. Select an incident.
2. Select **Run External Integration...** from the **Actions** menu.
3. From the **Choose Integration Policy** window, select the existing Integration Policy you want applied to the incident from the drop-down list.
4. When done, click **OK**.

Show in Instance

To show the incident from the Instance, take the following steps.

1. Select the incident.
2. Select **Show in instance** from the **Actions** menu.
3. Select **New windows** or **Current window**.

FortiSIEM Manager CMDB Users

The FortiSIEM Manager CMDB Users page contains information about the users of your system.

FortiSIEM Manager CMDB Adding Users

Complete these steps to add a user:

1. Navigate to **CMDB > Users > Ungrouped**.
2. Click **New** to create a new user.
3. In the **New User** dialog box, enter the detailed information about this user:
    a. Add the user profile information including **User Name**, **Full Name**, **Job Title** and **Company**.
    b. Click the drop-down list to select the **Importance** of this user - "Normal", "Important", "Critical", or "Mission Critical".
    c. Enable **Active** if this is an active user.
    d. Enter the user's **Domain**.
    e. Enter the user's Distinguished Name **DN**.
    f. For **User Lockout**, enter the number of minutes the user will be unable to log into the system after three successive authentication failures.
    g. For **Password Reset**, enter the number of days after which a user’s current password for logging in to the system will automatically expire. If left blank, the user's password will never expire.
    h. For **Idle Timeout**, enter the number of minutes after which an inactive user will be logged out.
    i. Enter the **Employee ID** of the user.
    j. Select the **Manager** to which this user belongs.
    k. For **System Admin**, enable by selecting the System Admin checkbox.
        i. For **Mode**, select **Local** or **External**.
        If you select **Local**, enter and then reconfirm the user password. For **External**, see Authentication Settings for more information about using external authentication.
        Note: If more than one authentication profile is associated with a user, then the servers will be contacted one-by-one until a connection to one of them is successful. Once a server has been contacted, if the authentication fails, the process ends, and the user is notified that the authentication failed.
        ii. Select a **Default Role** for the user.

See the topic Role Settings for a list of default roles and permission.

iii. Click **Back** when done.

l. Click **Contact Info** to enter your personal contact information.

i. Add user contact information to the appropriate contact information fields - **Work Phone**, **Mobile Phone**, **Home Phone**, **SMS**, **SMS Provider**, **ZIP**, **Email**, **Address**, **City**, **State**, and **Country** field.

ii. If your company uses S/MIME for email, make sure the **Email** field is filled out, and upload the S/MIME certificate in the **Certificate** field by clicking **Upload**, and selecting your certificate.

iii. Click **Back** when done.

m. Enter any **Description** about the user.

4. Click **Save**.
   The new user details appear in the list.

Notes:

- When viewing this user list as a Super global user, you may see repetitions of a few **User Names**, where those names exist in multiple Organizations. This can be determined by checking the contents of the Instance/Supervisor on FortiSIEM Manager.

FortiSIEM Manager - Editing User Information

Complete these steps to edit a CMDB user:

1. Navigate to **CMDB > Users >**.
2. Click **Edit**.
3. In the **Edit User** dialog box, update any detailed information about this user:
   a. Edit user profile information including **User Name**, **Full Name**, **Job Title** and **Company**.
   b. Click the drop-down list to select the **Importance** of this user - "Normal", "Important", "Critical", or "Mission Critical".
   c. Enable **Active** if this is an active user.
   d. Update the user's **Domain**.
   e. Update the user's Distinguished Name **DN**.
   f. For **User Lockout**, enter the number of minutes the user will be unable to log into the system after three successive authentication failures.
   g. For **Password Reset**, enter the number of days after which a user’s current password for logging in to the system will automatically expire. If left blank, the user's password will never expire.
   h. For **Idle Timeout**, enter the number of minutes after which an inactive user will be logged out.
   i. Enter the **Employee ID** of the user.
   j. Select the **Manager** to which this user belongs.
   k. For **System Admin**, enable by selecting the System Admin checkbox.
      i. For **Mode**, select **Local** or **External**.
         If you select **Local**, enter and then reconfirm the user password. For **External**, see Authentication Settings for more information about using external authentication.
         Note: If more than one authentication profile is associated with a user, then the servers will be contacted one-by-one until a connection to one of them is successful. Once a server has been contacted, if the authentication fails, the process ends, and the user is notified that the authentication failed.

    ii. Select a **Default Role** for the user.
        See the topic Role Settings for a list of default roles and permission.
    iii. Click **Back** when done.
  l. Click **Contact Info** to update the user's personal contact information.
    i. Update the user contact information in the appropriate contact information fields - **Work Phone**, **Mobile Phone**, **Home Phone**, **SMS**, **SMS Provider**, **ZIP**, **Email**, **Address**, **City**, **State**, and **Country** field.
    ii. If your company uses S/MIME for email, make sure the **Email** field is filled out, and upload the S/MIME certificate in the **Certificate** field by clicking **Upload**, and selecting your certificate.
    iii. Click **Back** when done.
  m. Update the **Description** about the user.
4. Click **Save**.

You can also use the following functions on the **Actions** menu:

- **Unlock** - to unlock a user, select the user from the list and click **Actions** >**Unlock**.

FortiSIEM Manager Resources

The following sections provide the procedures for managing Resources from FortiSIEM Manager:

FortiSIEM Manager Resources Rules

FortiSIEM continuously monitors your IT infrastructure and provides information to analyze performance, availability, and security. There may also be situations in which you want to receive alerts when exceptional, suspicious, or potential failure conditions arise. You can accomplish this using rules that define the conditions to watch out for, and which trigger an incident when those conditions arise. FortiSIEM includes over 500 system-defined rules, which you can see in **RESOURCES > Rules**.

From FortiSIEM Manager, you can export rules to enable, disable, or change the severity.

- Enable/Disable Rules
- Change Rule Severity

You cannot add, import, clone, or test rules from FortiSIEM Manager.

Enable/Disable Rules

To enable/disable rules, take the following steps.

1. Select the rule(s) you wish to enable or disable.
2. Click on the **Active** column where the rule(s) are selected.
3. Check or uncheck the **Active** box to enable or disable the rules, and select the organization(s).
4. Click **Save**.

Change Rule Severity

To change a rule's severity, take the following steps.

1. Select the rule you wish to change the severity of.
2. Click **Edit > Selected Rule**.
3. Click **Step 3: Define Action**.
4. From the **Severity** drop-down list, change the severity of the rule.
5. Click **Save**.

FortiSIEM Manager Resources Connectors

FortiSIEM Manager allows you to update Connectors from FortiSIEM Instances. See Updating Connectors for more information.

A connector is a solitary action that can be run by a user. Connectors can only be added, modified, or deleted through FortiSOAR. A connector can be run on an event or incident. After creating a FortiSIEM user in FortiSOAR and configuring Connector on FortiSIEM, connectors can be run through FortiSIEM. Additional information can also be found in Playbooks and Connectors under Writing FortiSIEM Compatible FortiSOAR Playbooks available in the Appendix.

FortiSIEM Manager Resources Playbooks

FortiSIEM Manager allows you to update Playbooks from FortiSIEM instances. See Updating Playbooks for more information.

A Playbook is a chain of actions that are taken based on logic programmed by a user. A Playbook can only be added, modified, or deleted through FortiSOAR. Playbooks can be executed on an event or incident. After creating a FortiSIEM user in FortiSOAR and configuring Playbook on FortiSIEM, playbooks can be executed through FortiSIEM. Additional information can also be found in Writing FortiSIEM Compatible FortiSOAR Playbooks available in the Appendix.

FortiSIEM Manager Resources - Event Types

The FortiSIEM Manager Resources Event Types page allows you to view existing event types.

FortiSIEM Manager Admin

The following sections provide the procedures under FortiSIEM Manager ADMIN:

See Settings for configuring FortiSIEM Manager as a FortiSIEM instance.

FortiSIEM Manager Setup

The FortiSIEM Manager Setup page allows you to add, edit, delete, or unregister FortiSIEM instances. Existing FortiSIEM instances appear on this page. For information about the existing FortiSIEM instances, see the table.

- Add a FortiSIEM Instance
- Edit a FortiSIEM Instance
- Delete a FortiSIEM Instance
- Unregister a FortiSIEM Instance

Column	Description
ID	Displays the ID of the FortiSIEM instance.
Name	Displays the name of the FortiSIEM instance.
FQDN	Displays the fully qualified domain name of the FortiSIEM instance.
Admin User	Displays the role.
Registered	Shows whether an instance is registered or not.
Description	Any additional information about the FortiSIEM instance is shown here.

Add a FortiSIEM Instance

To add a FortiSIEM instance, take the following steps from FortiSIEM Manager.

From **ADMIN > Setup**, take the following steps.

1. Click **New**.
2. In the **FortiSIEM Instance Name** field, enter the name of the FortiSIEM Instance.
3. In the **Admin User** field, enter the administrator user name.
4. In the **Admin Password** field, enter the password to be associated with the administrator user name.
   Note: The password must be between 8-64 characters, with at least one uppercase letter, one lowercase letter, one number and 1 special character.
5. In the **Confirm Admin Password** field, re-enter the password from step 4.
6. (Optional) In the **Description** field, enter any additional information you wish to have related to the FortiSIEM instance.
7. Click **Save**.

At this point, you can register the instance by following the steps in Configuring FortiSIEM Instance for FortiSIEM Manager.

Edit a FortiSIEM Instance

To edit a FortiSIEM instance, take the following steps from FortiSIEM Manager.

From **ADMIN > Setup**, take the following steps.

Note: The Admin User and Password cannot be changed.

1. Select the FortiSIEM instance you wish to edit.
2. Click **Edit**.
3. In the **FortiSIEM Instance Name** field, enter the name of the FortiSIEM Instance.
4. (Optional) In the **Description** field, enter any additional information you wish to have related to the FortiSIEM instance.
5. Click **Save**.

Delete a FortiSIEM Instance

To delete a FortiSIEM instance, take the following steps from FortiSIEM Manager.

From **ADMIN > Setup**, take the following steps.

1. Select the FortiSIEM instance you wish to delete.
2. Click **Delete**.
3. Click **Yes** to confirm.

Unregister a FortiSIEM Instance

To unregister a FortiSIEM instance, take the following steps from FortiSIEM Manager.

From **ADMIN > Setup**, take the following steps.

1. Select the FortiSIEM instance you wish to unregister.
2. Click **Unregister**.
3. Click **Yes** to confirm.

FortiSIEM Manager Health

The FortiSIEM Manager Health page displays the health of your FortiSIEM Manager, FortiSIEM Instances, and their worker's, collector's and agent's health, if applicable. The status is also color coded to quickly identify any health issues. Green is normal "Example FortiSIEM Instance", yellow is a risk "Example FortiSIEM Instace", and red is critical, "Example FortiSIEM Instance".

The name of the FortiSIEM Manager or FortiSIEM Instance is displayed in the header. Each row displays the health status of related FortiSIEM devices, and if more than one device exists for a worker, collector, or agent, the number is displayed as well.

Clicking on the header of the FortiSIEM Manager or a FortiSIEM instance will take you to the Cloud Health page. See FortiSIEM Manager Cloud Health for more information.

Clicking on the Collector link will take you to the Collector Health page. See FortiSIEM Manager Collector Health for more information.

FortiSIEM Manager Cloud Health

The FortiSIEM Manager Cloud Health page displays the status of the nodes in your deployment and the processes running on them. The top frame displays all of the available clouds and the lower frame provides information about the applications that are contained in the cloud selected in the main frame.

Click on the FortiSIEM Manager or FortiSIEM Instance heading (center top) to return to the FortiSIEM Manager Health Page.

Complete these steps to view the information about Cloud health:

- From the FortiSIEM Manager Health page, click on the FortiSIEM Manager header or a FortiSIEM instance header. The Cloud Health page displays the health of your FortiSIEM Manager or instance.
  See the FortiSIEM Back-End Processes table for more information about the system role played by each process.
  or
- From the FortiSIEM Manager Health page, click on a Collector link from a FortiSIEM instance to go to the Collector Health page for that FortiSIEM Instance's Collector(s).

First Frame

Note: For some settings, a chart icon will appear when hovering over a value. Click on the icon to get chart information.

Settings	Description
Name	Name of the available clouds
IP Address	IP address of the available clouds
Module Role	Module role, for example, 'Supervisor'
Health	Current health of the cloud. This is color coded (normal - green, warning - yellow, critical - red)
Last Status Updated	The date and time when the most recent status occurred.
Version	Current version of the cloud
Cores	Number of cores
Memory Size	The memory size
Swap Size	The swap size
EPS	Events per second **Note**: Only appears for instances, not FortiSIEM Manager.
Load Average	Average load of the cloud
CPU	Percentage CPU used
Memory	Percentage Memory used
Swap	Percentage Swap space used
Disk	Percentage Disk used
Max Disk Read Wait	The maximum disk read/wait time (milliseconds).
Max Disk Write wait	The maximum disk write/wait time (milliseconds).
Upload Buffer	The current upload buffer size (KB) and queue.
Content Version	The version of the content.

Second Frame

Settings	Description
Process Name	Name of the process
Owner	The owner of the process
Status	Status of the process
Uptime	Total up time of the process
CPU	Measure of the CPU that the process is using
Memory	Measure of the Memory that the process is using
Resident Memory	The amount of memory the process is allocated
Disk Read Rate	The disk read rate speed (KBps)
Disk Write Rate	The disk write rate speed (KBps)
SharedStore Type	SharedStore type (reader, writer)
SharedStore Position	SharedStore location
SharedStore Percent	SharedStore utilization percentage

FortiSIEM Back-End Processes

Process	Function	Present in Manager	Present in Supervisor	Present in Worker	Present in Collector
Apache	Webserver for front-ending http(s) requests to AppSvr or other FortiSIEM nodes	x	x	x	x
AppSvr	Middleware for handling GUI requests, storing and managing PostgreSQL database and serving REST API requests from FortiSIEM nodes	x	x		

Process	Function	Present in Manager	Present in Supervisor	Present in Worker	Present in Collector
DBSvr	PostgreSQL Database for storing information displayed in FortiSIEM GUI other than events	x	x		
Node.js-charting	Message				
Node.js-pm2					
phAgentManager	Collects logs and metrics from devices or servers using protocols other than SNMP and WMI.		x	x	x
phCheckpoint	Collects logs from Checkpoint firewalls via LEA				
phDataManager	Stores the parsed events to event store (FortiSIEM EventDB or Elasticsearch)		x	x	
phDataPurger	Archives online event store (FortiSIEM EventDB or Elasticsearch). Implements event retention policy for FortiSIEM EventDB - both online FortiSIEM EventDB and archive.		x		
phDiscover	Discovers devices using various protocols such as SNMP, WMI and SSH		x		x
phEventForwarder	Forwards events from FortiSIEM to external Systems		x	x	x
phIpIdentityMaster	Merges Identity and location audit trails from multiple phIpIdentityWorker modules to produce the final Identity and location audit trail. Stores the trail in PostgreSQL Database.				
phIpIden-	Produces Identity and loc-		x	x	

Process	Function	Present in Manager	Present in Supervisor	Present in Worker	Present in Collector
tityWorker	ation audit trail based on its own view of events				
phMonitor	Monitors the health of FortiSIEM processes. Distributes tasks from AppSvr to various processes on Supervisor and to phMonitor on Worker for further distribution to processes on Worker nodes.	x	x	x	x
phParser	Parses raw events and prepares them for storing into event store (FortiSIEM EventDB or Elasticsearch)		x	x	x
phPerfMonitor	Continually collects performance monitoring and configuration change data after discovery completes		x	x	x
phQueryMaster	Handles Adhoc queries from GUI for FortiSIEM EventDB. Paralellizes queries by sending them to phQueryWorkers and merges individual results to produce the final result.		x		
phQueryWorker	Handles individual FortiSIEM EventDB queries from phQueryMaster		x	x	
phReportLoader	Loads Report data into Report Server.		x		
phReportMaster	Handles individual FortiSIEM EventDB inline reports. Produces results every 5 minutes.		x		
phReportWorker	Handles inline event reports FortiSIEM EventDB.Merges individual inline report results multiple		x		

Process	Function	Present in Manager	Present in Supervisor	Present in Worker	Present in Collector
	phReportMaster modules to produce the final result. Rolls up results from 5 minute intervals to 15 minute intervals and then to 60 minute intervals.				
phRuleMaster	Triggers a rule in real time by evaluating rule summaries from individual phRuleWorker modules		x		
phRuleWorker	Evaluates a rule in real time based on events seen by the worker and sends a summary to the phRuleMaster module		x	x	
Redis	In-memory distributed database for holding results returned by Elasticsearch and for distributing CMDB objects between Supervisor and Worker nodes.		x	x	
Rsyslogd	Responsible for forwarding locally generated logs to FortiSIEM.	x	x	x	x
SVNLite	A light weight version of Subversion, this file revision management tool stores the file change history for windows/linux servers, routers/switches and windows/linux agents. **Note**: • Files are stored in `/svn/repos`. • To conserve space, files are automatically deleted when the disk gets full based on thresholds defined in		x		

Process	Function	Present in Manager	Present in Supervisor	Present in Worker	Present in Collector
	svn-lite.revisions.purge on the Supervisor.				

FortiSIEM Manager Collector Health

If your FortiSIEM deployment includes Collectors, you can monitor the status of the Collectors by clicking on a Collector link from the FortiSIEM Manager Health page.
Refer to the 'FortiSIEM Back-End Processes' table below for information about the processes that run on Collectors.

Click on the FortiSIEM Instance heading (center top) to return to the FortiSIEM Manager Health Page.

Properties Associated with Collector Health

Note: For some settings, a chart icon will appear when hovering over a value. Click on the icon to get chart information.

Collector Property	Description
Organization	Name of the organization to which the Collector belongs.
Name	Name of the Collector.
IP Address	IP address of the Collector.
Health	The health of the Collector. If Health is **Critical**, it means that one of the modules is not running on the Collector.
Last Status Updated	Health of the Collector based on the health of the modules running on it.
Collector Type	The Collector type is displayed.
Version	The version of the Collector is displayed.
Cores	The number of cores on the Collector is displayed.
Memory Size	The memory size of the Collector is displayed.
Swap Size	The swap size of the Collector is displayed.
Uptime	Total time that the Collector has been up.

Collector Property	Description
EPS	The EPS that the Collector is currently seeing.
CPU	Overall CPU utilization of the Collector.
Memory	Overall memory utilization of the Collector.
Swap	Overall swap utilization of the Collector.
Disk	Overall disk utilization of the Collector.
Max Disk Read Wait	The maximum disk read/wait time (milliseconds).
Max Disk Write wait	The maximum disk write/wait time (milliseconds).
Upload Buffer	The total Buffer in KB used for upload.
Last Event Time	The time when the collector last reported events to the cloud.
Last File Received	The time when the collector last reported its performance status to the cloud.
Upgrade Version	If the Collector has been upgraded, the new version.
Build Date	Date on which the version of FortiSIEM the Collector is running on was built.
Content Version	Version of FortiSIEM the Collector is running on.
Content Update Status	The status of the content update is displayed.
Collector ID	The Collector's ID is displayed.
Install Status	The Install Status of the Collector is displayed.
Download Status	The download status for the Collector is displayed.

Process Properties

Process Property	Description
Process Name	Name of the process.

Process Property	Description
Owner	The owner of the process.
Status	Status of the process as either **Up** or **Down**.
Uptime	Total time that the process has been up.
CPU	Measure of the CPU that the process is using.
Memory	Measure of the Memory that the process is using.
Resident Memory	The amount of memory the process is allocated.
Disk Read Rate	The disk read rate speed (KBps)
Disk Write Rate	The disk write rate speed (KBps)

FortiSIEM Back-End Processes

Process	Function	Used by Supervisor	Used by Worker	Used by Collector
phAgentManager	Execute event pulling job	**X**	**X**	**X**
phCheckpoint	Execute checkpoint monitoring	**X**	**X**	**X**
phDiscover	Pulling basic data from target	**X**		**X**
phEventForwarder	Responsible for forwarding events and incidents from FortiSIEM to external systems	**X**	**X**	**X**
phEventPackage	Uploading event/SVN file to Supervisor/Worker			**X**
phMonitorAgent	Monitoring other processes	**X**	**X**	**X**
phParser	Parsing event to shared store (SS)	**X**	**X**	**X**
phPerfMonitor	Execute performance job	**X**	**X**	**X**

Process	Function	Used by Supervisor	Used by Worker	Used by Collector
rsyslogd	Responsible for forwarding locally generated logs to FortiSIEM	X	X	X

Collector Property	Description
Host IP	The Host IP address of the tunnel.
Super Port	The supervisor port.
Protocol	The protocol used by the tunnel.
Protocol Port	The port used by the protocol.
Collector	The collector with the open tunnel.
PID	The Process ID.
Opened Time	The amount of time the tunnel is open.

FortiSIEM Manager License

The FortiSIEM Manager License page displays information about your FortiSIEM Manager license and any registered FortiSIEM instances. It is color coded.

- Green - License expiration date is greater than or equal to two weeks.
- Yellow - License expires in less than two weeks.
- Red - License has expired.

To upload a license, click **UPLOAD**, select your license, enter your User ID, Password, then click **Upload**.

To refresh the status, click **Refresh**.

FortiSIEM Manager	Description
Serial Number	Displays the serial number.
Hardware ID	Displays the hardware ID, if applicable.
License Type	Displays the license type.
FIPS Mode	Displays whether FIPS mode is enabled or disabled.
Instances	Displays the number of active instances, the total number of instances available

FortiSIEM Manager	Description
	under the license, and the expiration date of the license.
Maintenance and Support	Displays the status and expiration date for your maintenance and support license.

FortiSIEM Supervisor Instance	Description
Serial Number	Displays the serial number.
Hardware ID	Displays the hardware ID, if applicable.
License Type	Displays the license type.
FIPS Mode	Displays whether FIPS mode is enabled or disabled.
Devices	Displays the number of active devices under use from the license, the total number of devices allocated to the license, and expiration date.
EPS	Displays the total active Events Per Second (EPS) number, the total available EPS under the license, and expiration date. A chart icon can be clicked to view a chart showing EPS trends.
Agents	Displays the number of active Agents, the total number of Agents available under the license, and expiration date.
UEBA	Displays the number of User and Entity Behavior (UEBA) Analytics under use, the total number of User and Entity Behavior Analytics available and expiration date.
IOC Service	Displays the status and expiration date for your Indicator of Compromise (IOC) service license.
Support	Displays the status and expiration date for your support license.

FortiSIEM Manager Content Update

The **ADMIN** > **Content Update** page displays the FortiSIEM Manager version that is running and can be used to check if there are available updates. If any updates are available, they can be downloaded and installed. Content Updates must be done in the following order:

1. Upgrade FortiSIEM Manager.
2. Upgrade FortiSIEM Supervisor.
3. Upgrade FortiSIEM Worker.

Specific Content Pack Updates information can be found here.

Instructions for content updates on the FortiSIEM Manager are the same as the FortiSIEM Supervisor. See Content Update for more information.

Appendix

Administrative Tools and Information

The following administrative tools and procedures are available.

Adding Network Interfaces

FortiSIEM is configured to only use eth0 network interface by default. This section describes steps to add another interface, so that GUI traffic, storage traffic, and device access traffic can be split across multiple interface via proper routing.

Notes:

1. Primary (eth0) should not be removed or disabled and is required for normal operation of FortiSIEM.
2. These are general steps to add interfaces. These instructions do not cover making changes to the firewall.

To configure an additional network interface, choose the appropriate FortiSIEM deployment.

- Adding Interfaces for FortiSIEM Virtual Machine Based Deployments
- Adding Interfaces for FortiSIEM Hardware Appliances

Adding Interfaces for FortiSIEM Virtual Machine Based Deployments

Take the following steps to configure your FortiSIEM Virtual Machine based deployment with an additional network interface.

Step 1 - Modify VM Hardware Configuration on the Hypervisor

Log into the hypervisor and add a new network interface into FortiSIEM.

1. Edit the Supervisor VM.
2. Add a new network device to the VM.
3. Associate it with the desired network on the host.
4. Save configuration.
   Note: You may be required to reboot the FortiSIEM VM so that the network interface is available within the FortiSIEM VM.

Step 2 - Configure the Additional Interface on FortiSIEM

SSH into the Supervisor as root.

1. Verify if the interface added in Step 1 is available by running the following command.
   `ifconfig -a`

   Note: eth1, bolded in ifconfig -a Output, is the name of the new interface that was added.

   ifconfig -a Output

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.30.57.230  netmask 255.255.252.0  broadcast 172.30.59.255
        inet6 fe80::250:56ff:fea9:c9c9  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:a9:c9:c9  txqueuelen 1000  (Ethernet)
        RX packets 50833491  bytes 30705896470 (28.5 GiB)
        RX errors 0  dropped 26644  overruns 0  frame 0
        TX packets 9726951  bytes 66973923534 (62.3 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::d215:a34c:98a5:6e23  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:a9:78:29  txqueuelen 1000  (Ethernet)
        RX packets 1200  bytes 74944 (73.1 KiB)
        RX errors 0  dropped 5  overruns 0  frame 0
        TX packets 13  bytes 1790 (1.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 110506670  bytes 72885247042 (67.8 GiB)
        RX errors 0  dropped 418  overruns 0  frame 0
        TX packets 110506670  bytes 72885247042 (67.8 GiB)
```

```
              TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Configure the interface by taking the following steps.
   Note: The interface name may differ due to hypervisor naming of interfaces. Below is an example of interface named eth1.

   a. Run the following command to go to the network-scripts directory.

   ```
   cd /etc/sysconfig/network-scripts/
   ```

   b. Run the following command to create the ifcfg-eth1 file from ifcfg-eth0.

   ```
   cp -a ifcfg-eth0 ifcfg-eth1
   ```

   c. Edit the `ifcfg-eth1` file and save changes (can be done via vi editor for example), following the instructions that appear after "<<".

   ```
   TYPE=Ethernet
   BOOTPROTO=static
   NAME=eth0   << change to new interface name
   DEVICE=eth0 << change to new interface name
   ONBOOT=yes
   IPV6INIT=no

   IPADDR=172.30.57.230  << change the IP to the new IP
   NETMASK=255.255.252.0 << change the netmask to the new netmask
   GATEWAY=172.30.56.1   << remove the line or comment as eth0 typically has
   the default gateway defined.

   DNS1=1.1.1.1
   DNS2=172.30.1.106
   ```

   d. Reset the interface to take the configuration in effect by running the following commands.

   ```
   # ifdown eth1
   # ifup eth1
   ```

3. Optional: Configure routes to other networks via the additional interface
   Adding route example:

   ```
   # ip route add <network_ip>/<cidr> via <gateway_ip> dev <network_card_name> metric <metric_value>
   ```

   Example:
   ```
   ip route add 172.30.0.0/16 via 172.30.52.1 dev eth1 metric 101
   ```

   If you want to manually create a routing configuration file and make it persistent across reboots, then follow these steps. Suppose you want to create an IPv4 route to the 172.30.0.0/16 network via eth1 interface, with 172.30.52.1 as the default gateway. The gateway for the static route must be directly reachable on eth1.

   a. Add the static IPv4 route to the `/etc/sysconfig/network-scripts/route-eth1` file:

   ```
   172.30.0.0/16 via 172.30.52.1 dev eth1
   ```

b. Restart the network:

```
# systemctl restart network
```

4. Verify connectivity through all interfaces.

Adding Interfaces for FortiSIEM Hardware Appliances

The physical interfaces should already be available. The number may vary depending on the HW appliance, e.g. the HW appliance may display 4 interfaces: eth0 thru eth3 (4 interfaces in total).

After you SSH onto the supervisor as root, take the following steps.

1. Verify the available interfaces by running the following command.

```
# ifconfig -a
```

Your ifconfig -a output should appear similar to the following, and allow you to confirm the available interfaces. In this case, eth1, eth2, eth3, which are bolded, are identified interfaces.

ifconfig -a Output

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.65.20.201  netmask 255.255.252.0  broadcast 10.65.23.255
        inet6 fe80::ae1f:6bff:fe47:b318  prefixlen 64  scopeid 0x20<link>
        ether ac:1f:6b:47:b3:18  txqueuelen 1000  (Ethernet)
        RX packets 31177113  bytes 7280636740 (6.7 GiB)
        RX errors 0  dropped 3746071  overruns 0  frame 0
        TX packets 617574  bytes 142045223 (135.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfb560000-fb57ffff

eth1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether ac:1f:6b:47:b3:19  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfb540000-fb55ffff

eth2: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether ac:1f:6b:47:b3:1a  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfb520000-fb53ffff

eth3: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether ac:1f:6b:47:b3:1b  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
            device memory 0xfb500000-fb51ffff

    lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
            inet 127.0.0.1  netmask 255.0.0.0
            inet6 ::1  prefixlen 128  scopeid 0x10<host>
            loop  txqueuelen 1000  (Local Loopback)
            RX packets 7419278  bytes 387353322 (369.4 MiB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 7419278  bytes 387353322 (369.4 MiB)
            TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Configure the new interface.
   Note: Choose any interface you would like to configure. This example provides an example for configuring eth1.

   a. Run the following command to go to the network-scripts directory.

   ```
   cd /etc/sysconfig/network-scripts/
   ```

   b. Run the following command to create ifcfg-eth1 using ifcfg-eth0.

   ```
   cp -a ifcfg-eth0 ifcfg-eth1
   ```

   c. Edit the ifcfg-eth1 file and save changes, following the instructions that appear after the "<<".

   ```
   TYPE=Ethernet
   BOOTPROTO=static
   NAME=eth0   << change to new interface name
   DEVICE=eth0 << change to new interface name
   ONBOOT=yes
   IPV6INIT=no

   IPADDR=172.30.57.230  << change the IP to the new IP
   NETMASK=255.255.252.0 << change the netmask to the new netmask
   GATEWAY=172.30.56.1   << remove the line or comment as eth0 typically has
   the default gateway defined.

   DNS1=1.1.1.1  << add at least one DNS server
   DNS2=172.30.1.106
   ```

   If using vi, save the configuration by pressing ESC then :x!

   d. Reset the interface to take the configuration in effect by running the following commands.

   ```
   # ifdown eth1
   # ifup eth1
   ```

3. Optional: Configure routes to other networks via the additional interface.
   Adding route example:

   ```
   # ip route add <network_ip>/<cidr> via <gateway_ip> dev <network_card_name> met-
   ric <metric_value>
   ```

   Example:

   ```
   ip route add 172.30.0.0/16 via 172.30.52.1 dev eth1 metric 101
   ```

If you want to manually create a routing configuration file and make it persistent across reboots, then follow these steps. Suppose you want to create an IPv4 route to the 172.30.0.0/16 network via eth1 interface, with 172.30.52.1 as the default gateway. The gateway for the static route must be directly reachable on eth1.

a. Add the static IPv4 route to the `/etc/sysconfig/network-scripts/route-eth1` file:

```
172.30.0.0/16 via 172.30.52.1 dev eth1
```

b. Restart the network.

```
# systemctl restart network
```

4. Verify connectivity through all interfaces.

Backing Up and Restoring Databases

- Backing Up and Restoring CMDB
- Backing Up and Restoring EventDB
- Backing Up and Restoring SVN

Backing Up and Restoring CMDB

The FortiSIEM Configuration Management Database (CMDB) contains discovered information about devices, servers, networks and applications. You should create regular backups of the CMDB that you can use to restore it in the event of database corruption.

- CMDB Backup Procedure
- CMDB Restore Procedure

CMDB Backup Procedure

The database files are stored in `/cmdb/data`. FortiSIEM automatically backs up this data twice daily and the backup files are stored in `/data/archive/cmdb`. To perform a backup, move these files to another location. For example:

```
[root@SaaS-Sup cmdb] #cd /data/archive/cmdb

[root@SaaS-Sup cmdb] #cp phoenixdb* /<another>/<mount>/<point>
```

If your `/data` disk is on an external NFS mount then your CMDB backup is already separate from the VM infrastructure.

```
[root@SaaS-Sup cmdb]# pwd

/data/archive/cmdb

[root@SaaS-Sup cmdb]# ls -lt

total 1213952

-rw-rw-rw- 1 root root 95559457 Apr 20 03:02 phoenixdb_2011-04-20T03-00-01

-rw-rw-rw- 1 root root 93010144 Apr 19 13:04 phoenixdb_2011-04-19T13-00-02

-rw-rw-rw- 1 root root 91142941 Apr 19 03:02 phoenixdb_2011-04-19T03-00-01

-rw-rw-rw- 1 root root 89686080 Apr 18 13:03 phoenixdb_2011-04-18T13-00-02
```

CMDB Restore Procedure

If your database becomes corrupted, you can restore it from backup by performing these steps on your Supervisor node.

1. Stop all processes with this phTools command:
   ```
   #phtools --stop all
   ```
2. Check that all processes have stopped.
   ```
   #phstatus
   ```
   These processes will continue to run, which is expected behavior:
   ```
   phMonitor     1-01:55:17     0            992m          540m
   Apache        1-01:56:45     0            236m          9720
   AppSvr        1-01:56:35     0            3908m         758m
   DBSvr         1-01:57:06     0            383m          6656
   ```
3. Copy the latest `phoenixdb_<timestamp>` file to a directory like `/tmp` on the Supervisor host.
4. Go to `/opt/phoenix/deployment`.
5. Run `db_restore /tmp/phoenixdb_<timestamp>`.
6. When this process completes, reboot the system.
   ```
   #reboot
   ```

Backing Up and Restoring EventDB

- EventDB Backup Procedure
- EventDB Restore Procedure

EventDB Backup Procedure

The event data is stored in `/data/eventdb`. Since this data can become very large over time, you should use a program such as rsync to incrementally move the data to another location. From version 4.2.1, the rsync program is installed on FortiSIEM by default.

Use this command to back up the EventDB.

```
#rsync -a --progress /data/eventdb /<another>/<mount>/<point>
```

EventDB Restore Procedure

To restore EventDB there are two options:

- Mount the directory where the event database was backed up.
- Copy the backup to the **/data/eventdb** directory.

These instructions are for copying the backup to the **/data/eventdb** directory.

1. Stop all running processes.
   ```
   #phtools --stop all
   ```
2. Check that all processes have stopped.
   ```
   #phstatus
   ```
   You will see that these processes are still running, which is expected behavior.
   These processes will continue to run, which is expected behavior:
   ```
   phMonitor     1-01:55:17     0            992m          540m
   Apache        1-01:56:45     0            236m          9720
   ```

```
AppSvr         1-01:56:35      0            3908m         758m
DBSvr          1-01:57:06      0            383m          6656
```

3. Copy the EventDB to the event DB location `/data/eventdb`. If you use the `cp` command, it may appear that the command has hung if there is a lot of data to copy.
   ```
   #cp -a /backup/eventdb /data/eventdb
   ```
   Alternatively, you can use rsync and display the process status.
   ```
   #rsync -a --progress /backup/eventdb /data/eventdb
   ```
4. Once complete, restart all processes.
   ```
   #phtools --start all
   ```
5. Check that all processes have started.
   ```
   #phstatus
   ```

Backing Up and Restoring SVN

FortiSIEM uses an inbuilt SVN to store network device configuration and installed software versions.

- SVN Backup
- SVN Restore

SVN Backup

The SVN files are stored in `/svn`. Copy the entire directory to another location.

```
# cd /
# cp -r /svn /<another>/<mount>/<point>
```

SVN Restore

Copy the entire `/svn` from the backup location and rename the directory to `/svn`.

```
# cd /<another>/<mount>/<point>
# cp -r svn /
```

Creating and Restoring ESX Snapshots

- Create FortiSIEM VM Snapshot
- Restoring FortiSIEM VM from Snapshot

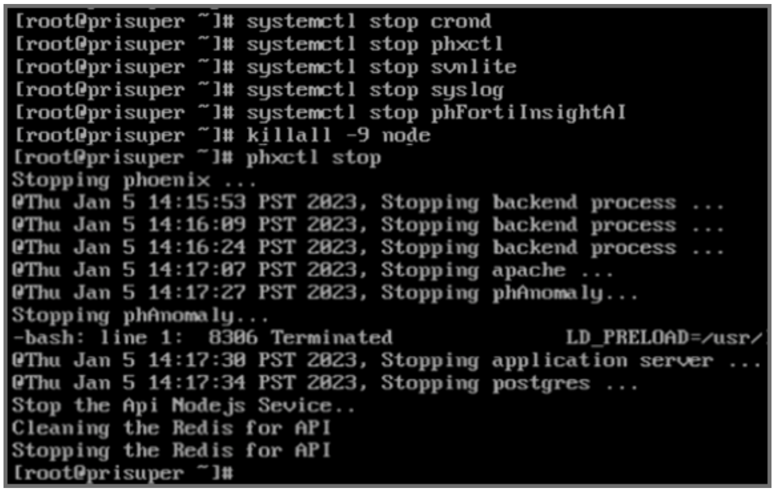
Create FortiSIEM VM Snapshot

Follow these steps to create snapshots for FortiSIEM nodes.

1. ssh into the supervisor node as root.
2. Run the following commands to stop all essential FortiSIEM services.

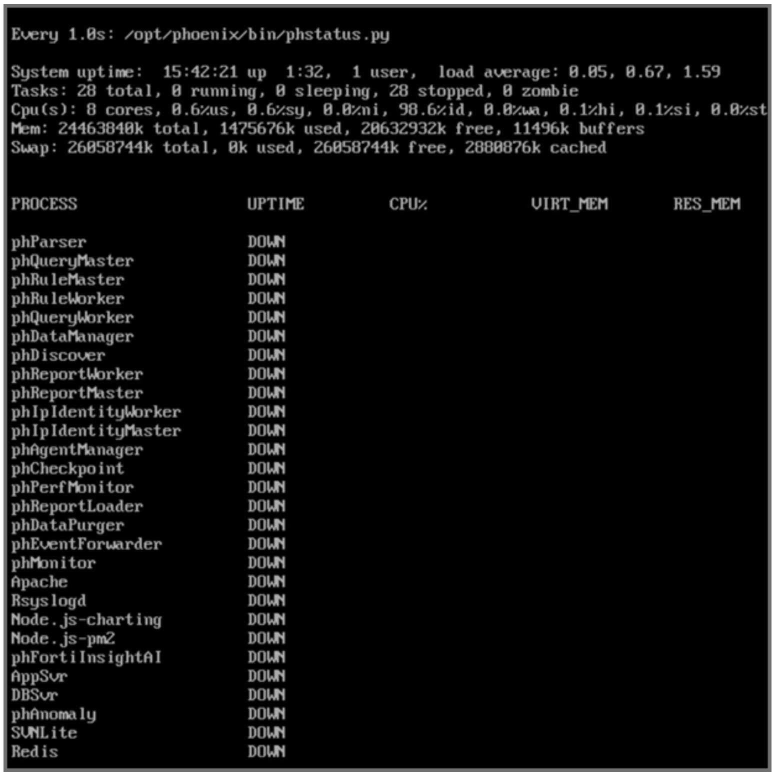
   ```
       # systemctl stop crond
       # systemctl stop phxctl
       # systemctl stop svnlite
       # systemctl stop syslog
       # systemctl stop phFortiInsightAI
   ```

```
# killall -9 node
# phxctl stop
```



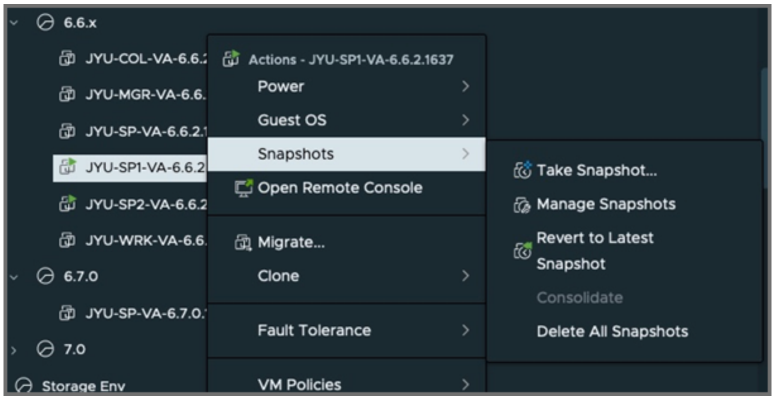
```
[root@prisuper ~]# systemctl stop crond
[root@prisuper ~]# systemctl stop phxctl
[root@prisuper ~]# systemctl stop svnlite
[root@prisuper ~]# systemctl stop syslog
[root@prisuper ~]# systemctl stop phFortiInsightAI
[root@prisuper ~]# killall -9 node
[root@prisuper ~]# phxctl stop
Stopping phoenix ...
@Thu Jan 5 14:15:53 PST 2023, Stopping backend process ...
@Thu Jan 5 14:16:09 PST 2023, Stopping backend process ...
@Thu Jan 5 14:16:24 PST 2023, Stopping backend process ...
@Thu Jan 5 14:17:07 PST 2023, Stopping apache ...
@Thu Jan 5 14:17:27 PST 2023, Stopping phAnomaly...
Stopping phAnomaly...
-bash: line 1:  8306 Terminated              LD_PRELOAD=/usr/
@Thu Jan 5 14:17:30 PST 2023, Stopping application server ...
@Thu Jan 5 14:17:34 PST 2023, Stopping postgres ...
Stop the Api Nodejs Sevice..
Cleaning the Redis for API
Stopping the Redis for API
[root@prisuper ~]#
```

3. Run `phstatus` and verify all services are down.

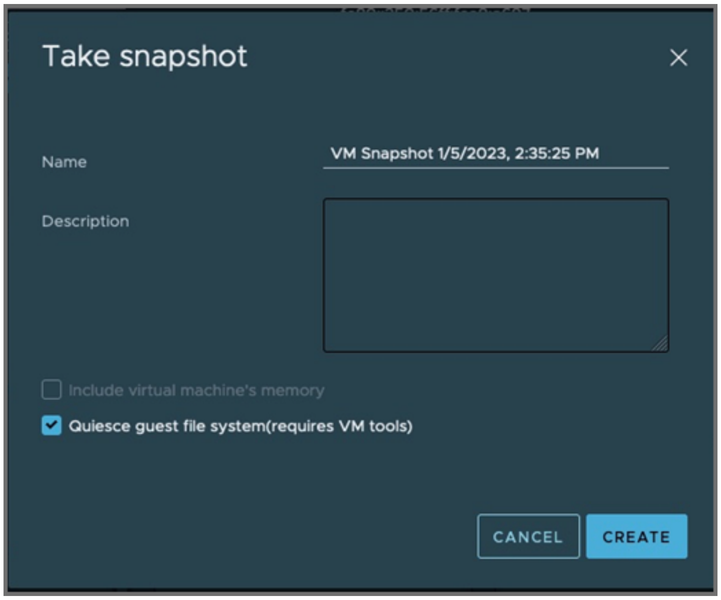


```
Every 1.0s: /opt/phoenix/bin/phstatus.py

System uptime:  15:42:21 up  1:32,  1 user,  load average: 0.05, 0.67, 1.59
Tasks: 28 total, 0 running, 0 sleeping, 28 stopped, 0 zombie
Cpu(s): 8 cores, 0.6%us, 0.6%sy, 0.0%ni, 98.6%id, 0.0%wa, 0.1%hi, 0.1%si, 0.0%st
Mem: 24463840k total, 1475676k used, 20632932k free, 11496k buffers
Swap: 26058744k total, 0k used, 26058744k free, 2880876k cached


PROCESS                  UPTIME         CPU%           VIRT_MEM       RES_MEM

phParser                 DOWN
phQueryMaster            DOWN
phRuleMaster             DOWN
phRuleWorker             DOWN
phQueryWorker            DOWN
phDataManager            DOWN
phDiscover               DOWN
phReportWorker           DOWN
phReportMaster           DOWN
phIpIdentityWorker       DOWN
phIpIdentityMaster       DOWN
phAgentManager           DOWN
phCheckpoint             DOWN
phPerfMonitor            DOWN
phReportLoader           DOWN
phDataPurger             DOWN
phEventForwarder         DOWN
phMonitor                DOWN
Apache                   DOWN
Rsyslogd                 DOWN
Node.js-charting         DOWN
Node.js-pm2              DOWN
phFortiInsightAI         DOWN
AppSvr                   DOWN
DBSvr                    DOWN
phAnomaly                DOWN
SVNLite                  DOWN
Redis                    DOWN
```

4. Find the FortiSIEM VM inside your hypervisor and click **Snapshots > Take Snapshot...**.



5. In the follow up dialog, take the following steps.
   a. Uncheck the **Include virtual machine’s memory** checkbox for a quick snapshot.
   b. Check the **Quiesce guest file system** checkbox to ensure filesystem integrity.
   c. Click **CREATE**.



Take snapshot

Name: VM Snapshot 1/5/2023, 2:35:25 PM

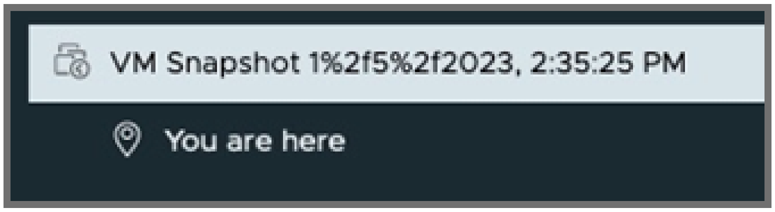
Description:

□ Include virtual machine's memory

☑ Quiesce guest file system(requires VM tools)

CANCEL CREATE

6. Check the Snapshot section of the VM in order to verify snapshot has been taken.

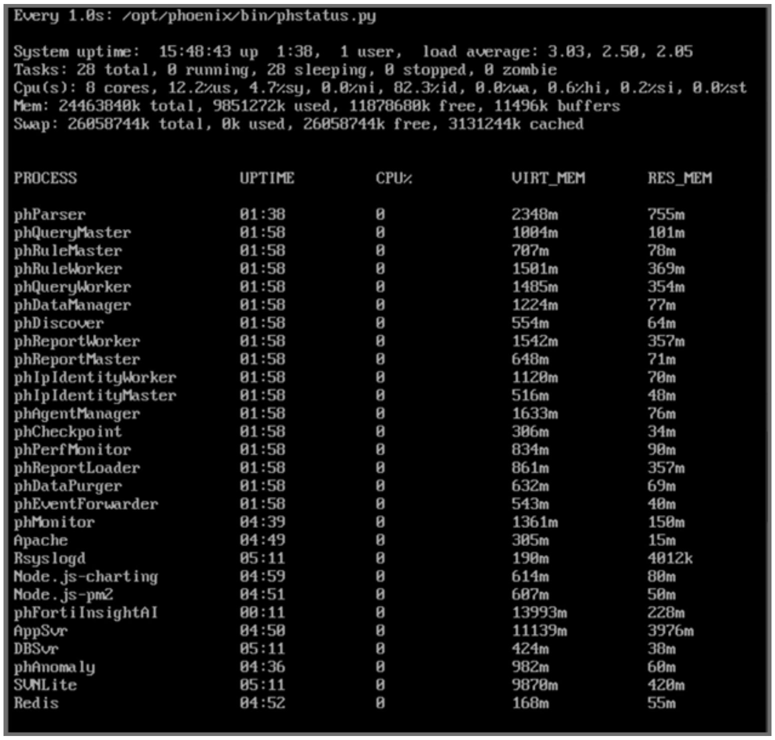


VM Snapshot 1%2f5%2f2023, 2:35:25 PM

You are here

7. Restart all FortiSIEM Services after the snapshot has been taken, by running the following commands.

```
# systemctl start crond
# systemctl start phxctl
# systemctl start svnlite
# systemctl start syslog
# systemctl start phFortiInsightAI
# phxctl start
# phstatus
```

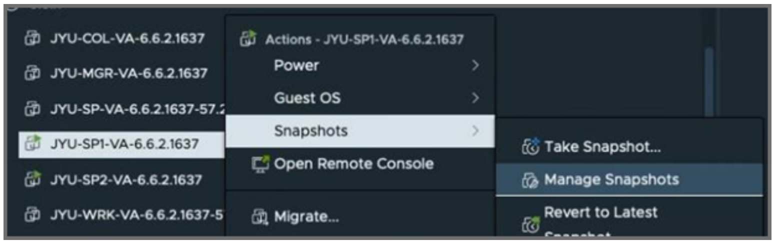


```
Every 1.0s: /opt/phoenix/bin/phstatus.py

System uptime:  15:48:43 up  1:38,  1 user,  load average: 3.03, 2.50, 2.05
Tasks: 28 total, 0 running, 28 sleeping, 0 stopped, 0 zombie
Cpu(s): 8 cores, 12.2%us, 4.7%sy, 0.0%ni, 82.3%id, 0.0%wa, 0.6%hi, 0.2%si, 0.0%st
Mem: 24463840k total, 9851272k used, 11878680k free, 11496k buffers
Swap: 26058744k total, 0k used, 26058744k free, 3131244k cached


PROCESS                 UPTIME         CPU%           VIRT_MEM       RES_MEM

phParser                01:38          0              2348m          755m
phQueryMaster           01:58          0              1004m          101m
phRuleMaster            01:58          0              707m           78m
phRuleWorker            01:58          0              1501m          369m
phQueryWorker           01:58          0              1485m          354m
phDataManager           01:58          0              1224m          77m
phDiscover              01:58          0              554m           64m
phReportWorker          01:58          0              1542m          357m
phReportMaster          01:58          0              648m           71m
phIpIdentityWorker      01:58          0              1120m          70m
phIpIdentityMaster      01:58          0              516m           48m
phAgentManager          01:58          0              1633m          76m
phCheckpoint            01:58          0              306m           34m
phPerfMonitor           01:58          0              834m           90m
phReportLoader          01:58          0              861m           357m
phDataPurger            01:58          0              632m           69m
phEventForwarder        01:58          0              543m           40m
phMonitor               04:39          0              1361m          150m
Apache                  04:49          0              305m           15m
Rsyslogd                05:11          0              190m           4012k
Node.js-charting        04:59          0              614m           80m
Node.js-pm2             04:51          0              607m           50m
phFortiInsightAI        00:11          0              13993m         228m
AppSvr                  04:50          0              11139m         3976m
DBSvr                   05:11          0              424m           38m
phAnomaly               04:36          0              982m           60m
SVNLite                 05:11          0              9870m          420m
Redis                   04:52          0              168m           55m
```

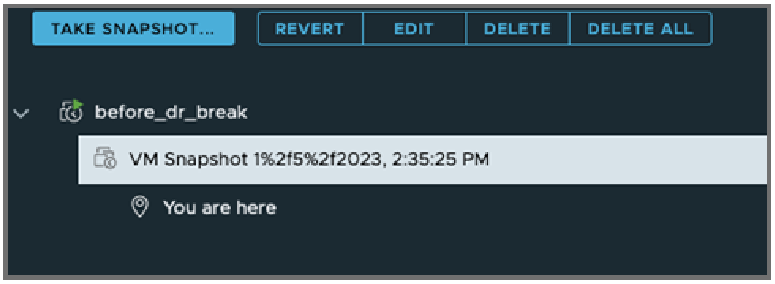
Restoring FortiSIEM VM from Snapshot

Take the following steps to restore a VM from a snapshot.

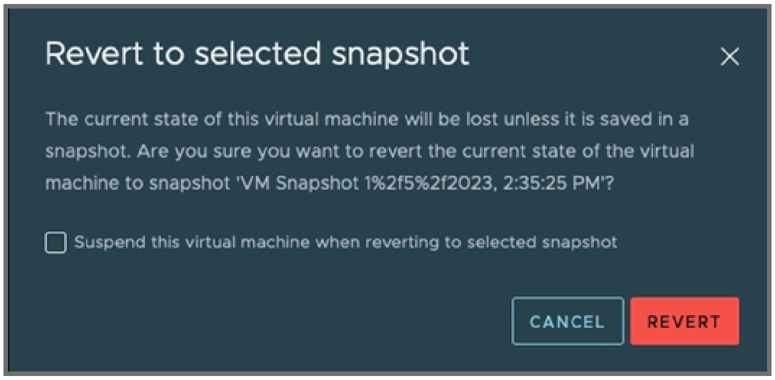
1. Find the currently running VM in vSphere, right click on the **VM**, and navigate to **Snapshots > Manage Snapshots**.



2. Select the snapshot in the list that you want to restore, and select **REVERT**.



3. On the pop-up window, select **REVERT**.

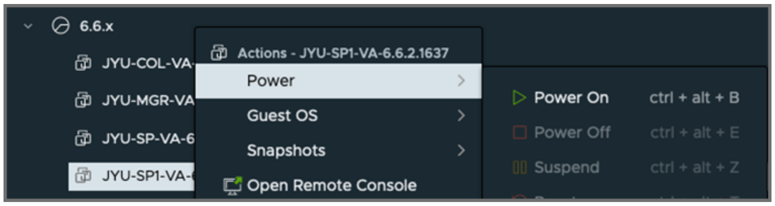


Revert to selected snapshot

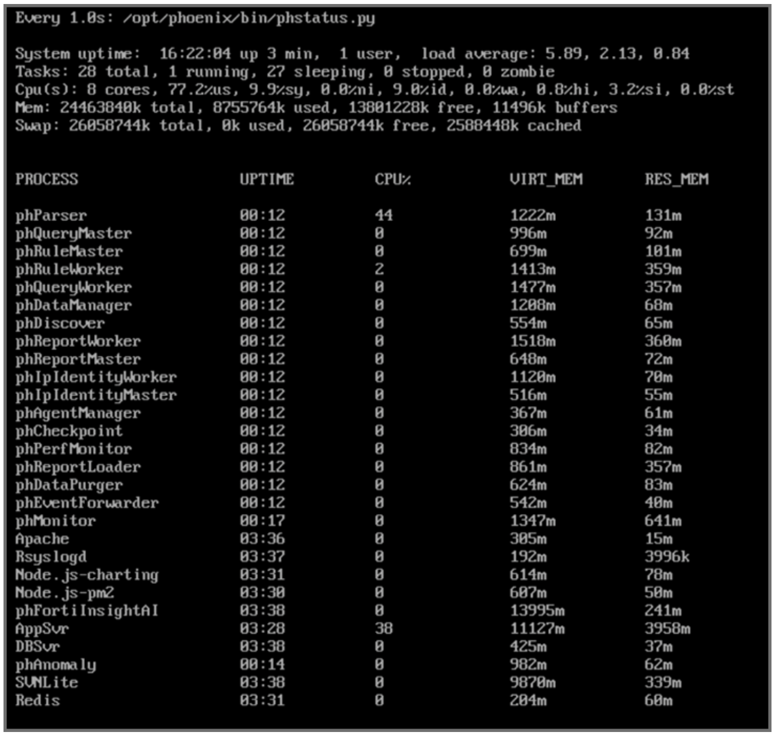
The current state of this virtual machine will be lost unless it is saved in a snapshot. Are you sure you want to revert the current state of the virtual machine to snapshot 'VM Snapshot 1%2f5%2f2023, 2:35:25 PM'?

□ Suspend this virtual machine when reverting to selected snapshot

4. The VM will be reverted to the selected snapshot and be left turned off. Right click the **VM**, and navigate to **Power > Power On**.



This will turn the VM on from the point of the snapshot and services will start up as normal.



```
Every 1.0s: /opt/phoenix/bin/phstatus.py

System uptime:  16:22:04 up 3 min,  1 user,  load average: 5.89, 2.13, 0.84
Tasks: 28 total, 1 running, 27 sleeping, 0 stopped, 0 zombie
Cpu(s): 8 cores, 77.2%us, 9.9%sy, 0.0%ni, 9.0%id, 0.0%wa, 0.8%hi, 3.2%si, 0.0%st
Mem: 24463840k total, 8755764k used, 13801228k free, 11496k buffers
Swap: 26058744k total, 0k used, 26058744k free, 2588448k cached


PROCESS                  UPTIME         CPU%           VIRT_MEM       RES_MEM

phParser                 00:12          44             1222m          131m
phQueryMaster            00:12          0              996m           92m
phRuleMaster             00:12          0              699m           101m
phRuleWorker             00:12          2              1413m          359m
phQueryWorker            00:12          0              1477m          357m
phDataManager            00:12          0              1208m          68m
phDiscover               00:12          0              554m           65m
phReportWorker           00:12          0              1518m          360m
phReportMaster           00:12          0              648m           72m
phIpIdentityWorker       00:12          0              1120m          70m
phIpIdentityMaster       00:12          0              516m           55m
phAgentManager           00:12          0              367m           61m
phCheckpoint             00:12          0              306m           34m
phPerfMonitor            00:12          0              834m           82m
phReportLoader           00:12          0              861m           357m
phDataPurger             00:12          0              624m           83m
phEventForwarder         00:12          0              542m           40m
phMonitor                00:17          0              1347m          641m
Apache                   03:36          0              305m           15m
Rsyslogd                 03:37          0              192m           3996k
Node.js-charting         03:31          0              614m           78m
Node.js-pm2              03:30          0              607m           50m
phFortiInsightAI         03:38          0              13995m         241m
AppSvr                   03:28          38             11127m         3958m
DBSvr                    03:38          0              425m           37m
phAnomaly                00:14          0              982m           62m
SVNLite                  03:38          0              9870m          339m
Redis                    03:31          0              204m           60m
```

Exporting Events from FortiSIEM

The following tools are provided:

- phExportESEvent Tool
- phExportEvent Tool
- TestESSplitter Tool
- phClickHouseCSVExport Tool

phExportESEvent Tool

Description: This tool exports events from Elasticsearch into a CSV file.

Usage: `phExportESEvent` *<ESUrl> <ESPort> <ESDeploymentType>* "*<ESUser>*" "*<ESPassword>*" *<ESIndexName> <ReportingDevIp> <destDir> <splitThreads> <LogLevel>*

Argument	Description
`ESUrl`	The Elasticsearch URL. Example, http://192.0.2.0.
`ESPort`	The Elasticsearch coordinating node port, e.g. 9200.
`ESType`	Provide the Elasticsearch type. 1: Native 2: AWS Elasticsearch Service 3: Elasticsearch Cloud
`ESUser`	Provide the Elasticsearch username. "" means no username.
`ESPassword`	Provide the Elasticsearch password. "" means no password.
`ESIndexName`	The name of the Elasticsearch index to be exported, for example, `fortisiem-event-2020.06.17-1`.
`ReportDevIp`	The IP address of the report device to be used to select events to export. "" means select all devices.
`destDir`	The export directory: `output_dir`.
`splitThreads`	The number of threads to be used for export, e.g., 10.
`logDevel`	The debug level for script output printing: `INFO` or `DEBUG`.

Notes:

1. Can be run from Supervisor or Worker.
2. Can be run as admin user.

Examples:

Native Elasticsearch Deployment Example

```
phExportESEvent https://192.0.2.0 9200 1 "Joe.123--test" "password" fortisiem-event-2021.08.05-1-000001 "192.0.2.4" /archive/ 10 INFO
```

AWS Elasticsearch Service Deployment Example

```
phExportESEvent https://search-eesna78-aaaa4ysukru3ui4ayaz2yya3km.us-east-1.es-
.amazonaws.com 443 2 "key" "secret" fortisiem-event-2021.09.29-1 "" /archive/ 10 INFO
```

Elasticsearch Cloud Deployment Example

```
phExportESEvent https://cpaagg33-d11e01.es.us-central1.gcp.cloud.es.io 9243 3
"elastic" "password" fortisiem-event-2021.10.01-1-000001 "" /archive/ 10 INFO
```

phExportEvent Tool

Description: This tool exports events from EventDB into a CSV file. The CSV file contains the following columns:

- Customer Id (applicable to SP license)
- Reporting Device IP
- Reporting Device Name
- Event Received Time
- Raw Message

Usage: `phExportEvent {--dest DESTINATION_DIR} {--starttime START_TIME | --relstarttime RELATIVE_START_TIME} {--endtime END_TIME | --relendtime RELATIVE_END_TIME} [--dev DEVICE_NAME] [--org ORGANIZATION_NAME] [-t TIME_ZONE]`

Argument	Description
`DESTINATION_DIR`	Destination directory where the exported event files are saved.
`START_TIME`	Starting time of events to be exported. The format is YYYY-MM-DD HH:MM:SS {+|-} TZ. If TZ is not given, the local time zone of the machine where the script is running will be used. Example: `2010-03-10 23:00:00 -8` means Pacific Standard Time, 23:00:00 03/10/2010. `2010-07-29 10:20:00 +5:30` means India Standard Time 10:20:00 07/29/2010.
`RELATIVE_ START_TIME`	This must be used together with `END_TIME`. Starting time of events to be exported is relative backwards to the end time, specified using `--endtime END_TIME`. The format is `{NUM}{d|h|m}` where `NUM` is the number of days or hours or minutes. For example, `-- rel-starttime 5d` means the starting time is 5 days prior to the ending time.
`END_TIME`	Ending time of events to be exported. The format is the same as described for `START_TIME`.
`RELATIVE_END_ TIME`	This must be used together with `START_TIME`. Ending time of events to be exported is relative forward to the start time, specified using `START_TIME`. The format is the same that is used for RELATIVE_START_TIME.
`DEVICE_NAME`	Provide the host name or IP address of the device with the events to be exported. Use a comma-separated list to specify multiple IPs or host names, for example, `--`

Argument	Description
	`dev 10.1.1.1,10.10.10.1,router1,router2`. Host name is case insensitive.
`ORGANIZATION_ NAME`	This is used only for Service Provider deployments. Provide the name of the organization with the events to be exported. To specify multiple organizations, enter a command for each organization, for example, `--org "Public Bank" --org "Private Bank"`. The organization name is case insensitive.
`TIME_ZONE`	Specifies the time zone used to format the event received time in the exported event files. The format is `{+|-}TZ`, for example, `-8` means Pacific Standard Time, `+5:30` means India Standard Time.

Notes:

1. Can be run from Supervisor or Worker.
2. Can be run as admin user.

TestESSplitter Tool

Description: This tool exports events from ElasticSearch to a directory in FortiSIEM EventDB format.

Usage: `TestESSplitter` *`<ESBroker> <ESPort> <ESClusterType> <ESUser> <ESPassword> <IndexName> <destDir> <splitThreads> <logLevel>`*

Argument	Description
`ESBroker`	The IP of ElasticSearch Co-ordinator node.
`ESPort`	The port used for ElasticSearch.
`ESClusterType`	The ElasticSearch Cluster type. Values are "1" for Native, "2" for Amazon OpenSearch Service (previously known as Amazon Elasticsearch Service), and "3" for Elastic Cloud.
`ESUser`	The ElasticSearch username for authentication.
`ESPassword`	The ElasticSearch password for authentication.
`IndexName`	Provide an Index name. A new Index is created per day. Here is an example index name, `fortisiem-event-2021.05.14-2000-000001` where“fortisiem-event-2021.05.14” is the day and “2000” is the Organization ID. To find a list of indexes, run this command: `curl -XGET '10.10.2.5:9200/_cat/shards?v'` replacing `10.10.2.5` with the IP of a Co-ordinator node.
`destDir`	Destination directory where the exported events are saved in FortiSIEM eventDB format.

Argument	Description
	Note: A trailing slash is mandatory. Example: `https://<destDir>/`.
`splitThreads`	Number of threads.
`logLevel`	INFO or DEBUG level log messages.

Notes:

1. Can be run from Supervisor or Worker.
2. Can be run as admin user.
3. This tool is located in `/opt/phoenix/bin/`.

Example:

```
[root@fsm]# /opt/phoenix/bin/TestESSplitter 10.10.2.5 "" "" fortisiem-event-
2021.05.14-2000-000001 /root/output 10 INFO

[PH_MODULE_LOG_LEVEL_CHANGE]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=phBaseProcess.cpp,[lineNumber]=675,[oldLogLevel]=2047,[newLogLevel]=424,[phLo-
gDetail]=Module received log level change
[PH_MODULE_LOCAL_CONFIG_LOADED]:[eventSeverity]=LM_INFO,[procName]=<unknown>,
[fileName]=phConfigLoader.cpp,[lineNumber]=166,[configName]=global,[phLo-
gDetail]=Module loaded local config successfully
[PH_MODULE_LOCAL_CONFIG_LOADED]:[eventSeverity]=LM_INFO,[procName]=<unknown>,
[fileName]=phConfigLoader.cpp,[lineNumber]=166,[configName]=phdatamanager,[phLo-
gDetail]=Module loaded local config successfully
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=phHttpClientPool.cpp,[lineNumber]=46,[phLogDetail]=phHttpClientPool: init host-
s/port/auth/header=10.10.2.5/9200/:****/Content-Type: application/json
*   Trying 10.10.2.5...
* TCP_NODELAY set
* Connected to 10.10.2.5 (10.10.2.5) port 9200 (#0)
> GET / HTTP/1.1
Host: 10.10.2.5:9200
Accept: */*
Content-Type: application/json

< HTTP/1.1 200 OK
< content-type: application/json; charset=UTF-8
< content-length: 530
<
* Connection #0 to host 10.10.2.5 left intact
```

```
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=EventLoader.cpp,[lineNumber]=1732,[phLogDetail]=Elastic init success:
http://10.10.2.5:9200/
* Found bundle for host 10.10.2.5: 0x18f0870 [can pipeline]
* Re-using existing connection! (#0) with host 10.10.2.5
* Connected to 10.10.2.5 (10.10.2.5) port 9200 (#0)
> GET /_cat/indices/fortisiem-event-2021.05.14-2000-000001?h=pri,rep,docs.count
HTTP/1.1
Host: 10.10.2.5:9200
Accept: */*
Content-Type: application/json
…
…
…
…

<
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=EventLoader.cpp,[lineNumber]=1974,[phLogDetail]=Elastic succeed hits total 66 for
index fortisiem-event-2021.05.14-2000-000001 slice 1 max 10
* Connection #0 to host 10.10.2.5 left intact
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=EventLoader.cpp,[lineNumber]=1974,[phLogDetail]=Elastic succeed hits total 61 for
index fortisiem-event-2021.05.14-2000-000001 slice 8 max 10
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=EventLoader.cpp,[lineNumber]=2002,[phLogDetail]=Elastic index query completed 0
seconds
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=EventLoader.cpp,[lineNumber]=2002,[phLogDetail]=Elastic index query completed 0
seconds
< HTTP/1.1 200 OK
< content-type: application/json; charset=UTF-8
< content-length: 47737
<
* Connection #0 to host 10.10.2.5 left intact
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=EventLoader.cpp,[lineNumber]=1974,[phLogDetail]=Elastic succeed hits total 53 for
index fortisiem-event-2021.05.14-2000-000001 slice 3 max 10
< HTTP/1.1 200 OK
< content-type: application/json; charset=UTF-8
< content-length: 47178
<
* Connection #0 to host 10.10.2.5 left intact
< HTTP/1.1 200 OK
< content-type: application/json; charset=UTF-8
< content-length: 41910
<
* Connection #0 to host 10.10.2.5 left intact
< HTTP/1.1 200 OK
< content-type: application/json; charset=UTF-8
< content-length: 53258
<
* Connection #0 to host 10.10.2.5 left intact
< HTTP/1.1 200 OK
< content-type: application/json; charset=UTF-8
< content-length: 60587
<
* Connection #0 to host 10.10.2.5 left intact
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=EventLoader.cpp,[lineNumber]=1974,[phLogDetail]=Elastic succeed hits total 59 for
index fortisiem-event-2021.05.14-2000-000001 slice 4 max 10
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=EventLoader.cpp,[lineNumber]=1974,[phLogDetail]=Elastic succeed hits total 53 for
index fortisiem-event-2021.05.14-2000-000001 slice 7 max 10
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=EventLoader.cpp,[lineNumber]=1974,[phLogDetail]=Elastic succeed hits total 68 for
index fortisiem-event-2021.05.14-2000-000001 slice 6 max 10
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=EventLoader.cpp,[lineNumber]=1974,[phLogDetail]=Elastic succeed hits total 46 for
index fortisiem-event-2021.05.14-2000-000001 slice 2 max 10
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=EventLoader.cpp,[lineNumber]=2002,[phLogDetail]=Elastic index query completed 0
seconds
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=EventLoader.cpp,[lineNumber]=2002,[phLogDetail]=Elastic index query completed 0
seconds
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=EventLoader.cpp,[lineNumber]=2002,[phLogDetail]=Elastic index query completed 0
seconds
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,
[fileName]=EventLoader.cpp,[lineNumber]=2002,[phLogDetail]=Elastic index query com-
pleted 0 seconds
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=EventLoader.cpp,[lineNumber]=2002,[phLogDetail]=Elastic index query completed 0
seconds
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]-
]=TestESSplitter.cpp,[lineNumber]=82,[phLogDetail]=Events processed for split: 559
3.15
```

The result will be eventDB structured directories and files.

```
[root@fsm]# ls -l /root/output/
total 0
drwx------ 3 root root 22 May 14 15:25 CUSTOMER_2000
[root@fsm]# ls -l /root/output/CUSTOMER_2000/
total 0
drwx------ 3 root root 19 May 14 15:25 internal
[root@fsm]# ls -l /root/output/CUSTOMER_2000/internal/
total 0
drwx------ 3 root root 37 May 14 15:25 18761
[root@fsm]# ls -l /root/output/CUSTOMER_2000/internal/18761/
total 4
drwx------ 12 root root 4096 May 14 15:25 450264-450287-168428094
[root@fsm]# ls -l /root/output/CUSTOMER_2000/internal/18761/450264-450287-168428094/
total 0
drwx------ 3 root root 18 May 14 15:25 seg-1-0-48-1620951010-1620971132
drwx------ 3 root root 18 May 14 15:25 seg-1-1-70-1620950470-1620971172
drwx------ 3 root root 18 May 14 15:25 seg-1-2-35-1620950916-1620971172
drwx------ 3 root root 18 May 14 15:25 seg-1-3-66-1620951819-1620969371
drwx------ 3 root root 18 May 14 15:25 seg-1-4-61-1620950830-1620970642
drwx------ 3 root root 18 May 14 15:25 seg-1-5-59-1620950830-1620971132
drwx------ 3 root root 18 May 14 15:25 seg-1-6-53-1620950482-1620970632
drwx------ 3 root root 18 May 14 15:25 seg-1-7-46-1620951278-1620971182
drwx------ 3 root root 18 May 14 15:25 seg-1-8-53-1620950470-1620970452
drwx------ 3 root root 18 May 14 15:25 seg-1-9-68-1620950650-1620971132
```

phClickHouseCSVExport Tool

Description: This tool exports events from ClickHouse into a CSV file. The file will contain these fields:

- Event Receive Time
- Reporting IP

- Event Type
- Raw Event Log.

Usage: `phClickHouseCSVExport --starttime [Start Time] --endtime [End Time] --outfile [Output file] --deviceip [Reporting Device IP Address] --devicename [Reporting Device Name] --orgid [Organization ID (0 - 4294967295)] --orgname [Organization Name] --eventtype [Event Type]`

Argument	Description
`--starttime [Start Time]`	Starting time of events to be exported. It must be in the following format: "YYYY-MM-DD hh:mm:ss". The supported time zone is GMT. Make sure to enclose the Start Time with quotation marks. Example: `phClickHouseCSVExport --outfile /home/user-/report.csv --starttime "2022-01-20 10:10:00" --endtime "2022-01-20 11:10:00"`
`--endtime [End Time]`	The end time of events to be exported. It must be in the following format: "YYYY-MM-DD hh:mm:ss". The supported time zone is GMT. Make sure to enclose the End Time with quotation marks. Example: `phClickHouseCSVExport --outfile /home/user-/report.csv --starttime "2022-01-20 10:10:00" --endtime "2022-01-20 11:10:00"`
`--outfile [Output file]`	The output file where the exported events are saved in FortiSIEM, CSV format.
`--deviceip [Reporting Device IP Address]`	Provide the IP address of the device with the events to be exported. Only one reporting device IP address is supported. For example, `--deviceip 10.1.1.1`.
`--devicename [Reporting Device Name]`	Provide the host name of the device with the events to be exported. For example, `--devicename router1`. Host name is case insensitive.
`--orgid [Organization ID]`	Provide the ID of the organization with the events to be exported. The number can be from 0 to 4294967295.
`--orgname [Organization Name]`	This is used only for Service Provider deployments. Provide the name of the organization with the events to be exported. To specify multiple organizations, enter a command for each organization, for example, `--org "Public Bank" --orgname "Private Bank"`. The organization name is case insensitive.
`--eventtype [Event Type]`	Specify the event types to be exported.

Notes:

1. Can be run from Supervisor or Worker.
2. Can be run as admin user.

Importing Events into FortiSIEM

The following tools are provided:

- phClickHouseImport Tool

phClickHouseImport Tool

Description: This tool is used to migrate EventDB data into your ClickHouse database.

Usage: `phClickHouseImport --src [Source Dir] --srcorgid [Organization ID] --dstorgid [Organization ID] --starttime [Start Time] --endtime [End Time] --host [IP Address of the ClickHouse Server that the data will be imported to] --orgid [Organization ID]`

Argument	Description
`--src [Source Dir]`	Provide the source directory that contains the eventDB data. The default path is `/data/eventdb/CUSTOMER_1/default` If a path is provided, the data path will be created as: *<user input path>* + “`/CUSTOMER_1/default`” Example: If `--src /test` is used, the data path will be created as `/test/CUSTOMER_1/default`
`--starttime [Start Time]`	Starting time of events to be imported. It must be in the following format: "YYYY-MM-DD hh:mm:ss". The supported time zone is GMT. Make sure to enclose the Start Time with quotation marks. Example: `phClickHouseImport --src /data/eventdb --starttime "2022-01-27 10:10:00" --endtime "2022-02-01 11:10:00"`
`--endtime [End Time]`	The end time of events to be imported. It must be in the following format: "YYYY-MM-DD hh:mm:ss". The supported time zone is GMT. Make sure to enclose the End Time with quotation marks. Example: `phClickHouseImport --src /data/eventdb --starttime "2022-01-27 10:10:00" --endtime "2022-02-01 11:10:00"`
`--host [IP Address of the ClickHouse Server that the data will be imported to]`	The IP address of the ClickHouse server that the data will be imported to. If the host IP address is not provided, then localhost is used. The default IP address is 127.0.0.1.
`--orgid [Organization ID]`	Provide the ID of the organization with the events to be imported. The number can be from 0 to 4294967295. Multiple entries are allowed by adding `--orgid [Organization ID]` for each entry. Only matched orgid will be migrated. Example: `phClickHouseImport --src /data/eventdb --starttime "2022-01-01 23:00:00" --endtime "2022-02-01 10:00:00" --orgid 1 --orgid 2001 --host 192.0.20.0`

Argument	Description
`--srcorgid [Organization ID] --dstorgid [Organization ID]`	The `--srcorgid` is the organization ID that data will be imported from and the `--dstorgid` is the target organization ID that the data will be imported into ClickHouse. Example: `phClickHouseImport --src /data/eventdb/ --starttime "2022-01-27 10:10:00" --endtime "2022-02-01 11:10:00" --srcorgid 2005 --dstorgid 2008 --host 192.0.20.0`

Notes:

1. Can be run from Supervisor or Worker.
2. Can be run as admin user.
3. `phClickHouseImport` tool requires FortiSIEM 6.5.0 or higher.
4. EventDB data needs to be copied to the machine where this tool can run.

Example:

```
phClickHouseImport --src /data/eventdb --starttime "2022-01-01 23:00:00" --endtime
"2022-02-01 10:00:00" --orgid 1 --orgid 2001 --host 192.0.20.0
```

Increasing Collector Event Buffer Size

Collectors can buffer events in case events cannot be uploaded fast enough to Worker(s) or Supervisor nodes or they are unavailable for a period of time. Events are stored in compressed format in the following location `/opt/phoenix/cache/parser/events` before being sent to Worker(s) or Supervisor nodes. By default, a maximum of 10K files are stored and each file has a maximum uncompressed file size of 10MB.

When the number of files reaches the limit, events are dropped by the Collector. To change this limit, modify the following line in `/opt/phoenix/config/phoenix_config.txt`.

```
[BEGIN phEventPackager]
```

```
max_num_event_files=10000
```

In case your Collectors are forwarding events to a 3rd party server, there is a similar limit of 10K files of events stored in `/opt/phoenix/cache/parser/fwd`. When this limit is reached, newer events are not forwarded. To change this limit, modify the following line in `/opt/phoenix/config/phoenix_config.txt`.

```
[BEGIN phEventForwarder]
```

```
max_num_fwd_files=10000
```

Note: You may need to increase the size of `/opt` disk if you significantly increase the number of files stored. For configuration information on how to increase your `/opt` disk size, see Collector with Different OPT Disk Sizes in the ESX Install Guide.

Listing Event Attributes seen by Elasticsearch

The following tools are provided:

- listElasticEventAttributes.sh Tool

listElasticEventAttributes.sh Tool

Description: This tool gathers Elasticsearch event attributes for the number of days specified with the `days` value into a CSV file that can be used to prepare a custom Elastic Search Event Attribute Template file. This file can be uploaded to replace the default Event Attribute template, potentially reducing the number of Event Attributes that Elasticsearch needs to search by default. For information on where to upload the custom file, see Configuring Elasticsearch Based Deployments.

Usage: `[root@FortiSIEM]#listElasticEventAtributes.sh` *`destURL httpPort(9200)`* `[`*`user passwd`*`]` *`dayssocketTimeoutInMinuteoutputFile`*

Argument	Description
`destURL`	The destination URL, normally the Elasticsearch URL.
`httpPort`	The port number used to connect to Elasticsearch.
`user`	Use your login username to access Elasticsearch.
`password`	Use your password associated with the username to access Elasticsearch
`days`	The number of days you want this custom configuration to be applied, starting when the custom template is added to your Elasticsearch Based Deployment.
`socketTimeoutInMinute`	The maximum time out period value in minutes for the socket .
`outputFile`	The name you wish to name your output file.

Notes:

1. You can change an Event Attribute type per your requirements if the default type is not suitable, but you will need to upload the custom Event Attribute template afterward.
2. This tool is located in `/opt/phoenix/config/javaQueryServer/`.

Example:

```
 [root@FortiSIEM javaQueryServer# ./listElasticEventAttributes.sh
https://172.30.56.180 9200 "username" "password" 3 10 /tmp/1.csv
```

Managing Events in EventDB

- TestDBPurger Tool
- EnforceRetentionPolicy Tool
- TestSegment Reader Tool

TestDBPurger Tool

Description: This tool is used to delete data for a single date.

Usage: `TestDBPurger {`*`EVENTDB`*`} {`*`DEST`*`} {`*`MODE`*`} {`*`CUSTID`*`} {`*`DATES`*`}`

Argument	Description
`EVENTDB`	The eventDB directory, for example: /data/eventdb.

Argument	Description
DEST	The directory to retain output data.
MODE	Control where to put processed (purged) data. 0 - Output the processed DB to destDir. It is possible to copy it back to eventDB manually. 1 - Output the processed DB to eventDB to make it effect for query. Move original data to destDir.
CUSTID	Customer ID for the organization to be purged.
DATES	Comma separated list of dates or date-range to process. A date is specified as the number of days since the UNIX epoch, 1970-01-01. A date-range is range specified by two dates inclusively separated by '-'. Use the following Linux command to generate a epoch date (**Note**: Replace *MM/DD/YYYY* with actual date): echo $(($(date --utc --date="*MM/DD/YYYY*" +%s)/86400))

Notes:

1. You should only use this script to delete data for a single date and organization. If you try to delete data for multiple dates, the script may fail.
2. The script is located at `/opt/phoenix/bin/TestDBPurger`. Run it in terminal mode and follow the instructions.
3. Should be run as admin user.
4. Make sure enough space is available for the directory holding the output data (/tmp/eventdb in the example) which is actually a backup of events and can be deleted later if not needed.

Example:

```
TestDBPurger /data/eventdb /tmp/eventdb 1 2000 16230,16233-16235
```

EnforceRetentionPolicy Tool

Description: This tool can be used to enforce retention policy on dates earlier than the retention policy normally covers.

Usage: `EnforceRetentionPolicy {`*`DATES`*`}`

Argument	Description
DATES	Comma separated list of dates or date-range on which to enforce retention policy. DATES is specified as the number of days since the UNIX epoch began, 1970-01-01. A date-range can be specified by two dates inclusively separated by '-'. Use the following Linux command to generate a epoch date (**Note**: Replace *MM/DD/YYYY* with actual date): echo $(($(date --utc --date="*MM/DD/YYYY*" +%s)/86400))

Notes:

1. Run the tool as admin user.

Example:

```
EnforceRetentionPolicy 16230,16233-16235
```

This example command enforces retention policies on these dates: 6/8/2014 and from 6/11/2014 to 6/13/2014.

TestSegmentReader Tool

Description: This tool is used to quickly read data segments in the eventDB through the command line. You can use this to manually inspect data integrity and parsed event attributes.

Usage: `TestSegmentReader {segmentDir}`

Argument	Description
segmentDir	The segment directory.

Notes:

1. Run the tool as admin user.

Example:

```
TestSegmentReader /archive/CUSTOMER_3/default/17897/429628-423551-172384880/seg-1-0-
300000-1545300800-1543305001/
```

Managing FortiSIEM Operations

The following tools are provided:

- phstatus Tool
- phtools Tool

phstatus Tool

Description: This tool is used to check the status of services on FortiSIEM. It lists the status of services running in FortiSIEM

Usage: `phstatus`

Notes:

1. Run the tool as admin user.
2. Run `phstatus -a` from the root account, and it shows the detailed status of all FortiSIEM processes along with events per second and local I/O rates.

phtools Tool

Description: This tool allows you to start and stop backend processes, and also lets you get change log information. When you upgrade your deployment, for example, you would use phTools to stop all backend processes.

Usage:`phtools {--changelog ([ALL | ERROR | TRACE | INFO | DEBUG | CRITICAL]) | --start {[ALL | <PROCESS>]}| --stop {[ALL | <PROCESS>]}| --stats (ALL | <PROCESS>)}`

Argument	Description
`--changelog`	Use ERROR, TRACE, INFO, DEBUG, or CRITICAL to get specific change log information.
`--start`	Start a specific process, or start all processes.
`--stop`	Stop a specific process, or stop all processes.
`--stats`	Get statistics for a specific process or for all processes.
PROCESS	The name of the FortiSIEM process. Examples: `phDataPurger`, `phDiscover`, `phMonitor`, `phParser`.

Notes:

1. Run the tool as admin user.

Examples:

```
phtools --start all
```

```
phtools --stop all
```

```
phtools --start phDataPurger
```

```
phtools --stop phDataPurger
```

ClickHouse Usage Notes

ClickHouse Index Design

ClickHouse uses Primary indices and Data Skipping indices to speed up queries. See the following links for more information:

Primary Index: https://clickhouse.com/docs/en/optimize/sparse-primary-indexes

Data Skipping Index: https://clickhouse.com/docs/en/optimize/skipping-indexes

Other helpful links:

https://clickhouse.com/docs/en/concepts/why-clickhouse-is-so-fast

In ClickHouse, the following event attributes are configured as Primary and data Skipping indices.

Primary Indices:

- phCustId (Organization ID)
- eventType (Event Type)

Data Skipping Indices:

- reptDevIpAddr (Reporting IP)
- reptDevName (Reporting Device Name)
- customer (Organization Name)
- eventId (Event ID)
- phEventCategory (System Event Category)
- collectorId (Collector ID)
- srcIpAddr (Source Ip Address)
- destIpAddr (Destination Ip Address)
- destIpPort (Destination TCP/UDP Port)
- user (User)
- hostIpAddr (Host Ip Address)
- hostName (Host Name)
- fileName (File Name)
- procName (Process Name)
- appName (Application Name)

ClickHouse Operational Overview

The following ClickHouse background topics are available.

- Shards and Replicas
- ClickHouse Related Processes
- Supervisor/Worker Nodes Running ClickHouse Functions
- ClickHouse Keeper Cluster Considerations
- Event Insertion Flow
- Event Replication Flow
- Query Flow

Shards and Replicas

A shard is a database partition designed to provide high insertion and query rates. Events are written to and read from multiple shards in parallel. You need to choose the number of shards based on your incoming EPS (see example below and the latest ClickHouse Sizing Guide located in Fortinet Documents Library here).

If you want replication, then you can have replicas within each shard. ClickHouse will replicate database writes to a node within a shard to all other replicas within the same shard. A typical choice for replication size = 2, implying that you will have 2 nodes in each shard. A replica provides (a) faster queries and (b) prevents data loss in case a node goes down.

It is important to understand how ClickHouse insertion, Replication and Query works in FortiSIEM.

ClickHouse Related Processes

ClickHouse is a distributed database with replication capabilities. FortiSIEM Supervisor and Worker software images include ClickHouse binaries. The user does not need to install anything else. You can configure a ClickHouse cluster from the FortiSIEM GUI.

There are two main ClickHouse processes:

- `ClickHouseServer` process: This is the ClickHouse Database Service.
- `ClickHouseKeeper` process: This is the ClickHouse Keeper Service providing Replication Management.

In addition, two more FortiSIEM processes provide ClickHouse related services:

- `phClickHouseMonitor` process: This runs on the Supervisor and Worker nodes and provides the following services:
  - On Supervisor/Worker nodes: CMDB Group Query helper, Lookup Table Query helper and DeviceToCMDBAttr Query helper.
  - On Supervisor node only: Provides Online data display and the list of available ClickHouse nodes.
- `phMonitor` process: Provides ClickHouse configuration management on Supervisor node.

Supervisor/Worker Nodes Running ClickHouse Functions

A FortiSIEM Supervisor/Worker node can be of 3 types (not mutually exclusive):

- ClickHouse Keeper Node: This node runs ClickHouse Keeper service providing replication management.
- ClickHouse Data Node: This node inserts events into ClickHouse database.
- ClickHouse Query Node: This node provides ClickHouse query services.

FortiSIEM Supervisor/Worker node can be a specific node only, or a mix of the 3 node types. For example:

Small EPS Environments: One Supervisor node that is a Keeper, Data and Query node

Medium EPS Environments:

- Supervisor node as ClickHouse Keeper Node. Note that 2 additional Keeper nodes are recommended (see ClickHouse Keeper Cluster Considerations).

High EPS Environments (Option 1):

- Supervisor node does not run any ClickHouse service
- 3 separate Worker nodes as ClickHouse Keeper Nodes - these form the ClickHouse Keeper cluster (see ClickHouse Keeper Cluster Considerations).
- N Worker nodes, with each node acting as both ClickHouse Data Node and ClickHouse Query Node - these form the ClickHouse Database cluster.

High EPS environments (Option 2):

- Supervisor node does not run any ClickHouse service
- 3 separate Worker nodes as ClickHouse Keeper Nodes – these form the ClickHouse Keeper cluster (see ClickHouse Keeper Cluster Considerations).
- A ClickHouse Database cluster consisting of
  - N/2 Worker nodes as ClickHouse Data Node only
  - N/2 Worker nodes as ClickHouse Query Node only

In Option 1, events are ingested at all N nodes, query goes to all N nodes. In Option 2, events are ingested in N/2 nodes and queried from N/2 nodes. There are other options with N/2 Data Only nodes and N Query Nodes for better query performance. Option 1 is the most balanced Option that has been seen to work well.

ClickHouse Keeper Cluster Considerations

ClickHouse Keeper provides the coordination system for data replication and distributed DDL queries execution. You should use odd number of nodes in Keeper Cluster for maintaining quorum, although ClickHouse Allows even number of nodes.

- If you use 3 nodes and lose 1 node, the Cluster keeps running without any intervention.
- If you use 2 nodes and lose 1 node, then quorum is lost. You need to use the following steps in Recovering from Losing Quorum in ClickHouse Cluster to recover quorum.
- If you use 1 node and lose that node, then the ClickHouse event database becomes read only and insertion stops. You need to use the following steps in Recovering from Complete Loss of ClickHouse Keeper Cluster to recover the ClickHouse Keeper database.

Note that for high EPS environments, ClickHouse recommends running ClickHouse Keeper and Database services on separate nodes, to avoid disk and CPU contention between Query and Replication Management engines. If you have powerful servers with good CPU, memory and high throughput disks, and EPS is not high, it may be reasonable to co-locate ClickHouse Keeper and Data/Query nodes.

See ClickHouse Reference in the Appendix for related information.

Event Insertion Flow

1. Collectors send events to the Worker list specified in **ADMIN > Settings > System > Event Worker**.
2. Data Manager process on each Worker node will first select a ClickHouse Data Node and insert to that node. It may be local or remote.

Event Replication Flow

1. After insertion, ClickHouse Data Node will inform a ClickHouse Keeper Node.
2. The ClickHouse Keeper Node initiates replication to all other nodes in the same shard.

Query Flow

1. GUI sends request to App Server which sends to Query Master on Supervisor
2. Query Master provides Query management. It sends the request to a (randomly chosen) ClickHouse Query node. Each query may go to a different ClickHouse Query node.
3. The ClickHouse Query node co-ordinates the Query (like Elasticsearch Coordinating node)
   a. It sends the results to other ClickHouse Query nodes
   b. It generates the final result by combining partial results obtained from all ClickHouse Query nodes
   c. It sends the result back to Query Master
4. Query Master sends the results back to App Server; which in turn, sends it back to GUI.

ClickHouse Query Optimization Guidelines

See ClickHouse Index Design for list of ClickHouse Primary and Data Skipping indices.

Primary indices provide the best query performance followed by Data Skipping indices. The following guidelines are recommended for best query performance.

1. Use Primary indices in Filter conditions as much as possible.
2. Use Data Skipping indices in Query Filter conditions, specially when Primary indices are not possible.
3. Operator usage:
   - Operator "=" provides best performance.
   - Operators "IN" and "NOT IN" with a small set provides good performance. For these queries, a direct SQL Query is performed by enumerating the set, until the size of the resulting SQL Query is less than 200KB. When the size of the SQL Query is more than 200KB, the query is converted into a LookupTable query, which are somewhat slower. For an end user, it is not possible to measure the size of the SQL Query, but the general idea is to use as narrow a group as the problem dictates.
   - CONTAIN and REGEXP queries for string valued attributes may be relatively slow, unless there are additional conditions using Primary/Data Skipping indices in the same Filter condition.

In conclusion, the general idea is to choose the *narrowest possible Filter Condition by always including ClickHouse Primary and Data skipping indices.*

Examples

Queries with Filter conditions like “*Raw Event Log* CONTAIN “User1”” will perform poorly, since *Raw Event Log* is neither a Primary index nor a Data Skipping index. To improve query performance, consider adding Primary index or Data Skipping index to the Filter condition, e.g.

1. *Event Type* = “*FortiGate Traffic Denied*” AND *Raw Event Log* CONTAIN “User1”
2. *Event Type* IN “*Denied Traffic*” AND *Raw Event Log* CONTAIN “User1”
3. *Event Type* IN “*Regular Traffic*” AND *Raw Event Log* CONTAIN “User1”

Option 1 will provide better performance than Option 2. Option 2 will likely perform better than Option 3 since *Regular Traffic* event group has 1500+ members while *Denied Traffic* event group has about 700 members, therefore the SQL Query in Option 3 has a higher probability of crossing the 200KB size limit.

As another example, a query with Filter conditions like “*Win Logon Id* = 2” will also perform poorly, since *Win Logon Id* is neither a Primary index nor a Data Skipping index. To improve performance, change the filter condition to

- *Event Type* = “Win-Security-4624” AND *Win Logon Id* = 2

Handling ClickHouse Node IP Change

IP address are embedded in various ClickHouse configuration files and Redis. If you change the IP address of any ClickHouse node, then take these following steps to restore communication.

Step 1: If Keeper node IP changed, then update ClickHouse Keeper registry file on all Keeper nodes to reflect the new IP address.

1. Login to the node.
2. Open the file `data-clickhouse-hot-1/clickhouse-keeper/conf/keeper.xml`.
3. Change the following section for the node whose IP changed.

```
<raft_configuration>
   <server>
```

```
    <id>1</id>
    <hostname>172.30.57.174</hostname>
    <port>3888</port>
   </server>
   <server>
    <id>2</id>
    <hostname>172.30.57.175</hostname>
    <port>3888</port>
   </server>
  </raft_configuration>
```

Step 2: If Data/Query node IP changed, then update ClickHouse Keeper file on all ClickHouse Data/Query nodes.

1. Login to the node.
2. Open the file `/etc/clickhouse-server/config.d/zookeeper.xml`.
3. Change the following section.

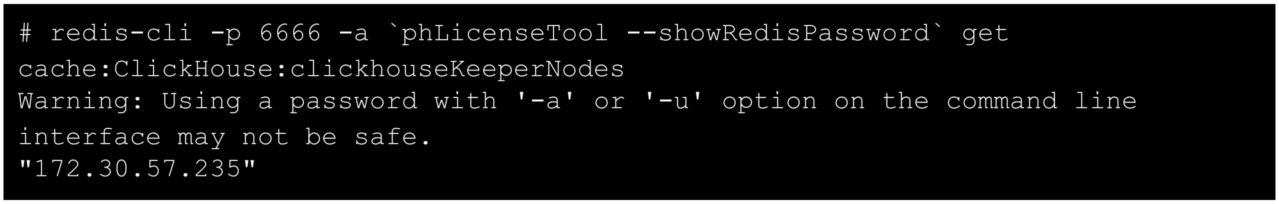
```
<zookeeper>
  <node>
   <host>172.30.57.174</host>
   <port>2181</port>
  </node>
  <node>
   <host>172.30.57.175</host>
   <port>2181</port>
  </node>
 </zookeeper>
```

Step 3: If Keeper node IP changed, then update Redis key of ClickHouse Keeper node from Supervisor.

1. Login to Supervisor node.
2. Run the following command to find out the list of ClickHouse Keeper IP addresses.

```
#redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` get
cache:ClickHouse:clickhouseKeeperNodes
```

Example Execution and Output:



```
# redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` get
cache:ClickHouse:clickhouseKeeperNodes
Warning: Using a password with '-a' or '-u' option on the command line
interface may not be safe.
"172.30.57.235"
```

3. Update the IP list with the new IP address.

```
#redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` set
cache:ClickHouse:clickhouseKeeperNodes '<new_ip_list>'
```

Example Execution and Output:

```
# redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` set
cache:ClickHouse:clickhouseKeeperNodes '172.30.57.230'
Warning: Using a password with '-a' or '-u' option on the command line
interface may not be safe.
OK
```

Step 4: If Data/Query node IP changed, then update Redis key of ClickHouse Data/Query node.

1. Login to Supervisor node.
2. Run the following command to find out the list of ClickHouse Keeper IP addresses.

   ```
   #redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` get
   cache:ClickHouse:clickhouseNodes
   ```

   Example Execution and Output:

   ```
   # redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` get
   cache:ClickHouse:clickhouseNodes
   Warning: Using a password with '-a' or '-u' option on the command line
   interface may not be safe.
   "172.30.57.235"
   ```

3. Update the IP list with the new IP address.

   ```
   #redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` set
   cache:ClickHouse:clickhouseNodes '<new_ip_list>'
   ```

   Example Execution and Output:

   ```
   # redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` set
   cache:ClickHouse:clickhouseNodes '172.30.57.230'
   Warning: Using a password with '-a' or '-u' option on the command line
   interface may not be safe.
   OK
   ```

Step 5: If Data/Query node IP changed, then update interserver_http_host and cluster file on this node where the IP changed.

`interserver_http_host` and `host` is the ip/hostname that can be used by other ClickHouse node to access this node.

1. Login to the Data/Query node where the IP changed.
2. Open `/etc/clickhouse-server/config.d/interserver_http_host.xml` file.
3. Change the following section to reflect the new IP. In this example: 172.30.58.241.

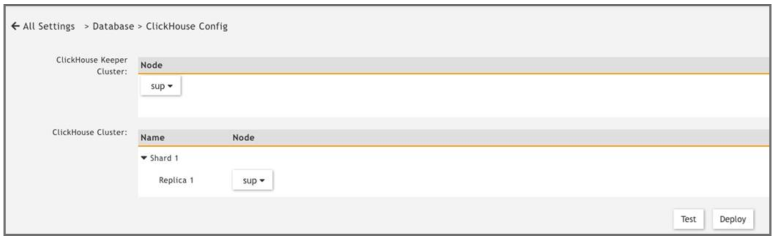
   ```
   <yandex>

     <interserver_http_host>172.30.58.241</interserver_http_host>

   </yandex>
   ```

4. Update the IP address by opening the `/etc/clickhouse-server/config.d/cluster.xml` file.
5. Change the following section to reflect the new IP. In this example: 172.30.58.241.

```
<yandex>

  <remote_servers>
    <fsiem_cluster>
      <shard>
        <internal_replication>true</internal_replication>
        <replica>
          <host>172.30.58.241</host>
          <port>9000</port>
        </replica>
      </shard>
    </fsiem_cluster>
  </remote_servers>

</yandex>
```

Step 6: Test and Save from FortiSIEM GUI

1. Login to the GUI.
2. Go to **ADMIN > Settings > Database > ClickHouse Config**.
3. Click **Test**.
4. If successful, then click **Deploy**.



ClickHouse Keeper Cluster:

Node
sup

ClickHouse Cluster:

Name	Node
Shard 1	
Replica 1	sup

Migrating ClickHouse Events from FortiSIEM 6.5.x to 6.6.0 or Later

FortiSIEM 6.5.x ran ClickHouse on a single node and used the Merge Tree engine. FortiSIEM 6.6.0 onwards runs ClickHouse on a cluster using Replicated Merge Tree engine. You need to follow these special steps to move the old events previously stored in Merge Tree to Replicated Merge Tree.

From FortiSIEM 6.5.x, you MUST first upgrade to FortiSIEM 6.6.x PRIOR to upgrading to FortiSIEM 7.x or later. If you directly upgrade from 6.5.x to 7.0.0 or later, upgrade will fail.

To upgrade your FortiSIEM 6.5.x to 6.6.x, take the following steps

1. Navigate to **ADMIN >Settings > Database > ClickHouse Config**.
2. Click **Test**, then click **Deploy** to enable the ClickHouse Keeper service which is new in 6.6.x.

3. Migrate the event data in 6.5.x to 6.6.x by running the script `/opt/phoenix/phscripts/clickhouse/clickhouse-migrate-650.sh`.
4. Verify that all events have been moved to the new table through GUI Search.
5. When the data migration is deemed successful, run the following command on every node where the `clickhouse-migrate-650.sh` script was run successfully to drop the old event table.

   ```
   clickhouse-client -q "DROP TABLE fsiem.events_non_replicated"
   ```

Now you can upgrade to FortiSIEM 7.x or later, if needed.

ClickHouse Backup and Restore Steps

This section covers the following ClickHouse backup/restore options:

- Backup to Remote SFTP Server
- Restore from Remote SFTP Server
- Backup to AWS S3
- Restore from AWS S3

Backup to Remote Server via SFTP

Backing up ClickHouse to a remote server via SFTP is done by creating a cron job to schedule a daily backup. The general steps that follow provide instructions to set up your cron job and verify that the backup is functioning.

Note: The following commands need to be run as root user in FortiSIEM.

- Step 1: Prepare the SFTP server
- Step 2: SSH to FortiSIEM node and Copy the ClickHouse Backup Config File
- Step 3: Modify the ClickHouse Backup Config File
- Step 4: Add a Crontab Job to Run the Backup Task Daily
- Step 5: Monitor the /var/log/clickhouse-backup.log to Verify if the Backup Task Happens Correctly
- Step 6: Back up All Other Shards

Step 1: Prepare the SFTP server

Once your backup server setup is complete, use the following command to verify that the backup server is set up correctly. The user *sftpuser* must have the permission to create/read/write folders.

Command:

```
sftp sftpuser@#.#.#.#
```

where `#.#.#.#` is your Backup Server IP address.

Example Execution and Output, and Creation of a Folder:

```
[root@Autosuper56206 ~]# sftp sftpuser@172.30.56.216
sftpuser@172.30.56.216's password:
Connected to 172.30.56.216.
sftp > pwd
```

```
Remote working directory: /public/sftp/sftpuser/home
sftp> ls test
Can't ls: "/public/sftp/sftpuser/home/test" not found
stfp> mkdir test
sftp> ls test
sftp>
```

Verify the backup with the following command.

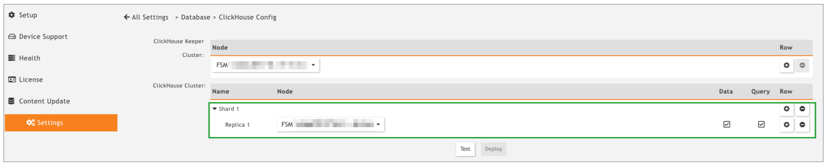
`ll clickhouse-backup/`

Example Execution and Output:

```
[root@sftpServer home]# ll clickhouse-backup/
total 16
drwxrwxr-x+ 4 sftpuser sftpusers 4096 Aug  7 13:47 backup_shard1_2023-08-07T20-47-
01
drwxrwxr-x+ 4 sftpuser sftpusers 4096 Aug  7 13:56 backup_shard2_2023-08-07T20-56-
01
```

Log in to the FortiSIEM node hosting the first replica for the first shard and follow Steps 2-5.

To identify the FortiSIEM node hosting the first replica for the first shard, navigate to **Admin > Settings > Database > ClickHouse Config**, and look at the first line to see if it is Shard 1 Replica 1.



ClickHouse Keeper Cluster:

Node	Row
FSM [redacted]	⊕ ⊖

ClickHouse Cluster:

Name	Node	Data	Query	Row
Shard 1				⊕ ⊖
Replica 1	FSM [redacted]	☑	☑	⊕ ⊖

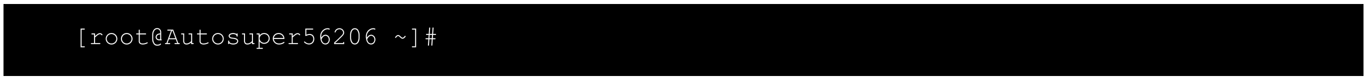
Step 2: SSH to FortiSIEM node and Copy the ClickHouse Backup Config File

Run the following command to copy the ClickHouse backup configuration from FortiSIEM to the backup server.

`cp /opt/phoenix/phscripts/clickhouse/backup_restore/config.yml /etc/clickhouse-backup`

Example Execution and Output:

```
[root@Autosuper56206 ~]# cp /opt/phoenix/phscripts/clickhouse/backup_restore/-
config.yml /etc/clickhouse-backup
[root@Autosuper56206 ~]# ll /etc/clickhouse-backup/
total 8
-rwxr-xr-x 1 root root 3146 Aug  7 11:53 config.yml
-rw-r--r-- 1 root root 3112 Dec 26  2022 config.yml.example
```



```
[root@Autosuper56206 ~]#
```

Step 3: Modify the ClickHouse Backup Config File

Edit the `/etc/clickhouse-backup/config.yml` file. In the general section, set `remote_storage` to `sftp` and add the sftp server information in the sftp section. This is required for the cron job in Step 4. After modifying the file, run the following command.

```
cat /etc/clickhouse-backup/config.yml
```

The file content should look similar to the following:

```
general:
  remote_storage: sftp
… …
sftp:
  address: "172.30.56.216"
  port: 22
  username: "sftpuser"
  password: "password"
  key: ""
  path: "clickhouse-backup"
  compression_format: tar
  compression_level: 1
  concurrency: 1
  debug: false
…
```

Step 4: Add a Crontab Job to Run the Backup Task Daily

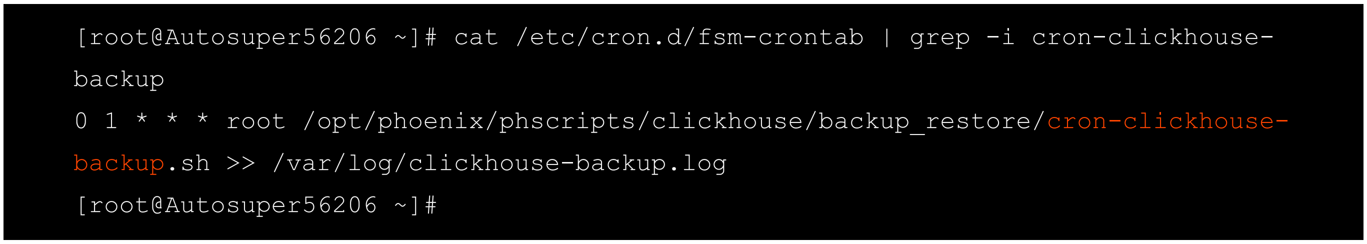
Run the following command to create a cron job that runs a daily backup task:

```
echo "0 1 * * * root /opt/phoenix/phscripts/clickhouse/backup_restore/cron-clickhouse-backup.sh >> /var/log/clickhouse-backup.log" >> /etc/cron.d/fsm-crontab
```

Verify the scheduled job is created as requested by running the following command:

```
cat /etc/cron.d/fsm-crontab | grep -i cron-clickhouse-backup
```

Example Execution and Output:



```
[root@Autosuper56206 ~]# cat /etc/cron.d/fsm-crontab | grep -i cron-clickhouse-backup
0 1 * * * root /opt/phoenix/phscripts/clickhouse/backup_restore/cron-clickhouse-backup.sh >> /var/log/clickhouse-backup.log
[root@Autosuper56206 ~]#
```

Step 5: Monitor the /var/log/clickhouse-backup.log to Verify if the Backup Task Happens Correctly

If Steps 2-4 were properly executed, you will see a log similar to the following:

```
2023-08-07T20-47-05: clickhouse-backup create and upload backup_shard1_2023-08-07T20-47-01 succeeded
```

Step 6: Back up All Other Shards

Now repeat Steps 2-5 for the first replica of every other existing shard that have not been backed up. You should see a log appear for each shard.

This is a sample log for after you have configured backup for shard2:

```
2023-08-07T20-56-04 clickhouse-backup create and upload backup_shard2_2023-08-07T20-56-01 succeeded
```

Restore from Remote SFTP Server

The following general steps that follow provide instructions that will restore a ClickHouse backup from a remote server.

- Step 1: Prepare the FortiSIEM Setup and Copy the ClickHouse Backup Config File
- Step 2: Modify the ClickHouse Backup Config File
- Step 3: Drop Schema Objects, then Download and Restore Schema Only for the fsiem.events_replicated Table
- Step 4: Drop Schema Objects, then Download and Restore Both Schema and Data for the fsiem.events_replicated Table
- Step 5: Verify the Event Count in the FortiSIEM Setup
- Step 6: Restore Other Existing Shards

Step 1: Prepare the FortiSIEM Setup and Copy the ClickHouse Backup Config File

This operation must be run on every ClickHouse replica node.

Prepare the FortiSIEM setup where the ClickHouse database will be restored. Then SSH to FortiSIEM node and copy the ClickHouse backup config file to the right location by running the following command:

```
cp /opt/phoenix/phscripts/clickhouse/backup_restore/config.yml /etc/clickhouse-backup
```

Example Execution and Output:

```
[root@Autosuper56206 ~]# cp /opt/phoenix/phscripts/clickhouse/backup_restore/-config.yml /etc/clickhouse-backup
[root@Autosuper56206 ~]# ll /etc/clickhouse-backup/
total 8
-rwxr-xr-x 1 root root 3146 Aug  7 11:53 config.yml
-rw-r--r-- 1 root root 3112 Dec 26  2022 config.yml.example
[root@Autosuper56206 ~]#
```

Step 2: Modify the ClickHouse Backup Config File

This operation must be run on every ClickHouse replica node. This is required for the restore process from your SFTP server.

Modify the backup config file - `/etc/clickhouse-backup/config.yml` as follows:

Set the `remote_storage` in the general section to `sftp`. Then add the SFTP server information in sftp section. After you have modified the backup config file, run the following command:

```
cat /etc/clickhouse-backup/config.yml.
```

The file content should look similar to the following:

```
general:
  remote_storage: sftp
… …

sftp:
  address: "172.30.56.216"
  port: 22
  username: "sftpuser"
  password: "password"
  key: ""
  path: "clickhouse-backup"
  compression_format: tar
  compression_level: 1
  concurrency: 1
  debug: false
…
```

Do the restoration Steps 3-5 for every shard.

Step 3: Drop Schema Objects, then Download and Restore Schema Only for the fsiem.events_replicated Table

This operation must be run on every ClickHouse replica node.

Find the backup name that needs be restored from the SFTP server, e.g. backup_shard1_2023-08-07T20-47-01. Then run the following commands:

```
backup="backup_shard1_2023-08-07T20-47-01"

/usr/bin/clickhouse-backup restore_remote --rm --schema -t fsiem.events_replicated
"${backup}"

clickhouse-backup delete local "${backup}"
```

Step 4: Drop Schema Objects, then Download and Restore Both Schema and Data for the fsiem.events_replicated Table

This operation must be run on the first ClickHouse replica node of one shard.

Run the following two commands:

```
/usr/bin/clickhouse-backup restore_remote --rm -t fsiem.events_replicated "${backup}"

clickhouse-backup delete local "${backup}"
```

```
    2023/08/07 15:29:36:182204 info done                       backup=backup_shard1_2023-
    08-07T20-47-01 operation=restore table=fsiem.events_replicated
    2023/08/07 15:29:36:182243 info done                       backup=backup_shard1_2023-
    08-07T20-47-01 duration=559ms operation=restore
    2023/08/07 15:29:36:182254 info done                       backup=backup_shard1_2023-
    08-07T20-47-01 operation=restore
```

Step 5: Verify the Event Count in the FortiSIEM Setup

Run the following command to verify the event count in your FortiSIEM.

```
echo 'select count() from fsiem.events_replicated' | curl 'http://#.#.#.#:8123/' --
data-binary @-;
```

where #.#.#.# is your FortiSIEM IP address.

Example Execution and Output:

```
    [root@Autoworker56226 ~]# echo 'select count() from fsiem.events_replicated' | curl
    'http://172.30.56.225:8123/' --data-binary @-;echo 'select count() from
    fsiem.events_replicated' | curl 'http://172.30.56.226:8123/' --data-binary @-; echo
    'select count() from fsiem.events_replicated' | curl 'http://172.30.56.224:8123/' -
    -data-binary @-;
    1065479
    531974
    1065479
```

Step 6: Restore Other Existing Shards

Repeat Steps 3-5 for all other shards that need to be restored. Note that the backup file will be different for every shard.

Backup to AWS S3

Backing up ClickHouse on AWS 3 is done by creating a cron job to schedule a daily backup. The general steps that follow provide the instructions to set up your cron job and verify that the backup is functioning.

- Step 1: Prepare the S3, Modify its Permission Policy
- Step 2: SSH to FortiSIEM Node and Copy the ClickHouse Backup Config File

- Step 3: Modify the ClickHouse Backup Config File
- Step 4: Add a Crontab Job to Run the Backup Task Daily
- Step 5: Verify that the Backup Task is Happening Correctly
- Step 6: Back up All Other Existing Shards

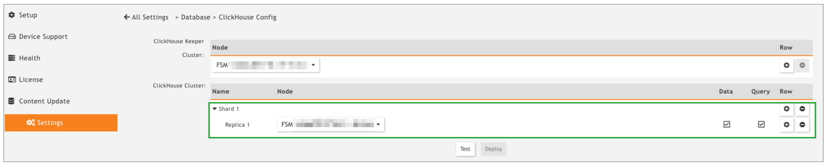
Step 1: Prepare the S3, Modify its Permission Policy

Modify your S3 permission policy.

```
{
        "Version": "2012-10-17",
        "Id": "PolicyXXXX",
        "Statement": [
                {
                        "Sid": "StmtXXXX",
                        "Effect": "Allow",
                        "Principal": {
                                "AWS": "arn:aws:iam::XXXX:user/USER"
                        },
                        "Action": "s3:*",
                        "Resource": "arn:aws:s3:::USER-clickhouse-backup-restore"
                }
        ]
}
```

Log in to the FortiSIEM node hosting the first replica for first shard and follow Steps 2-5.

To identify the FortiSIEM node hosting the first replica for the first shard, navigate to **Admin > Settings > Database > ClickHouse Config**, and look at the first line to see if it is Shard 1 Replica 1.



ClickHouse Keeper Cluster:

Node	Row
FSM [redacted]	⊕ ⊖

ClickHouse Cluster:

Name	Node	Data	Query	Row
▾ Shard 1				⊕ ⊖
Replica 1	FSM [redacted]	☑	☑	⊕ ⊖

Step 2: SSH to FortiSIEM Node and Copy the ClickHouse Backup Config File

Copy the ClickHouse backup configuration file from your FortiSIEM to AWS S3 by running the following command:

```
cp /opt/phoenix/phscripts/clickhouse/backup_restore/config.yml /etc/clickhouse-backup
```

Example Execution and Output:

```
[root@Autosuper56206 ~]# cp /opt/phoenix/phscripts/clickhouse/backup_restore/-
config.yml /etc/clickhouse-backup
[root@Autosuper56206 ~]# ll /etc/clickhouse-backup/
total 8
```

```
-rwxr-xr-x 1 root root 3146 Aug  7 11:53 config.yml
-rw-r--r-- 1 root root 3112 Dec 26  2022 config.yml.example
[root@Autosuper56206 ~]#
```

Step 3: Modify the ClickHouse Backup Config File

Edit the `/etc/clickhouse-backup/config.yml` file. In the general section, set the `remote_storage` to `s3`. Then add the S3 credentials and bucket information in the s3 section. This is required for the cron job in Step 4.

When you run the following command, your `etc/clickhouse-backup/config.yml` file content should be similar to the following.

```
cat /etc/clickhouse-backup/config.yml
```

```
    general:
      remote_storage: s3
    … …
    s3:
      access_key: "XXXXXXX"
      secret_key: "XXXXXXX"
      bucket: "XXXX-clickhouse-backup-restore"
      endpoint: ""
      region: us-east-1
      acl: private
      assume_role_arn: ""
      force_path_style: false
      path: "clickhouse-backup"
      disable_ssl: false
      compression_level: 1
      compression_format: tar
      sse: ""
      disable_cert_verification: false
      use_custom_storage_class: false
      storage_class: STANDARD
      concurrency: 1
      part_size: 0
      max_parts_count: 10000
      allow_multipart_download: false
      debug: false
    …
```

Step 4: Add a Crontab Job to Run the Backup Task Daily

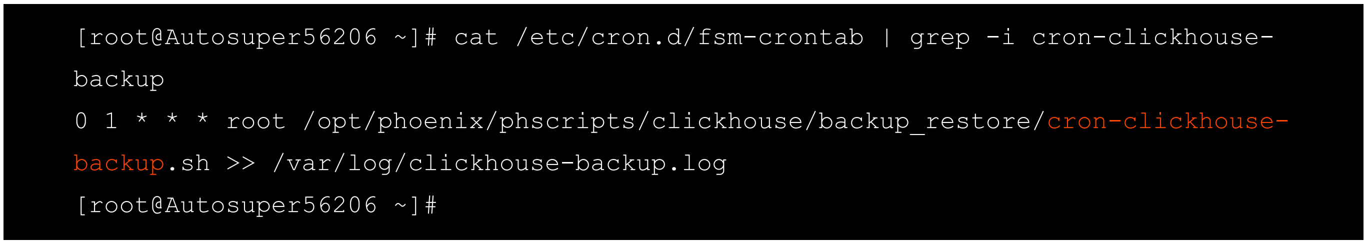
Run the following command to create a cron job that runs a daily backup task:

```
echo "0 1 * * * root /opt/phoenix/phscripts/clickhouse/backup_restore/cron-click-
house-backup.sh >> /var/log/clickhouse-backup.log" >> /etc/cron.d/fsm-crontab
```

Verify the job is created as requested:

```
cat /etc/cron.d/fsm-crontab | grep -i cron-clickhouse-backup
```

Example Execution and Output:



```
[root@Autosuper56206 ~]# cat /etc/cron.d/fsm-crontab | grep -i cron-clickhouse-
backup
0 1 * * * root /opt/phoenix/phscripts/clickhouse/backup_restore/cron-clickhouse-
backup.sh >> /var/log/clickhouse-backup.log
[root@Autosuper56206 ~]#
```

Step 5: Verify that the Backup Task is Happening Correctly

Monitor the `/var/log/clickhouse-backup.log` file. If the backup task happens, then you will see a log entry similar to the following.

```
2023-08-07T21-26-48: clickhouse-backup create and upload backup_shard1_2023-08-07T21-
26-01 succeeded
```

Step 6: Back up All Other Existing Shards

Now repeat Steps 2-5 for the first replica of every other shard. This is a sample log for after you have configured backup for shard2:

```
2023-08-07T21-26-27: clickhouse-backup create and upload backup_shard2_2023-08-07T21-
26-01 succeeded
```

Restore from AWS S3

The general steps that follow provide instructions that will restore ClickHouse from your AWS S3 backup.

- Step 1: Prepare the FortiSIEM Setup and Copy the ClickHouse Backup Config File
- Step 2: Modify the ClickHouse Backup Config File
- Step 3: Drop Schema Objects, then Download and Restore Schema Only for fsiem.events_replicated Table
- Step 4: Drop Schema Objects, then Download and Restore Both Schema and Data for fsiem.events_replicated Table
- Step 5: Verify the Event Count in the FortiSIEM Setup
- Step 6: Restore All Other Shards

Step 1: Prepare the FortiSIEM Setup and Copy the ClickHouse Backup Config File

This operation has to be run on every ClickHouse replica node.

Prepare the FortiSIEM setup where the ClickHouse database will be restored. Then SSH to FortiSIEM node and copy the ClickHouse backup config file to the right location by running the following command:

```
cp /opt/phoenix/phscripts/clickhouse/backup_restore/config.yml /etc/clickhouse-backup
```

Example Execution and Output:

```
[root@Autosuper56206 ~]# cp /opt/phoenix/phscripts/clickhouse/backup_restore/-
config.yml /etc/clickhouse-backup
[root@Autosuper56206 ~]# ll /etc/clickhouse-backup/
total 8
-rwxr-xr-x 1 root root 3146 Aug  7 11:53 config.yml
-rw-r--r-- 1 root root 3112 Dec 26  2022 config.yml.example
[root@Autosuper56206 ~]#
```

Step 2: Modify the ClickHouse Backup Config File

This operation has to be run on every ClickHouse replica node.

Modify the backup config file - `/etc/clickhouse-backup/config.yml` as follows:

Set the `remote_storage` in the general section to `s3`. Then add the S3 information in the s3 section. After your edit, run the following command:

```
cat /etc/clickhouse-backup/config.yml
```

The file content will look similar to the following:

```
general:
  remote_storage: s3
… …
s3:
  access_key: "XXXXXXX"
  secret_key: "XXXXXXX"
  bucket: "XXXX-clickhouse-backup-restore"
  endpoint: ""
  region: us-east-1
  acl: private
  assume_role_arn: ""
  force_path_style: false
  path: "clickhouse-backup"
  disable_ssl: false
  compression_level: 1
  compression_format: tar
  sse: ""
  disable_cert_verification: false
  use_custom_storage_class: false
  storage_class: STANDARD
  concurrency: 1
```

```
    part_size: 0
    max_parts_count: 10000
    allow_multipart_download: false
    debug: false
  …
```

Repeat the restoration Steps 3-5 for every shard.

Step 3: Drop Schema Objects, then Download and Restore Schema Only for fsiem.events_replicated Table

This operation must be run on every ClickHouse replica node.

Find the backup name that needs be restored from AWS S3, e.g. backup_shard1_2023-08-07T20-47-01. Then run the following commands:

```
backup="backup_shard1_2023-08-07T20-47-01"
```

```
/usr/bin/clickhouse-backup restore_remote --rm --schema -t fsiem.events_replicated
"${backup}"
```

```
clickhouse-backup delete local "${backup}"
```

Step 4: Drop Schema Objects, then Download and Restore Both Schema and Data for fsiem.events_replicated Table

This operation must be run on the first ClickHouse replica node of one shard.

Run the following two commands:

```
/usr/bin/clickhouse-backup restore_remote --rm -t fsiem.events_replicated "${backup}"
```

```
clickhouse-backup delete local "${backup}"
```

```
   2023/08/07 15:29:36:182204 info done                      backup=backup_shard1_2023-
   08-07T20-47-01 operation=restore table=fsiem.events_replicated
   2023/08/07 15:29:36:182243 info done                      backup=backup_shard1_2023-
   08-07T20-47-01 duration=559ms operation=restore
   2023/08/07 15:29:36:182254 info done                      backup=backup_shard1_2023-
   08-07T20-47-01 operation=restore
```

Step 5: Verify the Event Count in the FortiSIEM Setup

Verify the event count in your FortiSIEM by running the following command.

```
echo 'select count() from fsiem.events_replicated' | curl 'http://#.#.#.#:8123/' --
data-binary @-;
```

where #.#.#.# is your FortiSIEM Supervisor IP address.

Example Execution and Output:

```
[root@Autoworker56226 ~]# echo 'select count() from fsiem.events_replicated' | curl
'http://172.30.56.224:8123/' --data-binary @-;echo 'select count() from
fsiem.events_replicated' | curl 'http://172.30.56.225:8123/' --data-binary @-; echo
'select count() from fsiem.events_replicated' | curl 'http://172.30.56.226:8123/' -
-data-binary @-;
2327527
2327527
612053
```

Step 6: Restore All Other Shards

Repeat Steps 3-5 for all other shards that have not yet been restored. Note that the backup file will be different for every shard.

Deleting ClickHouse Organization Data

The following steps enable you to delete events belonging to an Organization in a Service Provider environment.

As a pre-requisite, collect the **Organization Id** for the "to-be-deleted" organization and the IP addresses of one data node from each shard.

1. Logon to any ClickHouse data node.
2. Run the following command as admin.
   `/opt/phoenix/phscripts/clickhouse/clickhouse-delete-org-events.sh <orgId> <data_node_shard1_ip>,<data_node_shard2_ip>`

   An example environment is provided below, for which we will run an example command.

   Shard1: Replica1: IP: 172.30.58.242

   Shard1: Replica2: IP: 172.30.58.243

   Shard2: Replica1: IP: 172.30.58.244

   Shard2: Replica2: IP: 172.30.58.245

   Org Id: 2002

   Run the following command:

   `/opt/phoenix/phscripts/clickhouse/clickhouse-delete-org-events.sh 2002 172.30.58.242,172.30.58.244`

This script uses ClickHouse Lightweight Delete concept, as illustrated here.

Rebalancing Shards

Suppose you have been running FortiSIEM on ClickHouse with one shard. The disks have become full, or your overall EPS has increased, and you want to add another shard. Then you should consider moving some data from the current shard (Shard1) to the new Shard (Shard2). Follow these steps to accomplish this objective.

1. Identify the Shard1 partition(s) that you want to move to Shard2.
2. For each partition to be moved, take the following steps:
   a. Logon to Supervisor node as admin.
   b. Copy the partition from Shard1 to one of the replicas of Shard2 running the following command. This is a replicated SQL, so you only need run it against one of the destination replicas.
      ```
      clickhouse-client -h <Shard2_Replica1_IP> -q "ALTER TABLE fsiem.events_replicated FETCH PARTITION <partition_id> FROM '/clickhouse/tables/<source_shard_id>/fsiem.events'"
      ```
   c. Detach the partition from the source shard by running the following command. This is a replicated SQL. You only need run it against one of the source replicas.
      ```
      clickhouse-client -h <Shard1_Replica1_IP> -q "ALTER TABLE fsiem.events_replicated DETACH PARTITION <partition_id>"
      ```
   d. Attach the partition to one of the destination replicas by running the following command. This is a replicated SQL. You only need run it against one of the destination replicas.
      ```
      clickhouse-client -h <Shard2: Replica1_IP> -q "ALTER TABLE fsiem.events_replicated ATTACH PARTITION <partition_id>"
      ```
   e. Delete the detached directories to release disk space by logging on to **each** node of Shard1 as root and running the following command. This is non-replicated SQL. You need run it against **all** source replicas.
      ```
      clickhouse-client -q " select path from system.detached_parts where partition_id = '<partition_id>'" | xargs rm -rf
      ```

Note: Data is not available for Query only during Step 2c and 2d above.

An example of shard rebalancing follows:

Suppose the existing ClickHouse Install has one shard (Shard1), and a new shard (Shard2) has been added.

Shard1: Replica1: IP: 172.30.58.242

Shard1: Replica2: IP: 172.30.58.243

Shard2: Replica1: IP: 172.30.58.244

Shard2: Replica2: IP: 172.30.58.245

To identify the partitions in Shard1 with the largest data, run the following command:

```
SELECT partition, formatReadableSize(sum(bytes_on_disk)) FROM system.parts where
table = 'events_replicated' and active group by partition order by partition
```

The following example output appears:

```
┌─partition──────────┬─formatReadableSize(sum(bytes_on_disk))─┐

│ (18250,20231017) │ 3.15 GiB │

│ (18250,20231018) │ 3.15 GiB │

│ (18250,20231019) │ 3.71 GiB │

│ (18250,20231020) │ 7.85 GiB │

│ (18250,20231021) │ 7.99 GiB │
```

```
│ (18250,20231022) │ 8.00 GiB │
│ (18250,20231023) │ 5.61 GiB │
└──────────────────┴───────────────────────────────────────────┘
```

Suppose you want to move partition (18250, 20231018) from Shard1 to Shard2. Proceed by taking the following steps:

1. **Copy Partition** (Step 2b above):

   ```
   clickhouse-client -h 172.30.58.244 -q "ALTER TABLE fsiem.events_replicated FETCH
   PARTITION (18250, 20231018) FROM '/clickhouse/tables/1/fsiem.events'"
   ```

2. **Detach Partition** (Step 2c above):

   ```
   clickhouse-client -h 172.30.58.242 -q "ALTER TABLE fsiem.events_replicated
   DETACH PARTITION (18250, 20231018)"
   ```

3. **Attach Partition** (Step 2d above):

   ```
   clickhouse-client -h 172.30.58.244 -q "ALTER TABLE fsiem.events_replicated
   ATTACH PARTITION (18250, 20231018)"
   ```

4. **Delete Detached Directories** (Step 2e above):

   a. Logon to Shard 1, Replica 1 (172.30.58.242).

   b. Run the following command as root:

      ```
      clickhouse-client -q " select path from system.detached_parts where par-
      tition_id = '18250-20231018'" | xargs rm -rf
      ```

   c. Logon to Shard 1, Replica 2 (172.30.58.243).

   d. Run the following command as root:

      ```
      clickhouse-client -q " select path from system.detached_parts where par-
      tition_id = '18250-20231018'" | xargs rm -rf
      ```

Advanced Operations

- Adding a Disk or Tier
- Deleting a Disk
- Deleting a Storage Tier
- Moving a Worker from One Shard to Another Shard
- Replacing a Worker with another Worker (within the same Shard)
- Recovering from Complete Loss of ClickHouse Keeper Cluster
- Recovering from Losing Quorum in ClickHouse Keeper Cluster
- Mitigating a Non-Responsive ClickHouse Keeper Node

Adding a Disk or Tier

To add a disk or tier, take the following steps.

1. Navigate to **ADMIN > License > Nodes**.
2. Select the node which you wish to add a disk or tier.
3. Click **Edit**.
4. Update the **Storage Tiers** drop-down number to change the number to tiers.
5. Click **+** from the **Hot Tier** or **Warm Tier** Row column respectively to add another Hot Tier or Warm Tier field to add a disk.
6. Click **Test**.
7. Click **Save**.
8. Navigate to **ADMIN > Settings > Database > ClickHouse Config**.
9. Click **Test**.
10. Click **Deploy**.

Notes:

- After **Deploy** succeeds, `phClickHouseMonitor` and `ClickHouseServer` processes will restart.
- When additional disks are added, the data is written across all available disks. If a disk becomes full, then data will be written to the disks with free space until all disks are full, at which point data will be moved to other ClickHouse storage tiers, archived, or purged depending on your FortiSIEM configuration.

Deleting a Disk

To delete a disk, take the following steps.

1. Unmount the disk.
2. Format the disk if you wish to remove its data.
3. Navigate to **ADMIN > License > Nodes**.
4. Select the node with the disk you wish to delete.
5. Click **Edit**.
6. Click **-** from the **Hot Tier** or **Warm Tier** Row column respectively to remove the disk.
   Note: You may see some error logs getting generated in `/opt/clickhouse/log/clickhouse-server.err.log`.

```
2022.06.20 15:55:31.761484 [ 98091 ] {} <Warning> fsiem.events_replicated (ReplicatedMergeTreePartCheckThread): Found parts with the same min block and with the same max block as the missing part 18250-20220620_371_375_1 on replica 1. Hoping that it will eventually appear as a result of a merge.

2022.06.20 15:55:31.764560 [ 98141 ] {} <Warning> fsiem.events_replicated (ReplicatedMergeTreePartCheckThread): Checking part 18250-20220620_353_378_2

2022.06.20 15:55:31.764841 [ 98141 ] {} <Warning> fsiem.events_replicated (ReplicatedMergeTreePartCheckThread): Checking if anyone has a part 18250-20220620_353_378_2 or covering part.

2022.06.20 15:55:31.765138 [ 98141 ] {} <Error> fsiem.events_replicated (ReplicatedMergeTreePartCheckThread): No replica has part covering 18250-20220620_353_378_2 and a merge is impossible: we didn't find a smaller part with the same max block.
```

```
2022.06.20 15:55:31.766222 [ 98141 ] {} <Warning> fsiem.events_replicated
(a5a85f1a-6ebf-4cf1-b82b-686f928798cc): Cannot commit empty part 18250-20220620_
353_378_2 with error DB::Exception: Part 18250-20220620_353_378_2 (state Out-
dated) already exists, but it will be deleted soon

2022.06.20 15:55:31.766574 [ 98141 ] {} <Warning> fsiem.events_replicated (Rep-
licatedMergeTreePartCheckThread): Cannot create empty part 18250-20220620_353_
378_2 instead of lost. Will retry later
```

These errors indicate that ClickHouse detected some missing data by comparing the local parts and the parts names stored in clickhouse-keeper. This is just a warning and does not affect operation. If you find this annoying, delete the entries in clickhouse-keeper by running the following commands on the Worker where the disk is deleted.

```
clickhouse-client --query "SELECT replica_path || '/queue/' || node_name FROM
system.replication_queue JOIN system.replicas USING (database, table) WHERE
last_exception LIKE '%No active replica has part%'" | while read i; do /op-
t/zookeeper/bin/zkCli.sh deleteall $i; done
```

```
clickhouse-client --query "SYSTEM RESTART REPLICAS"
```

Reference: https://github.com/ClickHouse/ClickHouse/issues/10368

7. Click **Test**.
8. Click **Save**.
9. Navigate to **ADMIN > Settings > Database > ClickHouse Config**.
10. Click **Test**.
11. Click **Deploy**.

Note: After **Deploy** succeeds, `phClickHouseMonitor` and `ClickHouseServer` processes will restart.

Deleting a Storage Tier

To delete a storage tier, take the following steps.

1. Unmount the disk.
2. Format the disk if you wish to remove its data.
3. Navigate to **ADMIN > License > Nodes**.
4. Select the node with the disk you wish to delete.
5. Click **Edit**.
6. Change **Storage Tiers** from "2" to "1".
7. Click **Test**.
8. Click **Save**.
9. Navigate to **ADMIN > Settings > Database > ClickHouse Config**.
10. Click **Test**.
11. Click **Deploy**.

Note: After **Deploy** succeeds, `phClickHouseMonitor` and `ClickHouseServer` processes will restart.

Moving a Worker from One Shard to Another Shard

To move a Worker from one shard to another shard, take the following steps.

1. Remove the Worker from the ClickHouse Keeper and ClickHouse Cluster.
2. Login to the Worker and run the following commands.
   ```
   clickhouse-client -q "DROP TABLE fsiem.events_replicated"
   clickhouse-client -q "DROP TABLE fsiem.summary"
   systemctl stop clickhouse-server
   ```
3. Login to any ClickHouse Keeper node and run the following commands to delete the registry entry from the ClickHouse Keeper cluster.
   ```
   /opt/zookeeper/bin/zkCli.sh deleteall /clickhouse/tables/<ShardID>/fsiem.events/replicas/<ReplicaID>
   /opt/zookeeper/bin/zkCli.sh deleteall /clickhouse/tables/<ShardID>/fsiem.summary/replicas/<ReplicaID>
   ```
4. Login to the Worker and navigate to `/etc/clickhouse-server/config.d`.
5. Remove all config xml under `/etc/clickhouse-server/config.d`**except** for `logger.xml`, `max_partition_size_to_drop.xml` and `max_suspicious_broken_parts.xml`.
6. Remove all config xml under `/etc/clickhouse-server/users.d/`.
7. Umount all disks that were used by ClickHouse.
8. Wipefs all disk devices that were assigned to ClickHouse.
9. Login to the Supervisor GUI, and navigate to **ADMIN > Settings > Database > ClickHouse Config**.
10. Select the target Worker and delete it from the existing shard by clicking **-** from the Row column.
11. Click **Test**.
12. Click **Deploy**.
13. Navigate to **ADMIN > License > Nodes**.
14. Select the target Worker.
15. Click **Delete** to remove the target Worker.
16. Wait for the Supervisor `phMonitor` process to come up.
17. Re-add the target Worker into the License Node with the desired disk configuration, following the instructions for adding a Worker.
18. Wait for the Supervisor `phMonitor` process to com up again.
19. Navigate to **ADMIN > Settings > Database > ClickHouse Config**.
20. Add the target Worker to the destination shard.
21. Click **Test**.
22. Click **Deploy**.

Replacing a Worker with another Worker (within the same Shard)

Currently, the GUI allows you to choose to replace one Worker (W1) with another Worker (W2) in ClickHouse Configuration. However, clicking on Test will fail since the shard and replica Ids are in use by the previous Worker (W1).

Follow these steps to replace W1 with W2.

1. Navigate to **ADMIN > Settings > Database > ClickHouse Config**.
2. Note the shardID and ReplicaID of W1. If the GUI shows Shard 3 and Replica 2, the ShardID is 3 and ReplicaID is 2. This will be needed later in Step 7.

3. Delete W1 from the ClickHouse Cluster Table by clicking **-** from the Row column.
4. Click **Test**.
5. Click **Deploy**.
6. Login to W1 and run the following SQL command in clickhouse-client shell to drop the events table.
   ```
   DROP TABLE fsiem.events_replicated
   ```
7. Login to any ClickHouse Keeper node and run the following commands to delete the registry entry from the ClickHouse Keeper cluster.
   ```
   /opt/zookeeper/bin/zkCli.sh deleteall /clickhouse/tables/<ShardID>/f-
   siem.events/replicas/<ReplicaID>
   /opt/zookeeper/bin/zkCli.sh deleteall /clickhouse/tables/<ShardID>/f-
   siem.summary/replicas/<ReplicaID>
   ```
8. Add W2 from the ClickHouse Cluster Table in same place where W1 was. It can use the same Shard ID and Replica ID.
9. Click **Test**.
10. Click **Deploy**.

Recovering from Complete Loss of ClickHouse Keeper Cluster

Complete loss of Keeper cluster may happen if you have only 1 node and it goes down.

A normal ClickHouse cluster looks like this.

```
[root@FSM-660-CH-58-246 ~]# echo stat | nc <IP> 2181
ClickHouse Keeper version: v22.6.1.1985-testing-7000c4e0033b-
b9e69050ab8ef73e8e7465f78059
Clients:
[::ffff:172.30.58.246]:36518(recved=0,sent=0)

Latency min/avg/max: 0/0/0
Received: 0
Sent: 0
Connections: 0
Outstanding: 0
Zxid: 145730
Mode: follower
Node count: 305
```

If you see logs indicating ClickHouse event Table is read only, then you know that the ClickHouse Keeper needs to be restored:

```
grep PH_DATAMANAGER_HTTP_UPLOAD_ERROR /opt/phoenix/log/phoenix.log| grep TABLE_IS_
READ_ONLY

2022-07-22T13:00:10.945816-07:00 FSM-Host phDataManager[9617]: [PH_DATAMANAGER_HTTP_
UPLOAD_ERROR]:[eventSeverity]=PHL_ERROR,[procName]=phDataManager,[fileName]-
]=ClickHouseWriterService.cpp,[lineNumber]=459,[errReason]=Uploading events to
```

```
ClickHouse failed. respCode:500 resp:Code: 242. DB::Exception: Table is in readonly
mode (replica path: /clickhouse/tables/1/fsiem.events/replicas/1). (TABLE_IS_READ_
ONLY) (version 22.6.1.1985 (official build))
```

To recover, take the following steps:

1. Login to Supervisor's redis:

   ```
   redis-cli -p 6666 -a $(grep pass /opt/phoenix/redis/conf/6666.conf | awk '{print
   $2}')

   127.0.0.1:6666> del cache:ClickHouse:clickhouseKeeperNodes
   (integer) 1
   ```

2. Navigate to **ADMIN > Settings > Database > ClickHouse Config**, and replace the dead worker with a new worker to ClickHouse Keeper cluster.
3. Click **Test**.
4. Click **Deploy**.
5. Login in to clickhouse-client on each ClickHouse node and execute the following commands.

   ```
   SYSTEM RESTART REPLICA fsiem.events_replicated
   SYSTEM RESTORE REPLICA fsiem.events_replicated
   ```

Recovering from Losing Quorum in ClickHouse Keeper Cluster

Quorum is lost when more than half of the nodes in the Keeper cluster goes down.

To identify if a ClickHouse Keeper needs recovery, you can check via log or command line.

From Log:

```
/data-clickhouse-hot-1/clickhouse-keeper/app_logs/clickhouse-keeper.err.log

2022.07.22 12:27:10.415055 [ 52865 ] {} <Warning> RaftInstance: Election timeout, ini-
tiate leader election
2022.07.22 12:27:10.415169 [ 52865 ] {} <Warning> RaftInstance: total 1 nodes (includ-
ing this node) responded for pre-vote (term 0, live 0, dead 1), at least 2 nodes
should respond. failure count 163
```

From Command Line:

```
[root@FSM-660-CH-58-246 ~]# echo stat | nc 172.30.58.216 2181
This instance is not currently serving requests
```

To recover, take the following steps:

Login to the ClickHouse Keeper node that needs recovery and run the following command.

```
echo rcvr | nc localhost 2181
```

Mitigating a Non-Responsive ClickHouse Keeper Node

To resolve a non-responsive ClickHouse Keeper node, take the following steps.

1. Check the status of Keeper cluster by running the following command on EACH Keeper node.
   ```
   echo stat | nc localhost 2181
   ```
2. Restart any non-responsive Keeper by running the following command.
   ```
   systemctl restart ClickHouseKeeper
   ```
3. If the command from step 2 does not resolve the problem, take the following steps:
   a. On the non-responsive ClickHouse Keeper node, make sure that there is ONLY a single line of `ARG1=--force-recovery` in `/data-clickhouse-hot-1/clickhouse-keeper/.systemd_argconf`. Normally, the file contains `ARG1=`.
      Modify the file so that there is only a single line of `ARG1=--force-recovery` that appears in `/data-clickhouse-hot-1/clickhouse-keeper/.systemd_argconf`.
   b. Restart the Keeper by running the following command.
      ```
      systemctl restart ClickHouseKeeper
      ```
   c. Next, run the following command to check the recovery status.
      ```
      echo stat | nc localhost 2181
      ```

Reference

The following ClickHouse References are available.

General Introduction

https://clickhouse.com/docs/en/intro

Concepts and Architecture

https://clickhouse.com/docs/en/development/architecture

ClickHouse Keeper

https://clickhouse.com/docs/en/operations/clickhouse-keeper

Performance Tuning

https://clickhouse.com/docs/en/operations/tips

Troubleshooting

https://kb.altinity.com/altinity-kb-schema-design/how-much-is-too-much/

https://clickhouse.com/docs/en/operations/system-tables/

https://clickhouse.com/docs/en/sql-reference/statements/system/#query_language-system-restore-replica

Configuration Notes

Automated CMDB Disk Space Management

If the CMDB disk partition becomes full, then the system may not work correctly. To prevent this from happening, 6.3.2 introduced a CMDB disk space management framework.

Three parameters are introduced in `phoenix_config.txt`.

- `month_retain_limit`: Number of months for which incidents on the Supervisor node should be retained (default value 6 months).
- `cmdb_disk_space_low_threshold` (in MB): When free CMDB disk space falls below this defined threshold, disk management kicks in (default value 50MB).
- `cmdb_disk_space_high_threshold` (in MB): When disk management kicks in, incidents are purged until CMDB disk space reaches this defined threshold (default value 100MB).

Two audit events are introduced.

- `PH_AUDIT_CMDB_DISK_PRUNE_SUCCESS`: This event indicates that free CMDB disk space fell below the low threshold (`cmdb_disk_space_low_threshold`) and old incidents and identity / location data were pruned to bring the free CMDB disk space above the high threshold (`cmdb_disk_space_high_threshold`).
- `PH_AUDIT_CMDB_DISK_PRUNE_FAILED`: This event indicates that free CMDB disk space fell below the low threshold (`cmdb_disk_space_low_threshold`) and in spite of pruning older incidents and identity / location data, free CMDB disk space stays below the high threshold (`cmdb_disk_space_high_threshold`). To remedy this situation, the user must reduce the number of months of incidents and identity / location data in CMDB (`month_retain_limit`).

Two system defined rules are included.

- FortiSIEM: CMDB Disk space low - Prune successful.
- FortiSIEM: CMDB Disk space low - Prune failed to keep free disk space above high threshold.

Component Communication and Network Port Usage

Information on external communication ports needed for various FortiSIEM nodes to work can be found in the External Systems Configuration Guide, here.

Configuring FortiSIEM Application Server for Proxy Connectivity

Follow these steps to configure the FortiSIEM application server to support proxy connectivity for Integrations (for example, Incidents, CMDB, Indicators of Compromise).

1. Edit the Glassfish configuration file using your favorite text editor: `/opt/glassfish/domains/domain1/config/domain.xml`.
2. Replace the `172.30.57.100` host value in the sample configuration to the Proxy Server IP, port and/or username and password in the environment.
3. If no user name and password is required, then remove the `Dhttp.proxyUser` and `Dhttp.proxyPassword` lines from the configuration file..
4. If a proxy exclusion for certain destination hosts is required, then add the `http.nonProxyHosts` configuration option to exclude the proxy server. If this is not required, then delete the line.
5. If the proxy server allows only HTTPS, then add '`s`' to `http`. For example, change `http.proxyHost` to `https.proxyHost`.

The following is a sample configuration:

```
        <jvm-options>-Dhttp.proxyHost=172.30.57.100</jvm-options>
        <jvm-options>-Dhttp.proxyPort=3128</jvm-options>
        <jvm-options>-Dhttp.proxyUser=foobar</jvm-options>
        <jvm-options>-Dhttp.proxyPassword=password</jvm-options>
        <jvm-options>-Dhttp.nonProxyHosts=172.30.59.130|localhost|update.fortiguard.com</jvm-
options>
```

Editing phoenix_config.txt File

The file `/opt/config/phoenix_config.txt` contains FortiSIEM run-time parameters. The parameters belong to 2 classes:

- Group 1: Preserved between upgrades - these parameters can be changed by the user and the changes will be preserved. For example:
  # FSM upgrade preserves customer changes to parameter value
  num_event_parser=16 #timeWithinSec requires at least 2 parser when former event will depend on later event
- Group 2: Overwritten during upgrade - these parameters are considered internal to and owned by FortiSIEM and will be overwritten during upgrade. For example:
  # FSM internal parameter; FSM overwrites
  raw_sharedstore_size=268435456 #15M = 15728640, 64M = 67108864, 256M = 268435456, 512M = 536870912

Please follow these methods if you are intentionally making changes to these parameters.

1. For parameters *affecting Supervisor and Worker nodes*, you can safely change Group 1 parameters and they will be preserved across upgrades. For Group 2 parameters, the changes will be effective, but will be overwritten during upgrade. Please contact Fortinet Support if you really need to preserve Group 2 parameter changes.
2. For parameters *affecting Collectors*, instead of changing the `/opt/config/phoenix_config.txt` file, you need to change `/opt/phoenix/config/collector_config_template.txt` on the Supervisor. This ensures that new Collectors registering will get the new parameters and the changes are preserved across upgrades. If you want to change the parameters for an existing Collector, then you need to make the same change in 2 places:
   - Change the `/opt/config/phoenix_config.txt` file on the Collector and restart the Collector.
   - Make the same change on `/opt/phoenix/config/collector_config_template.txt` on the Supervisor. This ensures that new Collectors registering will get the new parameters and the changes are preserved across upgrades.

   Other than that, the same rules for Group 1 and Group 2 apply. You can safely change Group 1 parameters and they will be preserved across upgrades. For Group 2 parameters, the changes will be effective, but will be overwritten during upgrade.

FortiSIEM Deployment Scenarios

FortiSIEM can be deployed in Enterprise and Service Provider environments in a highly scale-out fashion.

- Enterprise Deployment
- Service Provider Deployment

Enterprise Deployment

Enterprise Deployments with Supervisor and no Collector

Enterprise deployment without Collector (Supervisor only) is the simplest setup where:

- Logs are sent to the Supervisor.
- Test Connectivity, Discovery performance monitoring, and Event pulling, (for example: Cloud Services, WMI based Windows log Collection, etc.) are all done from the Supervisor – Go to **ADMIN** > **Setup** > **Credentials** and **ADMIN** > **Setup** > **Discovery**.

This setup has the following drawbacks:

- Does not scale up when a large number of devices must be monitored or high EPS needs to be handled. This can be solved by deploying Workers – see here.
- Logs cannot be collected efficiently from devices across the Internet. Devices cannot be monitored across the Internet. This is because of latency and security issues over Wide Area Networks. This can be solved by deploying Collectors – see here.
- FortiSIEM Agents cannot be used as they need Collectors – see here.

Enterprise Deployment with Supervisor and Worker but no Collector

The scalability issue above can be resolved by deploying Worker nodes. To add a Worker node:

1. Install a Worker node.
2. Add the Worker to the Supervisor from **ADMIN** > **License** > **Nodes** > **Add**.

In this case:

- Logs can be sent to the Supervisor or Workers. Sending to Workers is recommended since you can load balance across multiple Workers.
- Test Connectivity and Discovery is always done from Super.
- However, Performance monitoring and Event pulling jobs (for example: Cloud Services, WMI based Windows log Collection and so on) are done by the Worker nodes in addition to the Supervisor nodes. After Test connectivity and Discovery, Supervisor node distributes the jobs to the Workers. When a new Worker is added to the FortiSIEM Cluster, jobs are re-distributed to the Workers.

Although it provides scalable event handling, this system has the following shortcomings:

- Logs cannot be collected efficiently from devices across the Internet. Devices cannot be monitored across the Internet. This is because of latency and security issues over Wide Area networks. This can be solved by deploying Collectors – see here.
- FortiSIEM Agents cannot be used, because they need Collectors – see here.

Enterprise Deployments with Supervisor, Worker and Collector

This solution provides the flexibility of log collection and performance across the Internet and behind firewalls. It also provides even more scalability because the Collectors, instead of the Workers, parse events.

To add a Collector node:

1. Go to **ADMIN** > **Setup** > **Collector** and create a Collector in the Supervisor.
2. If you have Workers, define the Workers that the Collectors will upload to (Go to **ADMIN > Settings > System > Worker Upload**).
3. If you are not using Workers you should define the Supervisor IP or DNS name of the Supervisor (Go to **ADMIN > Settings > System > Worker Upload**).
4. Install a Collector.
5. Register the Collector to the Supervisor using any FortiSIEM user credential with Admin privileges (see **CMDB** > **User**). The built-in admin credential will work. During registration, the Collector will get the Workers to upload events to.

In this case:

- Logs can be sent to Collectors (preferred). However, they can be sent to Workers or Super as well. Collectors will upload parsed logs to the Workers in a load-balanced fashion.
- For Test Connectivity and Discovery, choose the Collector for the job. Collectors will collect events and send them to Workers in a load-balanced fashion.

In this configuration, you can add FortiSIEM Windows and Linux Agents:

1. Go to **CMDB** > **User** > **Add** and create an Agent User for Agents to register to the Supervisor node.
2. Install the Agents and register them to the Supervisor using the Agent user credential created in the previous step.
3. Define the Agent Monitoring templates.
4. Assign templates to the Agents and choose Collectors from the set created earlier.

Agents will send logs to the Collectors in a load-balanced manner. Collectors can then send to Workers in a load-balanced manner. This enables log collection in a geographically distributed and scalable manner.

Service Provider Deployment

In a Service Provider deployment, there can be one or more Organizations. Devices and logs are kept logically separated for two Organizations.

Note: **It is very important to assign devices and logs to the correct Organization in FortiSIEM.**

A FortiSIEM Service Provider deployment consists of:

- Supervisor node
- Worker nodes for scalability
- Collector nodes for remote data collection
- Windows/Linux Agents for richer data collection without remote admin credentials

While Supervisor, Workers, and Agents are shared infrastructure across Organizations, Collectors may be present and may be dedicated or shared.

This section provides details on how various infrastructure components are deployed, with an eye towards assigning devices and logs to the right Organization.

- Organizations with Dedicated Collector
- Organizations with Shared Collector

Service Provider Deployment - Organizations with Dedicated Collector

In this case, Organization has one of more Collectors that belong to that Organization only. This is suited for large Organizations.

Setup

1. Create Organizations as follows:
    a. Log in to Super-Global Organization.
    b. Go to **ADMIN** > **Setup** > **Organizations** and create an Organization.
    c. Define Admin credentials (for Collector registration) and Agent credentials (for FortiSIEM Agent registration).
    d. Add Collectors to that Organization.
2. Install the Collectors and register them to Supervisor. Use any Organization Admin credentials defined in **ADMIN** > **Setup** > **Organizations**, to register the Collector.

Operations

Collecting Logs via Agents

1. Install Agents and register them to the Supervisor. Use the Agent credentials for the Organization that the Agents belong to.
2. Define the Agent Monitoring templates. Assign the templates to agents and designate Collectors belonging to the specific Organization.

Agents will send logs to Collectors in a load-balanced fashion. Since Agents are configured with the Organization ID, they include the Organization in every log. This information is used by Collectors to assign devices and logs to the correct Organization.

Collecting Logs without Agents

Configure devices to send logs to the Organization’s Collectors. Since these collectors belong to one organization, it assigns received devices and logs to that Organization.

Discovery and Performance Monitoring by IP Address Range

Log in to the specific Organization and:

1. Define the credential.
2. Do Test Connectivity and Discovery using a specific Collector.

Event Pulling for Cloud Services

Log in to the specific Organization and:

1. Define the credential.
2. Do Test Connectivity and Discovery using a specific Collector.

Service Provider Deployment - Organizations with Shared Multi-tenant Collector

It may not be economically viable for smaller Organizations to deploy their own collectors. But Collectors may be needed to deploy Agents and to scale out data collection across many smaller Organizations managed under the same FortiSIEM.

Setup

In this setup, special multi-tenant Collectors must be defined under the Super/Local Organization as follows:

1. Log in to the Super-Local Organization. This is a built-in organization meant for the Service Provider's use only .
2. Go to **ADMIN** > **Setup** > **Collector** and add Collectors to that Organization. These are called multi-tenant Collectors as they handle devices and logs from multiple Organizations.
3. Install the Collectors and register them to the Supervisor. Use any Full Admin user in **CMDB** > **User** to register the Collector.
4. For each Collector that will be multi-tenant, do the following:
   SSH into the Collector and modify the following line under `/opt/phoenix/config/phoenix_config.txt`:
   ```
   Multi_Tenant_Collectors=false
   ```
   Change:
   ```
   Multi_Tenant_Collectors=false
   ```
   To:
   ```
   Multi_Tenant_Collectors=true
   ```
5. Reboot the Collector.

Then create Organizations as follows:

1. Log in to Super-Global Organization.
2. Go to **ADMIN** > **Setup** > **Organizations** and create an Organization.
3. Add Agent credentials for Agent registration.
4. Define the Include/Exclude IP Address ranges if devices belonging to various Organizations are going to send logs to multi-tenant Collectors.

Operations

Collecting Logs via Agents

1. Install Agents and register them to the Supervisor. Use the Agent credentials for the Organization that the Agents belong to.
2. Define Agent Monitoring templates. Assign templates to Agents and designate multi-tenant collectors belonging to the Super-local Organization.

FortiSIEM Agents will send logs to multi-tenant Collectors in a load-balanced fashion. Since Agents are configured with the Organization ID, they include the Organization in every log. This information is used by multi-tenant Collectors to assign devices and logs to the correct Organization.

Collecting Logs without Agents

Configure devices to send logs to the multi-tenant Collectors. Make sure the reporting device IP matches the Include/Exclude IP ranges defined for that Organization in **ADMIN** > **Setup** > **Organization**. A multi-tenant Collector uses the reporting device IP to assign devices and logs to the correct Organization.

Discovery and Performance Monitoring by IP Address Range

This is possible so long as the IP Address range matches the Include/Exclude IP ranges defined for that Organization in **ADMIN** > **Setup** > **Organizations**.

This can be done in two ways:

1. (Recommended) From Super/Global Organization:
   a. Define the credential.
   b. Do Test Connectivity and Discovery. We will automatically choose a multi-tenant collector
2. Alternatively, log in to the Super/Local Organization and:
   a. Define the credential.
   b. Do Test Connectivity and Discovery using a specific multi-tenant Collector.

Approach #1 is recommended because the Collector is automatically chosen.

Event Pulling for Cloud Services

From Super/Global Organization:

1. Define the credential. Specify the Organization in the credential.
2. Perform Test Connectivity and Discovery.
   FortiSIEM will automatically choose a multi-tenant Collector.

Collecting Logs from Multi-tenant Devices

A shared Collector also enables you to collect logs from multi-tenant devices such as FortiGate with Virtual Domains (VDOM). This assumes that the logs contain an attribute (such as FortiGate VDOM) that enables FortiSIEM to classify logs from multi-tenant devices to different Organizations.

From a Super/Global Organization:

1. Go to **ADMIN** > **Settings** > **Event Handling** > **Event Org Mapping**.
2. Click **New** and enter the Organization mappings for the discriminating log attribute (such as VDOM).
3. Click **Save**.

FortiSIEM OS Updates and Internet Connectivity

The following table details hosts that FortiSIEM will connect to for package verification, content updates, lookups and OS updates.

Required By	Used For	Host
Super	IOC feed and IOC lookups, validation of Collector & Agent packages, Content Updated	update.fortiguard.net / TCP / 443
Super, Worker, Collectors	OS updates*	os-pkgs-cdn.fortisiem.fortinet.com / TCP / 443 os-pkgs-r8.-

Required By	Used For	Host
		fortisiem.fortinet.com / TCP / 443

*Please check the FortiSIEM - OS Update Lifecycle guide for additional information.

Elasticsearch Usage Notes

Note: AWS Elasticsearch Service is now officially known as AWS OpenSearch Service (See here). References to "AWS Elasticsearch Service" in this documentation can be considered the same as "AWS OpenSearch Service".

Configuring Elasticsearch Buffer

When there is a huge number of events, the Elasticsearch server may become overloaded with processing them and cannot accept all uploads during this time.

A solution to this issue is to save events to a local disk when events cannot be uploaded. FortiSIEM allows you to configure a disk based buffer to save these events until Elasticsearch is available again.

Fortinet recommends that a dedicated disk be used for this purpose. At a minimum, ensure it does not use shared NFS, which could cause latency. It is also strongly recommended that if you wish to use this feature on Workers, that all Workers be configured. If a Worker is not configured, it will be blocked, and consequently, will not accept Collector event uploads. In this situation, the Collector will fail to upload to the unconfigured Worker, and will attempt to connect to another Worker that accepts uploads.

To configure, access the `phoenix_config` file. If the buffer path is defined, the feature is enabled.

```
[BEGIN Elasticsearch]

log_buffer_per_customer_path=/eventbuffer #empty means disabled.

log_buffer_per_customer_reserved_disk_space=1 # GB

[END]
```

Next, in the `phoenix_config` file, in the Elastisearch section, modify `index_max_retry` to configure the number of times FortiSIEM will attempt to retry uploads. If the retry time is set to 0, FortiSIEM will never drop events and after the connection between FortiSIEM and Elasticsearch has recovered, all events will be uploaded.

After defining the event buffer path, restart `phDataManager`.

This feature can be enabled on the Supervisor and Workers.

Configuring Elasticsearch Timeout

To configure, go to the Elasticsearch section of `/opt/phoenix/config/phoenix_config.txt` and add the following line:

```
restapi_timeout_in_seconds=<# of seconds>
```

Example:

```
restapi_timeout_in_seconds=300
```

and restart phDataPurger.

Dynamic Scripting Limits

In FortiSIEM, Elasticsearch queries are run using dynamic scripts because of multi-field aggregation of query results. In Elasticsearch, there are two related limits.

1. Rate at which scripted queries can be compiled (cluster level limit)
2. Cache for the compiled scripts (node level limit)

If the compile limit is reached, then Elasticsearch will throw a circuit_breaking_exception error and the query will not run. If the cache limit is reached, then the query will need to be recompiled and may run a little slowly for the first time.

```
[PH_JAVA_QUERYSERVER_ERROR]:[eventSeverity]=PHL_ERROR,[phEventCategory]=3,[methodName]=innerFromXContent,[className]=org.elasticsearch.ElasticsearchException,[procName]=javaQueryServer,[lineNumber]=509,[errReason]=Elasticsearch exception [typee=circuit_breaking_exception, reason=[script] Too many dynamic script compilations within, max: [75/5m]; please use indexed, or scripts with parameters instead; this limit can be changed by the [script.context.aggs.max_compilations_rate] setting],[phLogDetail]=Elasticsearch exception [type=search_phase_execution_exception, reason=all shards failed]
```

Current limits in your environment can be obtained by running the following API.

```
GET /_nodes/stats?filter_path=nodes.*.script_cache.contexts
{
  "nodes": {
    "kISLOIv_QvGbFNnpDtLdyw": {
      "script_cache": {
        "contexts": [
          {
            "context": "aggregation_selector",
            "compilations": 0,
            "cache_evictions": 0,
            "compilation_limit_triggered": 0
          },
          {
            "context": "aggs",
            "compilations": 1795,
            "cache_evictions": 1695,
            "compilation_limit_triggered": 249
          },
    ...
}
```

You can change the compilation rates by running the query using the following API.

```
PUT _cluster/settings (For ES 7.9 and above)
{
    "persistent": {
        "script.context.aggs.max_compilations_rate": "150/5m"
    }
}

PUT _cluster/settings (For ES below 7.9)
{
    "persistent": {
        "script.max_compilations_rate": "150/5m"
    }
}
```

You can set `script.context.$CONTEXT.cache_max_size` in the `elasticsearch.yml` configuration file. For example, to set the max size for the `aggs` context, you would add the following to `elasticsearch.yml`.

```
script.context.aggs.cache_max_size: 300
```

This is a node level setting, which when changed, needs node restart.

References

1. https://www.elastic.co/guide/en/elasticsearch/reference/7.9/modules-scripting-using.html#prefer-params
2. https://alexmarquardt.com/2020/10/21/elasticsearch-too-many-script-compilations/

Elasticsearch Feature Compatibility

There are 3 distinct Elasticsearch deployments. This table shows the versions and features supported for each deployment type. Please also see the list of Elasticsearch related known issues in Elasticsearch Known Issues in Appendix - Elasticsearch Usage Notes.

Elasticsearch Deployment	API (Insertion and Search)	Supported Data Node Types	Disk Space based Retention	Age based retention (ILM)
Self-Managed (On-Prem or Hosted)	REST	Hot, Warm, Cold	Yes	Yes (6.8 and above)
AWS OpenSearch Service (Previously known as AWS Elasticsearch Service)	REST	N/A	Yes	No
Elastic Cloud	REST	N/A	Yes	No

Merging Small Elasticsearch Indices into a Big Index

In Elasticsearch, you may see older indices with few documents. You may want to merge these smaller indices into a bigger index and create an alias for them, by following these steps.

Elasticsearch reference: https://www.elastic.co/guide/en/elasticsearch/reference/7.13/docs-reindex.html

Notes:

1. Don't merge indices that belong to different organizations together.
2. The naming format for event index is: `fortisiem-event-<Year>.<Month>.<Date>-<OrgId>-<SeqNo>`
3. When merging indices from different days together, make sure to create aliases for the different days to point to the merged index

Steps

1. Create one new index.

```
curl -XPUT '172.30.56.182:9200/fortisiem-event-2021.07.30-3-000001-merged?pretty' -H 'Content-Type: application/json' -d'
{
    "settings" : {
        "index" : {
           "number_of_shards" : 1
        }
    }
}
'
```

2. Merge the smaller indices into the new index created in Step 1.

```
curl -XPOST '172.30.56.182:9200/_reindex?pretty' -H 'Content-Type: application/json' -d'
{
    "conflicts": "proceed",
    "source": {
        "index": "fortisiem-event-2021.07.30-3-000001,fortisiem-event-2021.07.29-3-000001"
    },
    "dest": {
        "index": "fortisiem-event-2021.07.30-3-000001-merged",
        "op_type": "create"
    }
}
'
```

3. Create aliases for all (newly created) merged indices.

   ```
   curl -X POST 'http://172.30.56.182:9200/_aliases' -H 'Content-Type: applic-
   ation/json' -d'
   {
      "actions":[
         {
            "add":{
               "index":"fortisiem-event-2021.07.30-3-000001-merged",
               "alias":"fortisiem-event-2021.07.30-3"
            }
         }
      ]
   }
   '
   ```

4. Delete all old indices.

   ```
   curl -XDELETE http://172.30.56.182:9200/fortisiem-event-2021.07.30-3-000001
   curl -XDELETE http://172.30.56.182:9200/fortisiem-event-2021.07.29-3-000001
   ```

Differences in Analytics Semantics between EventDB and Elasticsearch

FortiSIEM can run on EventDB, its own proprietary NoSQL database, or Elasticsearch. To make analytics work correctly in both environments, it is important to understand the differences. Analytics includes real-time search, historical search, and rule correlation.

FortiSIEM rule correlation and real-time search work identically in both environments, because computation is done in-memory. The database is not used.

However, for historical search, results are obtained from the database and the following differences exist in the area of string comparisons, primarily because of the way Elasticsearch, a third-party product, works.

- Issues
- Example 1 - Matching Event Types
- Example 2 - Matching Raw Messages
- Elasticsearch Support for Regex

Issues

1. EventDB is a sub-string match while Elasticsearch is a word-based match with white space as a delimiter between words. This means that the EventDB will find a match anywhere in the string. For Elasticsearch, you must explicitly include wildcard characters. This affects string operations involving the following operators: =, IN, CONTAIN, REGEXP and their inverse versions: !=, NOT IN, NOT CONTAIN and NOT REGEXP.
2. For Elasticsearch query, if an expression is defined as a display parameter and the expression includes aggregate functions, then the aggregates must be separately added as display parameters. For example, if a user wants to display an expression such as *100 - (100.0 * SUM(System Downtime))/SUM(Polling Interval)*, then the user must also add *SUM(System Downtime)* and *SUM(Polling Interval)* to the list of display parameters.

3. Sorting does not work for
   - LAST and FIRST operators when the operand is a non-Date type.
   - HourOfDay and DayOfWeek operators
4. When sorting is used for multiple key values, e.g. Group By Source IP, Destination IP, COUNT(*) DESC, then the results are presented by the last attribute (e.g. Destination IP). FortiSIEM EventDB sorts by all the fields taken as a tuple, e.g. (Source IP, Destination IP). See https://www.elastic.co/guide/en/elasticsearch/reference/current/search-aggregations-bucket-terms-aggregation.html
   See also Example 1 - Matching Event Types and Example 2 - Matching Raw Messages
5. Elasticsearch (and lucene) do not support full Perl-compatible regex syntax. https://www.elastic.co/guide/en/elasticsearch/reference/current/regexp-syntax.html
   The table in Elasticsearch Support for Regex lists what is supported and workaround suggestions.

Example 1 - Matching Event Types

Suppose you are trying to match PH_DEV_MON for Event Type:

- In EventDB, you can write any of the following:
  - *EventType CONTAIN PH_DEV_MON*
  - *EventType CONTAIN _DEV_MON*
  - *EventType CONTAIN ph_dev_MON*
  - *EventType CONTAIN _DEV_mon*
- In Elasticsearch, you can write any of the following. Note that since event types do not end with PH_DEV_MON, you have to add the wildcard ".*" at the end.
  - *EventType CONTAIN PH_DEV_MON.**
  - *EventType CONTAIN .*_DEV_MON.**

Suppose you are trying to exactly match PH_DEV_MON_INTF_UTIL for Event Type:

- In EventDB, you can write any of the following:
  - *EventType = PH_DEV_MON_INTF_UTIL*
  - *EventType = ph_dev_mon_intf_util*
  - *EventType = ph_dev_MON_INTF_UTIL*
- In Elasticsearch, you must write:
  - *EventType = PH_DEV_MON_INTF_UTIL*

Example 2 - Matching Raw Messages

REGEX matching using the FortiSIEM eventDB is case insensitive.

Suppose the raw message is:

- *XYZ info="ABB123CCC"*

To match this raw message:

- In EventDB, you can write any of the following:
  - *Raw Message REGEX bb[0-9]*c*X?*
  - *Raw Message REGEX Abb[0-9]*c*X?"$*

- In Elasticsearch, you can write any of the following:
  - *Raw Message REGEX BB[0-9]*c*X?*
  - *Raw Message REGEX .*BB[0-9]*c*X?*

Elasticsearch Support for Regex

Regex syntax	Elasticsearch support	Workaround (if any)
. ? + * |	Yes	
?? +? *?	No	Not possible
()	Yes	
(?:)	No	Use () instead. Replace (?:com|net|org) with (com|net|org)
[]	Yes	
[^]	Yes	
{}	Yes	
{}?	No	Not possible
^ $	No	Elasticsearch requires full match. Add .* for partial match.
\d \D \w \W \s \S	No	Replace \d with [0-9] Replace \D with [^0-9] Replace \w with [a-zA-Z0-9_] Replace \W with [^a-zA-Z0-9_] Replace \s with [\t \n \r] Replace \S with [^ \t \n \r]
\b \A \Z	No	Not possible
(?i:)	No	Not possible
\1 \2	No	Not possible
(?=)	No	Not possible
(?!)	No	Not possible

Regex syntax	Elasticsearch support	Workaround (if any)
(?#)	No	Not possible
Case sensitive match on keyword attributes	No	If an attribute is not a keyword, it will be stored as lower case in Elasticsearch. Use abc or [aA][bB][cC]
Entire raw message search	No	Elasticsearch tokenizes string attributes using space as tokens. So, it is not possible to search the whole string. Use CONTAIN operator.

Elasticsearch Known Issues

Note: AWS Elasticsearch Service is now officially known as AWS OpenSearch Service. References to "AWS Elasticsearch Service" can be considered the same as "AWS OpenSearch Service".

1. With pre-compute queries via Rollup, sorting on AVG() is not supported by Elasticsearch. See here.
2. Elasticsearch pre-compute is done using the Elasticsearch Rollup API, which requires raw events matching the pre-compute search condition be populated into a separate Elasticsearch index. This operation can become very expensive if a large number of events match the pre-compute search filter condition. Fortinet recommends that the user set up a report for pre-compute only if the search filter conditions for the pre-compute interval result in less than 100K entries. This allows the pre-computed result to exactly match the adhoc report for faster operation. Specifically, follow these steps:
    a. Suppose you want to run a report in pre-compute mode, with the operation running pre-computations hourly. This means the report will be run hourly, and when a user runs for a longer interval, the pre-computed results would be combined to generate the final result.
    b. Check for pre-compute eligibility.
        i. Run the report in adhoc mode for 1 hour by removing group by conditions.
        ii. If the number of rows is less than 100K, then the original report is a candidate for pre-computation.**Note**: This is for Elasticsearch only. If the number of results in #Bii is more than 100K, then the pre-computed results and adhoc results will be different since FortiSIEM caps the number of results retrieved via Rollup API to be less than 100K.
3. AWS Managed Elasticsearch 7.x limits search.max_buckets to 10K. In 6.8 there was no such limit. This may cause Elasticsearch to throw an exception and not return results for aggregated queries. Contact AWS Managed Elasticsearch Support to increase search.max_buckets to a large value (recommended 10M). There is an API to change this value, but this does not work in AWS Managed Elasticsearch. Therefore you must contact AWS Managed Elasticsearch Support before running queries.
    a. For general discussion about search.max_buckets, see here.
    b. For general discussion about this issue, see here.
    c. Elasticsearch does not consistently handle sorting functions when there are NULL values. For example:
        i. AVG(): NULL values are at the bottom.
        ii. MIN(): NULL values are considered to be the largest value possible, so if you choose ASC (respectively DESC) order, NULL values appear at the bottom (respectively top).
        iii. MAX():NULL values are considered to be the smallest value possible, so if you choose ASC (respectively DESC) order, NULL values appear at the top (respectively bottom).

4. Pre-compute queries do not work with the HAVING clause. Currently, the FortiSIEM GUI is preventing this operation. For public discussion about Rollup search and query scripts, see here.
5. The HourOfDay(Event Receive Time) and DayOfWeek(Event Receive Time) calculations are incorrect if Elasticsearch and Supervisor are in different time zones.
6. In Elasticsearch, a non-aggregated query spanning multiple display pages requires 1 open scroll context per shard. This enables the user to visit multiple pages and see the results. Elasticsearch has a (configurable) limit on open scroll contexts. This is defined in `phoenix_config.txt` on the Supervisor node. By default, FortiSIEM limits to 1000 open scroll contexts and each context remains open for 60 seconds, as shown.

   [BEGIN Elasticsearch]
   ```
   ...
   max_open_scroll_context=1000
   scroll_timeout=60000
   ...
   ```
   [END Elasticsearch]

   When the open scroll context limit is reached, Elasticsearch throws an exception and returns partial results. When 80% of the search context limit is reached, FortiSIEM writes a log in `/opt/phoenix/log/javaQueryServer.log`, as shown.

   ```
   com.accelops.elastic.server.task.ChoresTask - [PH_JAVA_QUERYSERVER_WARN]:
   [eventSeverity]=PHL_WARNING,[phEventCategory]=3,[procName]=javaQueryServer,
   [phLogDetail]=node=node236, openContexts=1000, it has 80 percent of available
   search contexts open
   ```

   - You can increase `max_open_scroll_context`. However, AWS Elasticsearch does not allow more than 500 open scroll contexts, and will enforce a 500 limit. Be careful in choosing very high `max_open_scroll_context`. It is strongly recommended to use a test instance to experiment with your number prior to production.
   - After changing `max_open_scroll_context`, you need to apply Test & Save from the GUI for changes to take effect. This is because `max_open_scroll_context` is a cluster level setting.
   - You can change `scroll_timeout`, but after changing this value, you must restart the Java Query Server on the Supervisor for the change to take effect.
     For Elasticsearch discussion forum information on this topic, see here.
7. The maximum number of group by query result is 2,000 by default. You can change the setting in `phoenix_config.txt`
   on the Supervisor node by taking the following steps.
   a. Change the setting: `aggregation_size=2000`
   b. Restart the JavaQueryServer.
8. FortiSIEM uses dynamic mapping for Keyword fields to save Cluster state. Elasticsearch needs to encounter some events containing these fields before it can determine their type. For this reason, queries containing `group by` on any of these fields will fail if Elasticsearch has not seen any event containing these fields. Workaround is to first run a non-group by query with these fields to make sure that these fields have non-null haves.

FortiEMS Endpoint Tagging

- Overview
- Updated Remediation Scripts

- Fortinet FortiEMS (Endpoint Management Server) Discovery Setup
- Best Practice Setup
- Scheduling Automatic Tagging Example

Overview

FortiSIEM now supports discovery of your FortiEMS servers using the FortiEMS Management Server API with basic authentication (username/password).

FortiSIEM will poll EMS, on a regular interval (default 5 min), and retrieve all vulnerabilities detected for managed FortiClient devices. FortiSIEM will send these as log events, which will create a CMDB entry for each device as unmanaged, if they don't already exist. You can then view vulnerability data about the FortiClient managed devices from the CMDB.

When FortiEMS discovery is done, FortiSIEM can tag or untag a host, using classification tags on FortiEMS server. In ZTNA, these tags are imported by member Fortinet devices, particularly FortiGate firewalls, and are referenced in ZTNA firewall rules.

A common use case would be tagging a host as suspicious, or potentially compromised, and having Firewall rules isolate or allow minimal network traffic for FortiClient managed devices that are assigned those tags.

Updated Remediation Scripts

FortiSIEM has updated several automated response (remediation) scripts to work with FortiEMS.

You can now, adhoc or via notification policy, execute a remediation script, via the **Incidents** page (From **Incidents**, select an incident and select **Remediate Incident** from the **Actions** drop-down list, and set/unset tag for the device in FortiEMS.) or **Analytics > Investigation** page.

This allows rules that have tags defined, to assign those tags to relevant hosts in the incident, that are also FortiClient managed devices.

The two primary remediation scripts are:

- Set tag for device in FortiEMS
- Unset tag for device in FortiEMS

Fortinet FortiEMS (Endpoint Management Server) Discovery Setup

To set up FortiEMS discovery, you will need to configure FortiEMS, then configure FortiSIEM.

Note: If you are just pulling in vulnerability data, you can just use a read only user role. If you'd like to use FortiSIEM remediation scripts to set/unset EMS tags of FortiClient host devices, some write permissions are required.

- FortiEMS Configuration
- FortiSIEM Configuration

FortiEMS Configuration

Here, you will configure an admin role, and create an administrator user with the configured admin role. Take the following steps.

1. Login to FortiEMS Server.
2. Navigate to **Administration > Admin Roles**.
3. Click **Add**.
4. In the **Name** field, enter a name, such as "read_plus_tagging" (or your preferred role name).
   a. (Optional) In the **Description** field, enter a description, for example: "Used by FortiSIEM to ingest vulnerability data and create/set/unset EMS tags.".
   b. Under **Endpoint permissions**, select the following checkboxes.
      i. Block/Unblock/Quarantine/Unquarantine/Reregister endpoints
      ii. View group assignment rules
      iii. View endpoint filter bookmarks
      iv. View quarantine management
      v. View software inventory
   c. Under **Policy permissions**, select the following checkboxes.
      i. View endpoint policies
      ii. View endpoint profiles
      iii. View Zero Trust tagging rules
      iv. View installers
      v. View CA certificates
      vi. View on-fabric detection rules
   d. Under **Settings permissions**, select the following checkboxes.
      i. View EMS settings
      ii. View Fortinet services settings
      iii. View alert settings
      iv. View custom message settings
      v. View features select settings
   e. Click **Save**.
5. Navigate to **Administration > Administrators**.
6. Click **Add**.
7. In the **Add user** window, select **Create a new user**.
   a. In the **Username** field, enter a name, for example "fortisiem_user".
   b. From the **Role** drop-down list, select the role created, earlier - "read_plus_tagging".
   c. (optional) Toggle **Restrict Login to Trusted Hosts** on and add the IP of FortiSIEM component (IP of FortiSIEM node completing the discovery e.g. collector IP address).
   d. Click **Next**.
   e. In the **Password** and **Confirm Password** fields, enter a password that meets the FortiEMS requirements and click **Finish**.

FortiSIEM Configuration

With the FortiEMS admin user configured, you will set up FortiSIEM with the admin user credentials. Take the following steps.

1. Login to the FortiSIEM GUI.
2. Navigate to **Admin > Setup > Credentials**.
3. Under **Step 1: Enter Credentials**, click **New**.

4. In the **Name** field, enter a credential, for example, "EMS_Server" (or your arbitrary name for the credential).
5. From the **Device Type** drop-down list, enter/select **Fortinet FortiClient EMS**.
6. Confirm **Access Protocol** is set to **FORTIEMS_API**. If not, select it.
7. Leave the **Pull Interval** at 5 minutes, or optionally change it to 1 minute to 24 hours (1440 minutes). 5 minutes is recommended.
8. Change the **Port** number if the admin port is different than the default 443.
9. In the **Serial Number** field, enter your serial number of your EMS server.
   Note: To get the EMS server serial number, login to your EMS server, navigate to **Dashboard > Status**. The serial number will appear next to **Serial Number**. The serial number is important for remediation script automation, discussed later.
10. In the **User Name** field, enter the FortiEMS admin username created earlier.
11. In the **Password** and **Confirm Password** fields, enter the password associated with the FortiEMS admin username.
12. Click **Save**.
13. Under **Step 2: Enter IP Range to Credential Associations**, click **New**.
14. In the **IP/Host Name** field, enter the IP address or hostname of the FortiEMS server.
15. From the **Credentials** drop-down list, select the EMS credential you just defined ("EMS_Server").
16. Click **Save**.
17. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping**. A pop up will appear and show the Test Connectivity results. Proceed to step 18 when connectivity succeeds.
18. Navigate to **ADMIN > Setup > Discovery** and click **New**.
    a. Enter the Name of the discovery entry.
    b. Select Discovery Type.
    c. Enter IP address or hostname of the FortiEMS server in the Include entry.
    d. Click **Save**.
19. Select the identified discovery, and click **Discover**.
20. Click the **Pull Events** tab at the top of the screen. A yellow star should appear next to your EMS server.
21. Wait approximately 5 minutes for the first job to start.
22. The Pull Events page will eventually show a green checkbox next to the EMS server job.
23. Navigate to **Analytics**, and confirm that EMS events are seen.

Best Practice Setup

The FortiEMS and the FortiGate firewall discoveries work in tandem to allow automatic tagging of devices via FortiSIEM triggering incidents.

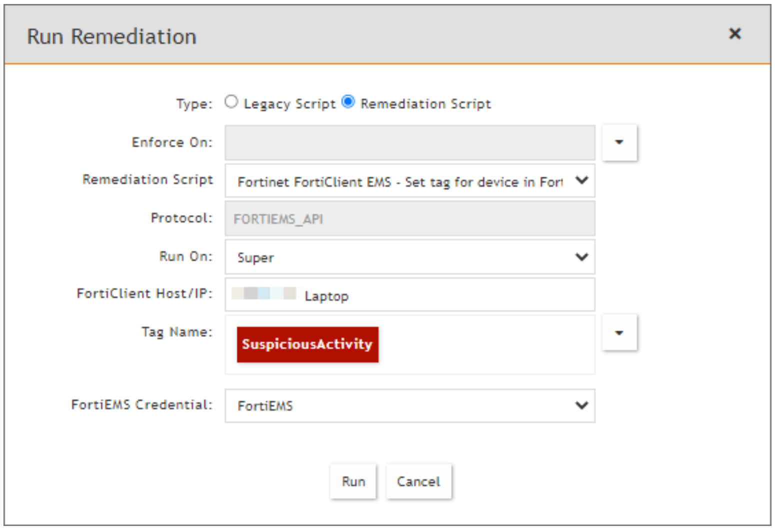
The rough structure looks like this:

1. You configure your FortiGate firewalls for API discovery, and user device store observed FortiClient managed devices will be imported into FortiSIEM.
   Each of these devices is imported into FortiSIEM CMDB, each with a special attribute called the FortiEMS serial number, which is the EMS server identification that the device is registered to.
2. You configure your FortiEMS server credential in FortiSIEM. In the credential, you also hand define the FortiEMS serial number, along with the service user account to access FortiEMS.
3. You define a number of tags in FortiSIEM by navigating to **Admin > Settings > Analytics > Tags**, and clicking **New** to create a tag.

4. You edit any desired FortiSIEM rules by navigating to **Resources > Rules > <*selected rule*>**, and adding a tag by clicking **Edit**, navigating to **Step 3: Define Action**, selecting the tag from the **Tag** drop-down list, and clicking **Save**.**Note**: For System rules, you may have to clone the rule, disable the old system rule, and edit the cloned rule.
5. You create a notification policy that includes a remediation action when the given rule is triggered, in our example, we will use "Set tag for device in FortiEMS".
    a. Navigate to **Admin > Settings > General > Notification Policy**, and click **New**.
    b. From **Rules**, select the individual rule you have that contains uses of the tag you defined.
    c. From **Affected Orgs**, select the affected organizations, if any.
    d. Next to **Run Remediation / Script**, click the Edit icon (pencil), then click **New**.
        i. For **Type**, select **Remediation Script**.
        ii. From the **Script** drop-down list, select **Fortinet FortiClient EMS - Set tag for device in FortiEMS**.
        iii. Leave **Enforce On** blank.
        iv. From the **Run On** drop-down list, select the target collector that you would like to execute the script from. Remember that if you have IP restrictions on user accounts, you must make sure that the node calling the API is allowed.
        v. Leave the **Tag Name** drop-down list alone to allow auto selection, or select a tag to force a particular tag be used.
        vi. Leave the **FortiEMS Credential** drop-down list alone to allow auto selection, or select which FortiEMS server to execute the script against.
        vii. Click **Save**.
    e. Ensure that the **Run Remediation/Script** checkbox is now checked.
    f. Click **Save**.

You can tag FortiClient hosts by IP or Hostname using remediation scripts adhoc via the **Incident s** page, by taking the following steps.

1. Navigate to **Incidents**.
2. Select an incident.
3. Click the **Actions** drop-down list and select **Remediate Incident**.
4. Set/Unset the tag for the device in FortiEMS.



Run Remediation ×

Type: ○ Legacy Script ● Remediation Script

Enforce On:

Remediation Script: Fortinet FortiClient EMS - Set tag for device in Fort

Protocol: FORTIEMS_API

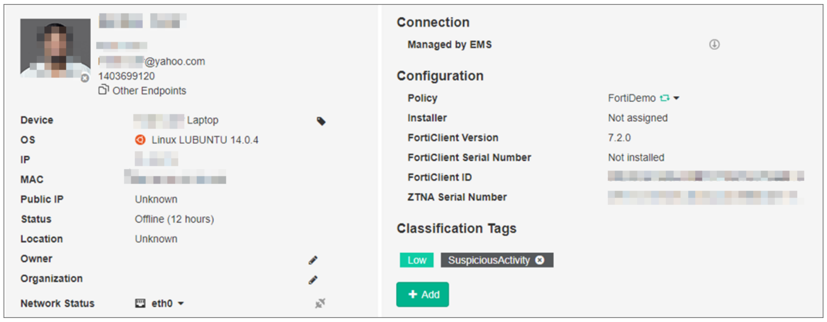
Run On: Super

FortiClient Host/IP: [redacted] Laptop

Tag Name: SuspiciousActivity

FortiEMS Credential: FortiEMS

When tagged, the laptop from the screenshot example above now has the additional classification tag in the FortiEMS server below, as shown in the below screenshot:



[redacted]
[redacted]
[redacted]@yahoo.com
1403699120
Other Endpoints

Device	[redacted] Laptop
OS	Linux LUBUNTU 14.0.4
IP	[redacted]
MAC	[redacted]
Public IP	Unknown
Status	Offline (12 hours)
Location	Unknown
Owner	
Organization	
Network Status	eth0

Connection

Managed by EMS	

Configuration

Policy	FortiDemo
Installer	Not assigned
FortiClient Version	7.2.0
FortiClient Serial Number	Not installed
FortiClient ID	[redacted]
ZTNA Serial Number	[redacted]

Classification Tags

Low SuspiciousActivity

Additional Information on Automatically Tagging a Host

When an incident triggers, and a matching notification policy action exists (in our case, Run Remediation Script), FortiSIEM must dynamically determine what to do.

In the context of tagging a host running FortiClient with a new tag in FortiEMS, it must determine the following based on the incident data.

1. Which host to tag
2. What tag to use
3. Which FortiEMS credential (which EMS server and authentication) to use.

FortiSIEM can only automatically do all 3 if you've followed the best practices above.

1. Which host to tag
   FortiSIEM looks at the incident source (either hostname or IP address), and if a value can be found, it checks if this device exists in the CMDB.
   If it exists in CMDB, it looks at the device's FortiEMS serial number attribute.
   If incident source is not found, it looks at incident destination (either hostname or IP address). It also checks if the device exists in CMDB and whether it has a FortiEMS serial number attribute.
2. What tag to use
   If the rule contains a tag value, it will read this.
   If the remediation script is executed adhoc by user, you can override this with your own.
3. Which FortiEMS credential (which FortiEMS server and authentication) to use.
   FortiSIEM lists all available FortiEMS Server credentials. Each has an associated serial number attribute.
   If the matching CMDB device found in the incident has a FortiEMS serial number match (This indicates the FortiEMS server it is registered to), it will use the associated credential.

Note: If a user is adhoc executing a FortiEMS remediation script (not automatically), then you can forcefully override the automatically detected host, tag, and credential to use.

Example Scenario

The rule "Traffic to FortiGuard Malware IP List" triggered for a given source device. This source is a Windows machine running FortiClient. This device was previously shallow discovered as unmanaged via a FortiGate firewall. Using this method, we know the FortiEMS serial number of the FortiEMS server it is registered to.

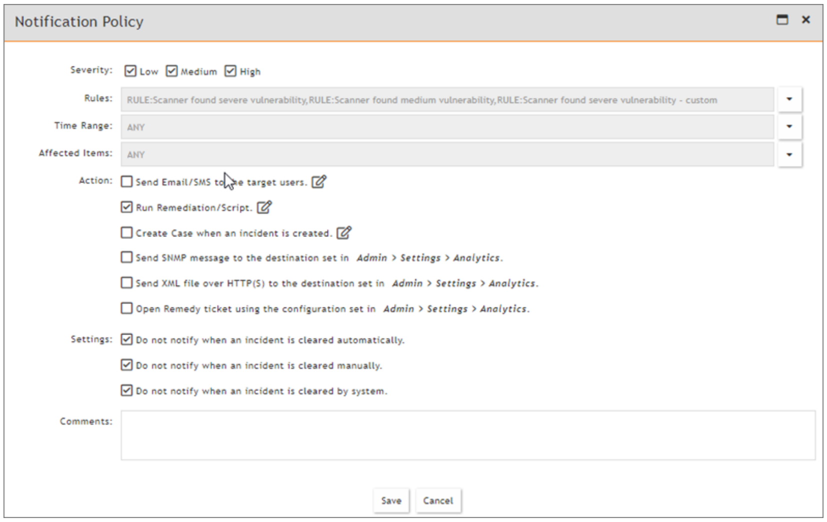
We can assign a tag, either within the rule, or during adhoc execution, such as "suspicious_activity", which will be assigned to the host in FortiEMS. Devices such as Firewalls that implement ZTNA policies based on this tag will take action according to how they are defined.

Action overview: FortiSIEM (tag a host) -> FortiEMS server -> Feed hosts and tag data -> FortiGate firewalls -> Implement ZTNA rules based on certain tags -> Take action if matching devices pass through Firewall.

Scheduling Automatic Tagging Example

You can schedule tagging for certain rules via Notification Policy, see herefor more information. Two example screenshots below provide an illustration of the following:

If any of the 3 rules selected trigger, FortiSIEM will automatically check the incident source or incident target and if the device exists in the FortiEMS server, it will be tagged with the tag "SuspiciousActivity".



Notification Policy

Severity: ☑ Low ☑ Medium ☑ High

Rules: RULE:Scanner found severe vulnerability,RULE:Scanner found medium vulnerability,RULE:Scanner found severe vulnerability - custom

Time Range: ANY

Affected Items: ANY

Action: ☐ Send Email/SMS to the target users.

☑ Run Remediation/Script.

☐ Create Case when an incident is created.

☐ Send SNMP message to the destination set in *Admin > Settings > Analytics*.

☐ Send XML file over HTTP(S) to the destination set in *Admin > Settings > Analytics*.

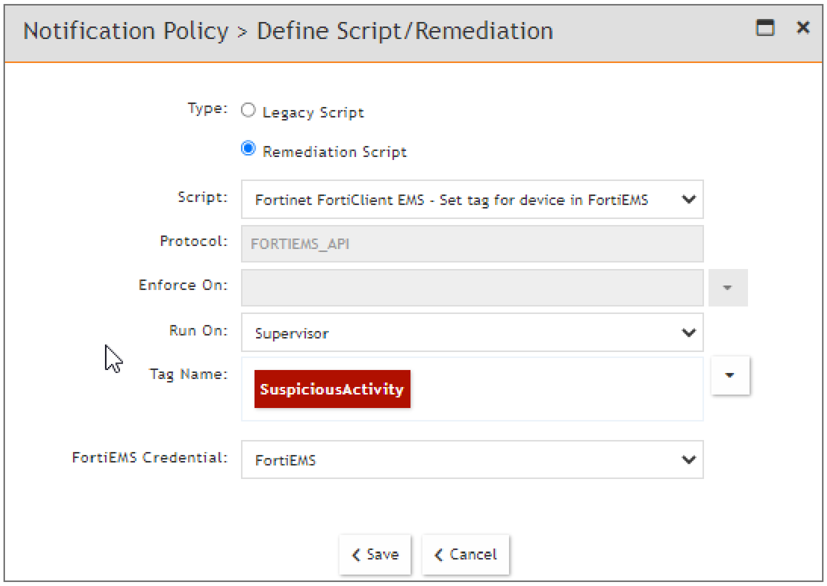
☐ Open Remedy ticket using the configuration set in *Admin > Settings > Analytics*.

Settings: ☑ Do not notify when an incident is cleared automatically.

☑ Do not notify when an incident is cleared manually.

☑ Do not notify when an incident is cleared by system.

Comments:



Notification Policy > Define Script/Remediation

Type: ○ Legacy Script

● Remediation Script

Script: Fortinet FortiClient EMS - Set tag for device in FortiEMS

Protocol: FORTIEMS_API

Enforce On:

Run On: Supervisor

Tag Name: SuspiciousActivity

FortiEMS Credential: FortiEMS

FortiSOAR Integration Notes

For additional information on the FortiSOAR for FortiSIEM Integration solution, see here.

Sample playbooks are available here.

Configuring FortiSOAR for FortiSIEM Integration

To set up FortiSOAR with a role so FortiSIEM integration can occur, take the following steps.

Set Up Authentication

HTTP Basic Authentication for API is used for authentication. A user that FortiSIEM can use to read, execute playbooks and connectors can be created by taking the following steps.

1. Click the Setting icon on top right hand of the FortiSOAR GUI.
2. Select **Roles** on left hand toolbar.
3. Click **Add**.
4. Give the Role a Name. For example, "FortiSIEM-Role".
5. In **Set Role Permissions**, set the following:
    a. For All Modules Except for Users, set to **Read allow**.
    b. Set Connectors to **Read + Execute**.
    c. Set Playbooks to **Read + Execute**.
    d. Click **Save**.
6. Select **Users** on left hand toolbar.
7. Click **Add**.
8. Set the following:
    a. Fill out the **First Name** and **Last Name** fields, such as First Name "FortiSIEM", and "Last Name" User".
    b. For **User Type**, select **Vendor**.
    c. Enter a valid email address, such as `yourname@yourdomain.tld`.
    d. Select your **Desired Team**.
    Note: You must assign the user to a Team in addition to a Role, otherwise authentication for executing playbooks will fail.
    e. For **Select Role**, you can select FortiSIEM-Role for minimal access, or a desired Role.
    f. Under **Authentication**, for **User Type**, select **Application User**.
    g. Under **Authentication**, specify the username. Note, it can be different from the Name display value: fortisiem-user.
    h. Click **Save**. An email will be sent to the email address provided to change the password.
    i. Keep a record of the changed password.

At this point, you can configure FortiSIEM for FortiSOAR Playbooks and FortiSOAR Connectors.

For additional information on the FortiSOAR for FortiSIEM Integration solution, see here.

Sample playbooks are available here. This contains:

- Playbook for getting IP address reputation via VirusTotal
- Playbook for getting Domain reputation via VirusTotal, Anomali, FortiGuard, MX Toolbox, URLVoid, Alienvault OTX
- Playbook for getting URL reputation via VirusTotal, Anomali, FortiGuard, MX Toolbox, URLVoid
- Playbook for getting file hash reputation via VirusTotal

Writing FortiSIEM Compatible FortiSOAR Playbooks

Introduction

Starting with 6.4.0, FortiSIEM provides the capability to adhoc execute FortiSOAR Playbooks and Connectors from the **INCIDENTS** page for individual incidents, or from the **ANALYTICS** page for individual events.

When FortiSIEM executes a Playbook, it provides the entire set of incident or raw event data , depending on execution from the **INCIDENTS** or **ANALYTICS** page respectively, as an argument to the Playbook in JSON format. The Playbook operates on that data, execute some actions, and returns the result to FortiSIEM.

For additional information on the FortiSOAR for FortiSIEM Integration solution, see here.

Sample playbooks are available here. This contains:

- Playbook for getting IP address reputation via VirusTotal
- Playbook for getting Domain reputation via VirusTotal, Anomali, FortiGuard, MX Toolbox, URLVoid, Alienvault OTX
- Playbook for getting URL reputation via VirusTotal, Anomali, FortiGuard, MX Toolbox, URLVoid
- Playbook for getting file hash reputation via VirusTotal

Prerequisites

In order to better understand the information here, it is recommended that you read the latest reference FortiSOAR **Playbooks Guide** under **Reference Manuals** first located here.

FortiSOAR Playbooks heavily use Jinja Templates. It is imperative that the Jinja template syntax is understood to design useful Playbooks. Jinja template designer documentation can be referenced here: https://jinja.palletsprojects.com/en/3.0.x/templates/

Playbooks and Connectors

A Playbook in FortiSOAR is a workflow that can be executed manually or automatically to complete some action within FortiSOAR itself, or to systems and applications in your environment. Playbooks can do entire chains of actions, while Connectors complete just one action at a time.

A Connector in FortiSOAR is an individual component integration to various FortiSOAR supported products. Playbooks can call multiple Connectors to create complex tasks. Every Connector can support one or more actions.

For example the Fortinet – FortiOS Connector can do the following actions on a FortiGate firewall, and return the response data to you:

- Get Policy
- Get Address Group
- Get Blocked IP Addresses
- Get Blocked URLs

- Get Web Filter Profiles
- Block IP Address
- Block URL
- Unblock URL
- Unblock IP Address
- Purge IP Block List
- Execute Command

You can adhoc execute a Connector from FortiSIEM, supplying the necessary arguments for any given action. The arguments required vary based on the action being completed.

Some examples of a Playbook with respect to FortiSIEM:

- An incident triggers in FortiSIEM, and you would like FortiSOAR to take that incident data, and do a reputation lookup of all the public IPs found in that incident.
- An incident triggers in FortiSIEM, and you would like FortiSOAR to generate an Alert on FortiSOAR, and block the source IP found in the incident on a specific firewall in your network for 24 hours.
- A raw event is observed in FortiSIEM on the **ANALYTICS** page by a security analyst, who decides to execute a Playbook that takes the following actions:
  - Disables the user observed in the event in Active Directory.
    and
  - Sends an email to the security team.

Some examples of a Connector execution from FortiSIEM:

- A security analyst observes a malicious IP in an incident, and executes a connector to block the IP on a firewall as a singular action.
- A security analyst observes suspicious behavior from a given user account in Active Directory, and executes the **Active Directory > Disable User Account** action on the account until further inspection can be completed.

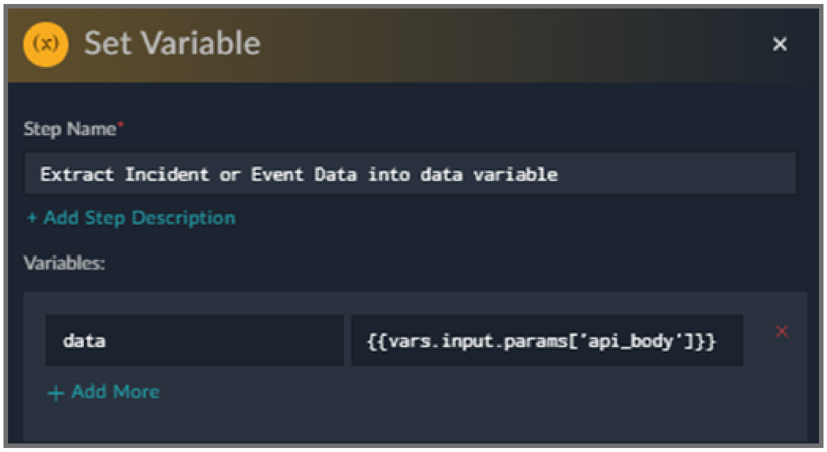
Jinja and its Use in Playbooks

Jinja is a templating engine that can be used to build complex documents dynamically. FortiSOAR uses this in their Playbook design interface so you can process variable data sent to or from various functions, utilities, or connectors.

There are a few kinds of delimiters. The default Jinja delimiters are configured as follows:

- `{% ... %}` for Statements
- `{{ ... }}` for Expressions to print to the template output
- `{# ... #}` for Comments not included in the template output

For example, in a FortiSOAR Playbook, the Set Variable Action can use the `{{…}}` expression to assign the FortiSIEM JSON data into a list variable called data.



Step Name*

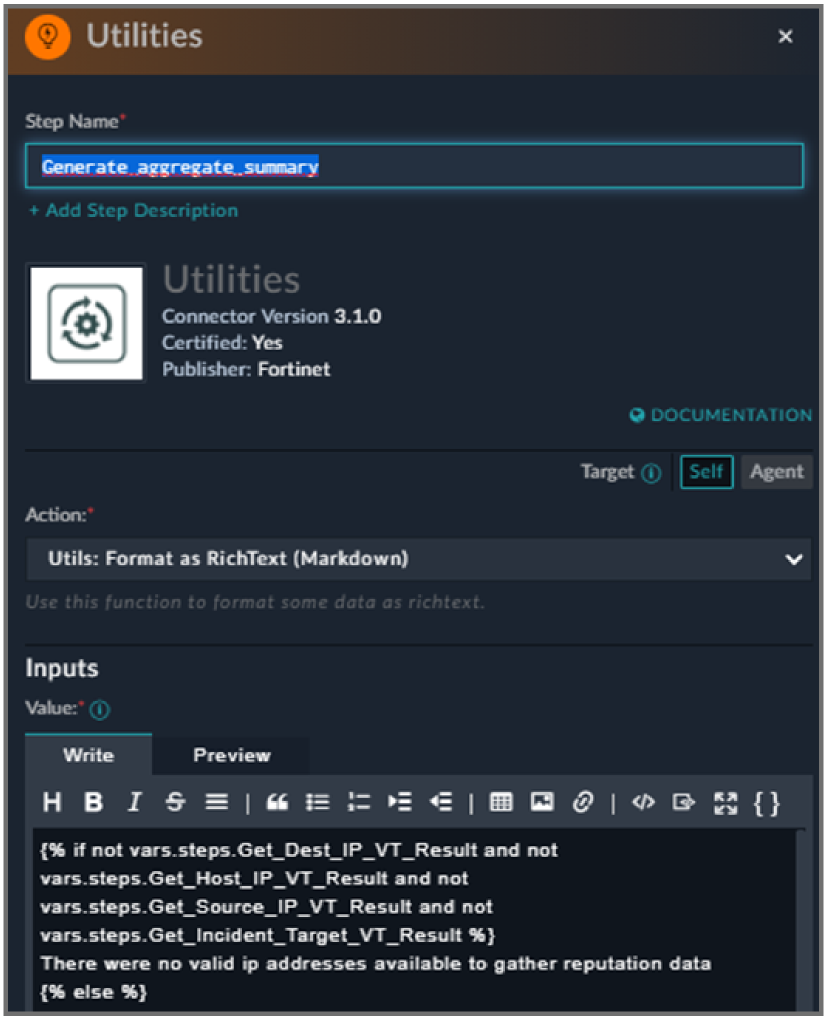
Extract Incident or Event Data into data variable

Variables:

data	{{vars.input.params['api_body']}}

For another example, using the step function Utility -> Format as RichText (Markdown), you can format a variable as a string of text, but use statements to only display text if certain conditions match.

The example here will only display the string “There were no valid ip addresses available to gather reputation data” if the following variables do not exist:



Step Name*

Generate_aggregate_summary

Utilities

Connector Version 3.1.0

Certified: Yes

Publisher: Fortinet

Action:*

Utils: Format as RichText (Markdown)

Use this function to format some data as richtext.

Inputs

Value:*

```
{% if not vars.steps.Get_Dest_IP_VT_Result and not
vars.steps.Get_Host_IP_VT_Result and not
vars.steps.Get_Source_IP_VT_Result and not
vars.steps.Get_Incident_Target_VT_Result %}
There were no valid ip addresses available to gather reputation data
{% else %}
```

If the 4 variables named above do not exist, a single line of text explains no result data was found, otherwise the rest of the data after the `{% else %}` statement is processed.

Building Custom Playbooks

With Playbooks you can build anything you like to complete any action.

As FortiSIEM incidents are generated, or raw events are parsed from various products, they each provide concrete sets of data to act on, either completing enrichment (looking up reputations), or taking some action such as disabling a user.

FortiSIEM sends this data over to a given Playbook in JSON format.

The FortiSIEM incident is in the following JSON format when supplied to a Playbook. The playbook can access argument data from FortiSIEM in the JSON variable `{{vars.input.params['api_body']}}`

Sample Incident JSON

```
    {
          "user": null,
          "count": 30,
          "srcName": null,
          "tagName": null,
          "customer": null,
          "destName": null,
          "hostName": null,
          "phCustId": 1,
          "procName": null,
          "resource": null,
          "eventName": null,
          "eventType": "PH_RULE_DNS_THREATSTREAM_MALWARE_DOMAIN",
          "srcGeoOrg": null,
          "srcIpAddr": "192.0.2.0",
          "bizService": null,
          "destGeoOrg": null,
          "destIpAddr": null,
          "hostGeoOrg": null,
          "hostIpAddr": null,
          "incidentId": 993,
          "phRecvTime": 1634249820000,
          "reptGeoOrg": null,
          "srcGeoCity": null,
          "destGeoCity": null,
          "hostGeoCity": null,
          "incidentSrc": "srcIpAddr:192.0.2.0,",
          "rawEventMsg": null,
          "reptGeoCity": null,
          "srcGeoState": null,
          "activityName": null,
          "attackTactic": "Exfiltration",
          "destGeoState": null,
          "hostGeoState": null,
          "incidentReso": 1,
          "reptGeoState": null,
          "eventSeverity": 9,
          "incidentCount": 30,
          "incidentRptIp": "198.51.100.0",
          "incidentTitle": "DNS Traffic from 192.0.2.0 to Threat Stream Malware Domain
    example.net",
          "srcGeoCountry": null,
          "destGeoCountry": null,
          "hostGeoCountry": null,
          "incidentDetail": "",
          "incidentStatus": 0,
          "incidentTarget": "destName:example.net,",
          "reptGeoCountry": null,
          "srcGeoLatitude": null,
          "attackTechnique": "[{\"name\":\"Exfiltration Over Alternative Protocol:
    Exfiltration Over Symmetric Encrypted Non-C2 Pro-
    tocol\",\"techniqueid\":\"T1048.001\"}]",
          "destGeoLatitude": null,
          "hostGeoLatitude": null,
          "incidentExtUser": null,
          "incidentTagName": null,
          "phEventCategory": 1,
          "reptGeoLatitude": null,
          "srcGeoLongitude": null,
          "destGeoLongitude": null,
          "eventSeverityCat": "HIGH",
          "hostGeoLongitude": null,
          "incidentComments": "test comment\n\n",
          "incidentLastSeen": 1634249820000,
          "incidentTicketId": null,
          "reptGeoLongitude": null,
          "attackTechniqueId": "T1048.001",
          "incidentFirstSeen": 1627508130000,
          "incidentNotiStatus": null,
          "incidentRptDevName": "HOST-198.51.100.0",
          "incidentTicketUser": null,
          "incidentViewStatus": 1,
          "phIncidentCategory": null,
          "incidentClearedTime": 0,
          "incidentClearedUser": null,
          "incidentExtTicketId": null,
          "incidentRptDevStatus": 1,
          "incidentTicketStatus": 6,
          "incidentClearedReason": null,
          "incidentExtTicketType": null,
          "phSubIncidentCategory": null,
          "incidentExtClearedTime": null,
          "incidentExtTicketState": null,
          "incidentNotiRecipients": ""
        }
```

Please note that depending on the type of FortiSIEM incident that fired, and the data used to populate that incident, the fields will contain various values. Your playbook must properly handle situations such as a field you need is blank, or properly extract data from a field that contains multiple values.

Similar to FortiSIEM Incidents, when executing a playbook on a FortiSIEM raw event, an entire copy of the parsed event attributes for that event is sent in JSON format, which looks like the following.

Sample Event JSON

```
{
    "count": "1",
    "opName": "New-InboxRule",
    "status": "True",
    "userId": "test.user@example.com",
    "eventId": "8263823841277690829",
    "srcName": "HOST-192.0.2.22",
    "customer": "Super",
    "phCustId": 1,
    "ruleName": "For all messages from test@email.com",
    "eventName": "create Inbox rules in mailboxes. Inbox rules process messages in the
Inbox based on conditions and take actions such as moving a message to a specified
folder or deleting a message",
    "eventType": "MS_OFFICE365_Exchange_New-InboxRule",
    "reptModel": "Office365",
    "srcIpAddr": "203.0.113.0",
    "srcIpPort": 11022,
    "deviceTime": 1624869759000,
    "parserName": "Office365Parser",
    "phRecvTime": 1635195584000,
    "reptVendor": "Microsoft",
    "srcGeoCity": "Cheshunt",
    "collectorId": "1",
    "eventSource": "Exchange",
    "reptDevName": "HOST-198.51.100.24",
    "srcGeoState": "England",
    "timeSkewSec": "10325825",
    "eventParsedOk": 1,
    "eventSeverity": 7,
    "reptDevIpAddr": "198.51.100.24",
    "srcGeoCountry": "United Kingdom of Great Britain and Northern Ireland",
    "relayDevIpAddr": "198.51.100.24",
    "senderMailAddr": "nobody@example.com",
    "srcGeoLatitude": "51.69989",
    "phEventCategory": "0 (External)",
    "srcGeoLongitude": "-0.02849",
    "eventRuleTrigger": 1,
    "eventSeverityCat": "MEDIUM",
    "extEventRecvProto": "Syslog",
    "office365UserType": "2 (An administrator)",
    "office365RecordType": "1 (ExchangeAdmin - Events from the Exchange admin audit
log)",
    "stopProcessingRules": "True",
    "srcGeoCountryCodeStr": "GB"
  }
```

Please also note that the contents in the event will vary based on the source. The fields present in a Firewall session log are not the same as a Windows login event, and certain attributes are not guaranteed to always be present, which is vendor dependent. Your Playbooks should properly handle edge cases where expected values are not present when the Playbook is called.

When a Playbook is executed, the FortiSIEM argument data is accessible in the following variable:

```
{{vars.input.params['api_body']}}
```

You are then free to parse that JSON data into its individual attributes to complete an action. These attribute names in the JSON match the programmatic attribute names in FortiSIEM. These can be observed in the FortiSIEM UI by navigating to **ADMIN > Device Support > Event Attributes**.

Below are some common attributes.

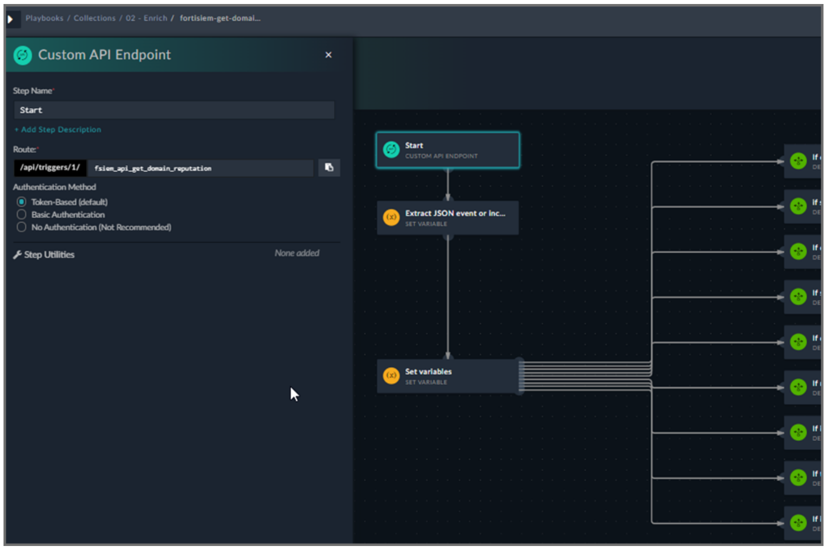
Sample Attribute Names

```
{
    "eventType": "PH_RULE_DNS_THREATSTREAM_MALWARE_DOMAIN",
    "srcIpAddr": "192.0.2.0",
    "destIpAddr": "203.0.113.0",
    "incidentSrc": "srcIpAddr:192.0.2.0,",
    "attackTactic": "Exfiltration",
    "eventSeverity": 9,
    "incidentCount": 30,
    "incidentRptIp": "198.51.100.0",
    "incidentTitle": "DNS Traffic from 192.0.2.0 to Threat Stream Malware Domain westlady.net",
    "incidentTarget": "destName:westlady.net,",
    "attackTechnique": "[{\"name\":\"Exfiltration Over Alternative Protocol: Exfiltration Over Symmetric Encrypted Non-C2 Protocol\",\"techniqueid\":\"T1048.001\"}]",
    "eventSeverityCat": "HIGH",
    "incidentRptDevName": "HOST-198.51.100.0"
}
```

Custom Playbook Requirements - API Endpoint Specification

FortiSIEM compatible Playbooks all start with a Step type called “Custom API Endpoint”. FortiSOAR then creates a URI for that specific Playbook that can be called.

Example:



Playbooks / Collections / 02 - Enrich / fortisiem-get-domai...
Start
CUSTOM API ENDPOINT
Extract JSON event or inc...
SET VARIABLE
Set variables
SET VARIABLE

Custom API Endpoint ×

Step Name*

Start

+ Add Step Description

Route:*

/api/triggers/1/ fsiem_api_get_domain_reputation

Authentication Method

● Token-Based (default)
○ Basic Authentication
○ No Authentication (Not Recommended)

Step Utilities None added

The get domain reputation Playbook creates a route called "/api/triggers/1/fsiem_api_get_domain_reputation".

Authentication Method: Token-Based

FortiSIEM can then make API calls to this endpoint in the format

`https://<`*`fortisoar-hostname`*`>/api/triggers/1/fsiem_api_get_domain_reputation`

FortiSIEM Prebuilt Playbooks

FortiSIEM and FortiSOAR teams have provided a content pack installable in your FortiSOAR system with the following Playbooks, which are commonly used, but can also be a building block for your own custom Playbooks.

Content Pack Playbooks

- fortisiem-get-domain-reputation
- fortisiem-get-hash-reputation
- fortisiem-get-url-reputation
- fortisiem-get-ip-reputation-summary

Reference Playbooks

To support complex tasks completed by the above Playbooks, the following Playbooks are not called directly, and are only used by the above Playbooks (nested Playbooks) – Do not delete them, but do not call them directly.

- fortisiem-reference-get-domain-rep
- fortisiem-reference-get-hash-reputation
- fortisiem-reference-get-url-rep
- fortisiem-reference-validate-ip
- fortisiem-reference-virustotal-summary

The naming convention of the playbooks are as follows:

<system>-<call method>-<purpose>

fortisiem – Indicates this is a Playbook for use by FortiSIEM only. Within the FortiSIEM UI, you can execute these Playbooks.

get or reference – get indicates this Playbook can be called by FortiSIEM. Reference indicates it is a reference Playbook and not called directly. **Never call a “reference” Playbook from FortiSIEM, these reference Playbooks are only called automatically from other Playbooks.

Playbook Tagging

It is **required** that every FortiSOAR Playbook that is designed to work with, and be called by FortiSIEM, should have a Playbook tag called “**FortiSIEM**” in case sensitive format. FortiSIEM may filter for Playbooks tagged in this way to avoid polling a list of all possible Playbooks.

Formatting Playbook Result Data back to FortiSIEM

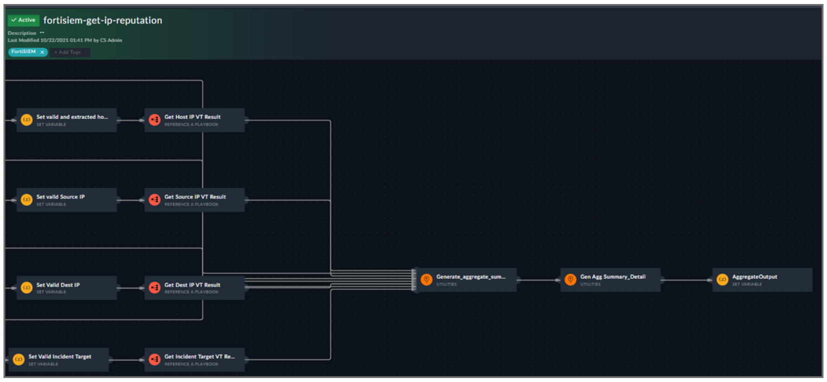
Once FortiSIEM has successfully executed a FortiSOAR Playbook, and supplied either Incident or Raw event JSON data for the Playbook to operate on, it will wait for a JSON response.

This response data is dynamically configured within your Playbook. You can return any variables you’d like, but there are a few special variables that you should standardize in your Playbooks that FortiSIEM will display in the results screen.

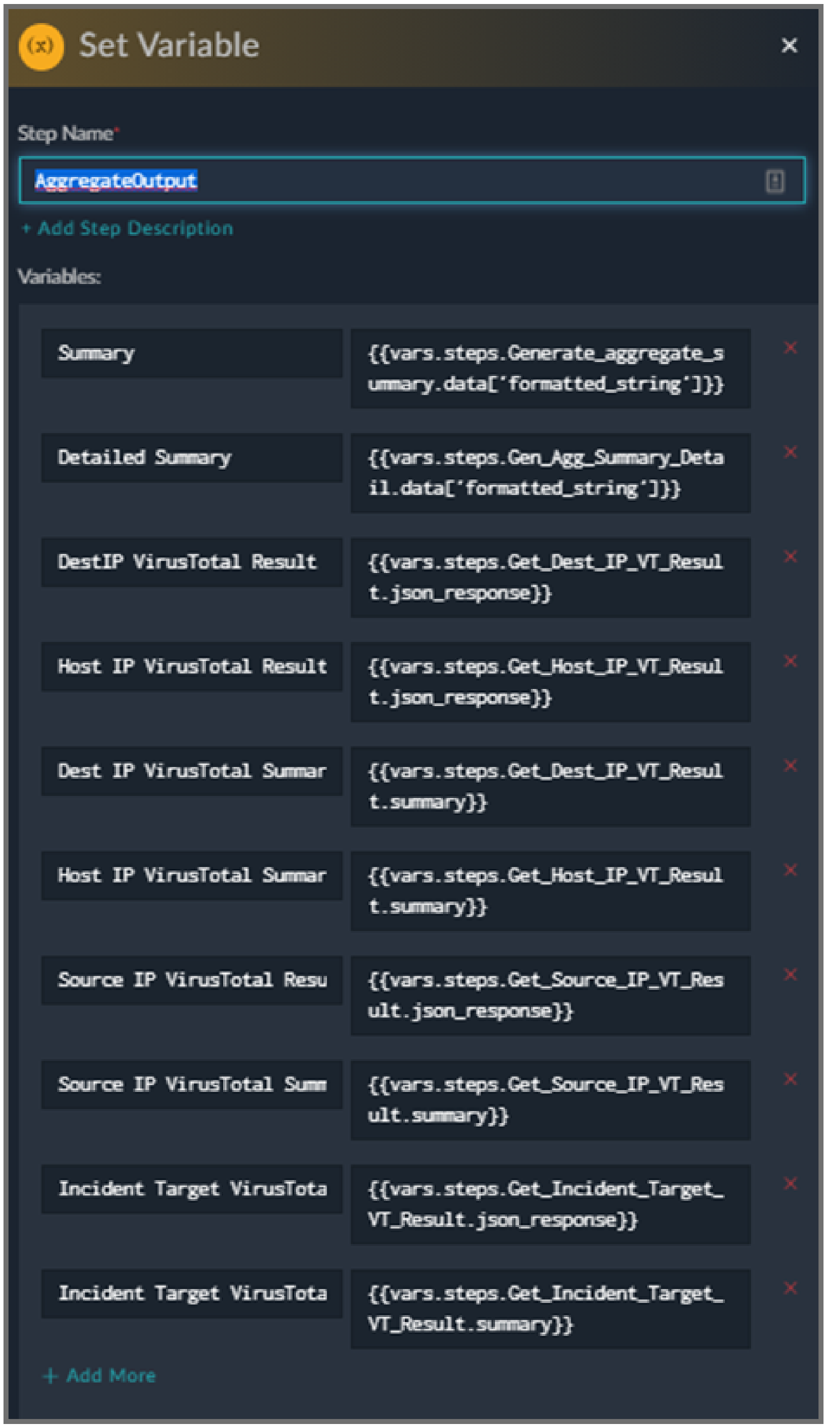
FortiSIEM Special Playbook Response Variables

- Summary – A string variable that shows high level result data from the execution of your Playbook. Short and high level.
- Details – A string variable that shows detailed result data that may be more verbose.

For a demonstration, take a look at the Playbook: fortisiem-get-ip-reputation



We have a final Set Variable step called “AggregateOutput” where we format resulting variables.



Step Name*

AggregateOutput

Variables:

Summary	{{vars.steps.Generate_aggregate_summary.data['formatted_string']}}
Detailed Summary	{{vars.steps.Gen_Agg_Summary_Detail.data['formatted_string']}}
DestIP VirusTotal Result	{{vars.steps.Get_Dest_IP_VT_Result.json_response}}
Host IP VirusTotal Result	{{vars.steps.Get_Host_IP_VT_Result.json_response}}
Dest IP VirusTotal Summar	{{vars.steps.Get_Dest_IP_VT_Result.summary}}
Host IP VirusTotal Summar	{{vars.steps.Get_Host_IP_VT_Result.summary}}
Source IP VirusTotal Resu	{{vars.steps.Get_Source_IP_VT_Result.json_response}}
Source IP VirusTotal Summ	{{vars.steps.Get_Source_IP_VT_Result.summary}}
Incident Target VirusTota	{{vars.steps.Get_Incident_Target_VT_Result.json_response}}
Incident Target VirusTota	{{vars.steps.Get_Incident_Target_VT_Result.summary}}

We have a string formatting step result that is stored in a variable called “Summary”. FortiSIEM simply takes this particular variable and displays it prominently in the response UI for display and saving.

We also have a string formatting step result that is stored in a variable called “Detailed Summary”. As the name suggests, it is meant for more verbose data.

Only “Summary” should be considered a mandatory set variable, the others are optional and can be viewed in the GUI.

References

Playbooks Guide: https://docs.fortinet.com/document/fortisoar/7.0.2/playbooks-guide

Connector Guide: https://docs.fortinet.com/document/fortisoar/7.0.2/connectors-guide

Jinja Template Designer Documentation: https://jinja.palletsprojects.com/en/3.0.x/templates/

Functions in Analytics

These functions are only available for ClickHouse and Elasticsearch Queries. See the full description link from the table for limitations of nesting operations.There is no support for EventDB queries and rules.

The following functions are available:

Type	Functions
Aggregate Functions	AVG, COUNT, COUNT DISTINCT, FIRST, LAST, MAX, MEDIAN, MIN, MODE, PctChange, PCTILE, Pctile95, STDDEV, SUM, VARIANCE
CMDB Lookup Function	DeviceToCMDBAttr
Conversion Functions	LOG, TO_DOUBLE, TO_INTEGER, TO_STRING
Date Conversion Functions	DayOfWeek, HourOfDay
Evaluate-and-Set Function	IF
Extraction Function	EXTRACT
LookupTable Functions	LookuptableGet, LookupTableHas
String Manipulation Functions	LEN, LTRIM, REPLACE, RTRIM, SUB_STR, TO_LOWER, TO_UPPER, TRIM, URL_DECODE
Time Window Functions	EMA, SMA

Aggregate Functions

Details of the following aggregate functions are available.

- AVG
- COUNT

- COUNT DISTINCT
- FIRST
- LAST
- MAX
- MEDIAN
- MIN
- MODE
- PctChange
- PCTILE
- Pctile95
- STDDEV
- SUM
- VARIANCE

AVG Function

AVG(<field>) returns the average of the values of the numerical field in all events matching the query criteria.

Syntax

AVG(<eventAttribute>) - eventAttribute must be a numerical type.

AVG (Function(<eventAttribute>)) – The *Function* must return a numerical value.

In Elasticsearch, these nested function categories are allowed:

- *Conversion Functions, Evaluate-and-Set Function, Extraction Function, String Manipulation Functions*
  ***Notes**: LOG not allowed in Conversion Functions, only LEN allowed in String Manipulation Functions*

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, Date Conversion Functions, Evaluate-and-Set Function, String Manipulation Functions*
  Note: *Only LEN allowed in String Manipulation Functions*

Scope

AVG() is available in EventDB, ClickHouse and Elasticsearch. Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Example

eventType	srcIpAddr	sentBytes
E1	10.1.1.1	10
E2	10.1.1.1	20
E3	10.1.1.2	30

```
AVG (sentBytes) = 20
```

With a Group By on srcIpAddr:

srcIpAddr	AVG(sentBytes)
10.1.1.1	15.5
10.1.1.2	30

COUNT Function

COUNT(*) returns the number of occurrences of each matched row in a query. *COUNT(<eventAttribute>)* counts the number of occurrences of the event attribute in a query.

Syntax

COUNT(*) or *COUNT(<eventAttribute>)* or *COUNT(Function(<eventAttribute>))*

In Elasticsearch, these nested function categories are allowed:

- *Extraction Function*

In ClickHouse, these nested function categories are allowed:

- *Extraction Function*

Scope

COUNT is available in EventDB, ClickHouse and Elasticsearch queries and rules. Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Example

eventType	srcIpAddr	user
E1	10.1.1.1	Bob
E2		Alice
E3	10.1.1.2	

```
COUNT (eventType) = 3
```

```
COUNT (srcIpAddr) = 2
```

```
COUNT(user) = 2
```

COUNT DISTINCT Function

COUNT DISTINCT(<field>) returns the number of *distinct* occurrences of the field in all events matching the query criteria.

Syntax

COUNT (DISTINCT <eventAttribute>), COUNT(DISTINCT Function(<eventAttribute>))

In Elasticsearch, these nested unction categories are allowed:

- *Extraction Function*

In ClickHouse, these nested function categories are allowed:

- *Extraction Function*

Scope

COUNT DISTINCT is available in EventDB, ClickHouse and Elasticsearch queries and rules. Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Example

eventType	srcIpAddr	user
E1	10.1.1.1	Bob
E2	10.1.1.1	Alice
E3	10.1.1.2	Bob

```
COUNT DISTINCT (eventType) = 3
```

```
COUNT DISTINCT (srcIpAddr) = 2
```

```
COUNT DISTINCT (user) = 2
```

FIRST Function

FIRST(<eventAttribute>) returns the value of the <eventAttribute> in the event with *earliest***phRecvTime** among all events matching the query criteria. Note that for every event, **phRecvTime** attribute is set to the time at which the event was first received at any FortiSIEM node (Collector, Worker or Supervisor).

Syntax

FIRST (<eventAttribute>) or *FIRST (FUNCTION(<eventAttribute>))*

In Elasticsearch, nested functions are not allowed.

In ClickHouse, these nested function categories are allowed:

- *Extraction Function, Evaluate-and-Set Function*

Scope

FIRST() is available in EventDB, ClickHouse and Elasticsearch.

Example

Time	Event Type	user	loginTime
T1	Login Success	Alice	T5
T1+1	Login Success	Bob	T6

Time	Event Type	user	loginTime
T1+2	Login Success	Bob	T7
T1+3	Login Success	Carl	T6

With a group By on user, then

user	FIRST(loginTime)
Alice	T5
Bob	T6
Carl	T6

LAST Function

LAST(<eventAttribute>) returns the value of the <eventAttribute> in the event with latest **phRecvTime** among all events matching the query criteria. Note that for every event, **phRecvTime** attribute is set to the time at which the event was first received at any FortiSIEM node.

Syntax

LAST(<eventAttribute>) or *LAST(FUNCTION(<eventAttribute>))*

In Elasticsearch, nested functions are not allowed.

In ClickHouse, these nested function categories are allowed:

- *Extraction Function, Evaluate-and-Set Function*

Scope

LAST() is available in EventDB, ClickHouse and Elasticsearch for all releases.

Example

Time	Event Type	user	loginTime
T1	Login Success	Alice	T5
T1+1	Login Success	Bob	T6
T1+2	Login Success	Bob	T7
T1+3	Login Success	Carl	T6

With a group By on user, then

user	LAST(loginTime)
Alice	T5

user	LAST(loginTime)
Bob	T7
Carl	T6

MAX Function

MAX(<field>) returns the maximum of the values of the numerical field in all events matching the query criteria.

Syntax

MAX(<eventAttribute>) - eventAttribute must be a numerical type.

MAX (Function(<eventAttribute>)) – The *Function* must return a numerical value.

In Elasticsearch, these nested function categories are allowed:

- *Conversion Functions, Evaluate-and-Set Function, Extraction Function, String Manipulation Functions*
  Notes: *LOG not allowed in Conversion Functions, only LEN allowed in String Manipulation Functions,*

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, Date Conversion Functions, Evaluate-and-Set Function, String Manipulation Functions*
  Note: *Only LEN allowed in String Manipulation Functions*

Scope

MAX() is available in EventDB, ClickHouse and Elasticsearch. Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Example

eventType	srcIpAddr	sentBytes
E1	10.1.1.1	10
E2	10.1.1.1	20
E3	10.1.1.2	30

```
MAX (sentBytes) = 30
```

With a Group By on srcIpAddr:

srcIpAddr	MAX(sentBytes)
10.1.1.1	20
10.1.1.2	30

MEDIAN Function

MEDIAN(<field>) returns the value lying at the midpoint of a frequency distribution of observed values of the field in all events matching the query criteria. In other words, it is the middle number in a sorted, ascending or descending list of the values.

Syntax

MEDIAN(<eventAttribute>) - eventAttribute must be a numerical type.

MEDIAN(Function(<eventAttribute>)) – The *Function* must return a numerical value.

In Elasticsearch, these nested function categories are allowed:

- *Conversion Functions, Evaluate-and-Set Function, Extraction Function, String Manipulation Functions*
  Notes: *LOG not allowed in Conversion Functions, only LEN allowed in String Manipulation Functions*

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, Date Conversion Functions, Evaluate-and-Set Function, Extraction Function*
  Note: *Only LEN allowed in String Manipulation Functions*

Scope

MEDIAN() is available in ClickHouse and Elasticsearch from release 7.0.0 onwards. Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Example

Time	hostName	cpuUtil (%)	memUtil(%)
T1	Host1	2.58	1.33
T2	Host1	0.00	0.07
T3	Host1	0.04	0.00
T4	Host1	0.02	1.16

```
MEDIAN(cpuUtil) = 0.66
```

```
MEDIAN(memUtil) = 0.64
```

MIN Function

MIN(<field>) returns the minimum of the values of the numerical field in all events matching the query criteria.

Syntax

MIN(<eventAttribute>) - eventAttribute must be a numerical type.

MIN (Function(<eventAttribute>)) – The *Function* must return a numerical value.

In Elasticsearch, these nested function categories are allowed:

- *Conversion Functions, Evaluate-and-Set Function, Extraction Function, String Manipulation Functions*
  Notes: *LOG not allowed in Conversion Functions, Only LEN allowed in String Manipulation Functions*

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, Date Conversion Functions, Evaluate-and-Set Function*
  Note: *Only LEN allowed in String Manipulation Functions*

Scope

MIN() is available in EventDB, ClickHouse and Elasticsearch. Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Example

eventType	srcIpAddr	sentBytes
E1	10.1.1.1	10
E2	10.1.1.1	20
E3	10.1.1.2	30

```
SUM (sentBytes) = 10
```

With a Group By on srcIpAddr:

srcIpAddr	MIN(sentBytes)
10.1.1.1	10
10.1.1.2	30

MODE Function

MODE(<field>) returns the value that appears most frequently in the field among all events matching the query criteria.

Syntax

MODE(<eventAttribute>) or *MODE (Function(<eventAttribute>))*

In Elasticsearch, these nested function categories are allowed:

- *Evaluate-and-Set Function, Extraction Function*

In ClickHouse, these nested function categories are allowed:

- *Date Conversion Functions, Evaluate-and-Set Function, Extraction Function*

Scope

MODE() is available in ClickHouse and Elasticsearch from release 7.0.0 onwards. Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Example

Identify the most common source IP address for each user.

Time	Event Type	user	srcIpAddr
T1	Login Success	Alice	10.1.1.1
T2	Login Success	Bob	10.1.1.2
T3	Login Success	Bob	10.1.1.2
T4	Login Success	Carl	10.1.1.3

```
MODE(srcIpAddr) = 10.1.1.2
```

```
MODE(user) = Bob
```

With a group By on user, then

user	MODE(srcIpAddr)
Alice	10.1.1.1
Bob	10.1.1.2
Carl	10.1.1.3

Restrictions

1. HAVING clause not supported.
2. Trend displayed only if X in MODE(X) is a numeric value.

PctChange Function

PctChange(<eventAttribute >) returns the percentage change of the numerical < *eventAttribute* > from the first event and the last event among all events matching the query criteria.

Syntax

PctChange(<eventAttribute>) - *eventAttribute* must be a numerical type.

In Elasticsearch, these nested function categories are allowed:

- *Conversion Functions*

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, Evaluate-and-Set Functions*

Scope

Available for EventDB, ClickHouse and Elasticsearch queries.

Example

Consider the following set of events matching the query conditions:

phEventRecvTime (ascending)	hostName	cpuUtil
T1	Host1	10
T2	Host1	20
T3	Host1	30
T4	Host1	40

Then `PctChange (cpuUtil) = (40-10)/10 * 100 = 300%`

PCTILE Function

PCTILE(N,<field>) returns Nth percentile value of the numeric valued <field> in all events matching the query criteria. N is between 0 and 100. This generalizes the Pctile95() function found in earlier releases.

Syntax

PCTILE (N,<eventAttribute>) - *eventAttribute* must be a numerical type.

PCTILE (N,Function(<eventAttribute>)) – The *Function* must return a numerical value.

In Elasticsearch, these nested function categories are allowed:

- *Conversion Functions, Extraction Function, String Manipulation Functions*
  Notes: *LOG not allowed in Conversion Functions, only LEN allowed in String Manipulation Functions*

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, String Manipulation Functions*
  Note: *Only LEN allowed in String Manipulation Functions*

Scope

Available for ClickHouse and Elasticsearch queries from release 7.0.0 onwards.

Example

hostName	diskName	cpuUtil	diskUtil
Host1	Disk1	2.58%	20.98%
Host1	Disk1	0.00%	19.09%
Host1	Disk1	0.04%	3.21%
Host1	Disk1	0.02%	1.02%

```
PCTILE(95,cpuUtil) = 2.58
```

```
PCTILE(95,diskUtil) = 20.98
```

Pctile95 Function

Pctile95(<field>) returns the 95th percentile value of the numeric valued <field> in all events matching the query criteria.

Syntax

Pctile95(<eventAttribute) - eventAttribute must be a numerical type.

In Elasticsearch, these nested function categories are allowed:

- *Conversion Functions, Extraction Function, String Manipulation Functions*
  Notes: *LOG not allowed in Conversion Functions, only LEN allowed in String Manipulation Functions*

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, String Manipulation Functions*
  Note: *Only LEN allowed in String Manipulation Functions*

Scope

Available for EventDB, ClickHouse and Elasticsearch queries.

Example

hostName	intfName	intfUtil
Host1	Wan	2.58
Host1	Wan	0.00
Host1	Wan	0.04
Host1	Wan	0.02

```
PCTILE(95,intfUtil) = 2.58
```

STDDEV Function

STDDEV(<field>) returns the *standard deviation* of the values of the numerical valued field among all events matching the query criteria. *STDDEV(<field>)* is the square root of *VARIANCE(<field>)* defined below.

Syntax

STDDEV (<eventAttribute>) - eventAttribute must be a numerical type.

STDDEV (Function(<eventAttribute>)) – The *Function* must return a numerical value.

In Elasticsearch, these nested function categories are allowed:

- *Conversion Functions, Extraction Function, Evaluate-and-Set Function, String Manipulation Functions*
  Notes: *LOG not allowed in Conversion Functions, only LEN allowed in String Manipulation Functions*

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, Date Conversion Functions, Evaluate-and-Set Function, Extraction Function, String Manipulation Functions*
  Note: *Only LEN allowed in String Manipulation Functions*

Scope

Works for ClickHouse and Elasticsearch queries from release 7.0.0 onwards.

Example

Time	hostName	cpuUtil	memUtil
T1	Host1	2.58	1.33
T2	Host1	0.00	0.07
T3	Host1	0.04	0.00
T4	Host1	0.02	1.16

```
STDDEV(cpuUtil) = 1.1086
```

```
STDDEV(memUtil) = 0.6084
```

SUM Function

SUM(<field>) returns the sum of the values of the numerical field in all events matching the query criteria.

Syntax

SUM(<eventAttribute>) - eventAttribute must be a numerical type.

SUM (Function(<eventAttribute>)) – The *Function* must return a numerical value.

In Elasticsearch, these nested function categories are allowed:

- *Conversion Functions, Evaluate-and-Set Function, Extraction function, String Manipulation Functions*
  Notes: *LOG not allowed in Conversion Functions, only LEN allowed in String Manipulation Functions*

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, Date Conversion Functions, Evaluate-and-Set Function, String Manipulation Functions*
  Note: *Only LEN allowed in String Manipulation Functions*

Scope

SUM is available in EventDB, ClickHouse and Elasticsearch. Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Example

eventType	srcIpAddr	sentBytes
E1	10.1.1.1	10

eventType	srcIpAddr	sentBytes
E2	10.1.1.1	20
E3	10.1.1.2	30

```
SUM (sentBytes) = 60
```

With a Group By on srcIpAddr:

srcIpAddr	SUM(sentBytes)
10.1.1.1	30
10.1.1.2	30

VARIANCE Function

VARIANCE(<field>) returns the *variance* of the values of the numerical valued <field> among all events matching the query criteria.

Syntax

VARIANCE (<eventAttribute>) - eventAttribute must be a numerical type.

VARIANCE (Function(<eventAttribute>)) – The *Function* must return a numerical value.

In Elasticsearch, these nested function categories are allowed:

- *Conversion Functions, Evaluate-and-Set Function, Extraction Function, String Manipulation Functions*
  Notes: *LOG not allowed in Conversion Functions, only LEN allowed in String Manipulation Functions*

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, Date Conversion Functions, Evaluate-and-Set Function, String Manipulation Functions*
  Note: *Only LEN allowed in String Manipulation Functions*

Scope

Works for ClickHouse and Elasticsearch queries from release 7.0.0 onwards.

Example

Time	hostName	cpuUtil	memUtil
T1	Host1	2.58	1.33
T2	Host1	0.00	0.07
T3	Host1	0.04	0.00
T4	Host1	0.02	1.16

```
VARIANCE(cpuUtil) = 1.229
```

```
VARIANCE(memUtil) = 0.37025
```

CMDB Lookup Function

Details of the following CMDB lookup function is available.

- DeviceToCMDBAttr Function

DeviceToCMDBAttr Function

DeviceToCMDBAttr(<deviceId>,<cmdbAttribute>) returns the value of <cmdbAttribute> for the device specified by <deviceId>. The device must be present in CMDB (postGreSQL database).

Syntax

For simple CMDB Attributes that are attached to a device, the syntax is:

DeviceToCMDBAttr(<deviceId >,<cmdbAttr>)

- deviceId can be any event attribute that can be used by FortiSIEM can look up the device in CMDB. Common examples are device name and Ip fields, e.g. hostName, hostIpAddr, srcName, srcIpAddr, destName, destIpAddr, etc.
- *cmdbAttr* are defined in **Admin > Device Support > Custom Properties**.

Some CMDB Attributes are attached to an interface or a disk of a device. In this case the syntax:

DeviceToCMDBAttr(<deviceId >,<deviceAttr>,<cmdbAttr>)

- deviceId can be any event attribute that can be used by FortiSIEM can look up the device in CMDB. Common examples are device name and Ip fields, e.g. hostName, hostIpAddr, srcName, srcIpAddr, destName, destIpAddr, etc.
- *deviceAttr* is Device Attribute: *intfName, diskName*
- *cmdbAttr* are defined in **Admin > Device Support > Custom Properties**

As an example:

DeviceToCMDBAttr(hostIpAddr,intfName,IntfErrPctThreshCrit))

DeviceToCMDBAttr(hostIpAddr,diskName,DiskSpaceUtilThreshCrit)

Scope

Available for rules and EventDB, ClickHouse and Elasticsearch queries.

Example

CMDB:

Device Name	country	intfName	NetIntfUtilThreshCrit
Host1	U.S.A	Intf1	75
Host2	France	Intf1	90
Host2	France	Intf2	75

Event Matching:

phRecvTime	**eventType**	**hostName**	***intfName***	***intfUtil***	***DeviceToCMDBAttr(hostname,city)***	***DeviceToCMDBAttr(hostName,intfName,NetIntfUtilThreshCrit)***
T1	Intf_Usage	Host1	Intf1	40	U.S.A	75
T2	Intf_Usage	Host2	Intf1	80	France	90
T2	Intf_Usage	Host2	Intf2	60	France	75
T3	Intf_Usage	Host3	Intf1		<No match>	<No match>

Conversion Functions

Details of the following conversion functions are available.

- LOG
- TO_DOUBLE
- TO_INTEGER
- TO_STRING

LOG Function

LOG(<field>, <base>) calculates the log of a numeric <field> to its <base>.

Syntax

LOG(<field>, <base>)

- <field> is a numeric *eventAttribute*. <base> is optional and default is 10.

LOG(FUNCTION(<field>), <base>)

- *Function* must return a numeric value. <base> is optional and default is 10.

Elasticsearch does not support nested functions.

In ClickHouse, these nested function categories are allowed:

- *Aggregation Functions, Conversion Functions, Evaluate-and-Set Function*

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Example

hostName	recvBytes64	LOG(recvBytes64,10)	LOG(recvBytes64,”e”)
Host1		6.67	15.36
Host2		7.35	16.73
Host3		2.66	6.12

TO_DOUBLE Function

TO_DOUBLE(<field>) converts a string valued event attribute X to a double number.

Syntax

TO_ DOUBLE (<field>)

- *<field>* is a string valued eventAttribute or a *Function* of an eventAtribute that returns a string

TO_ DOUBLE (FUNCTION(<field>))

- *Function* must return a STRING value

Elasticsearch does not support nested functions.

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, Extraction Functions, String Manipulation Functions*
  Note: *Only LEN allowed in String Manipulation Functions*

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Example

attr1	TO_DOUBLE(attr1)
“1234.56”	1234.56
“-1234.56”	-1234.56

TO_INTEGER Function

TO_INTEGER(<field>, <base>) converts a string valued <field> to a integer with <base>. <base> is optional and default is 10.

Syntax

TO_ INTEGER (<field>, <base>)

- *<field>* is a string valued eventAttribute or a *Function* of an eventAtribute that returns a string
- *<base>* is an integer. It is optional and default is 10

TO_ INTEGER (FUNCTION(<field>), <base>)

- *Function* must return a STRING value
- *<base>* is an integer. It is optional and default is 10

In Elasticsearch, nesting is not supported.

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, Extraction Functions, String Manipulation Functions*
  Note: *Only LEN allowed in String Manipulation Functions*

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Example

field	TO_INTEGER(field,10)	TO_INTEGER(field,2)	TO_NUMBER(field,16)
“1000”	1000	1111101000	3E8
“1234”	1234	10011010010	4D2

Restrictions

1. <field> has to be string representation of an integer.
2. If <base> is 2 or 16, X must be a string representation of a positive integer.

TO_STRING Function

TO_STRING(<field>) converts an input <field> to a string. If the <field> is an integer, then it reformats the number as a string. If the <field> is an Boolean value, then it returns “True” of “False”.

Syntax

TO_STRING(<field>)

- <field> is a numeric eventAttribute, or a *Function* returning a number, or a Boolean expression.
- Return value: If the <field> is an integer, then it reformats the number as a string. If the <field> is an Boolean value, then it returns “True” of “False”.

TO_STRING(FUNCTION(<field>))

- *Function* must return a numeric value or a Boolean expression.
- Return value: If the <field> is an integer, then it reformats the number as a string. If the <field> is an Boolean value, then it returns “True” of “False”.

Elasticsearch does not support nested functions.

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, Evaluate-and-Set Function, Extraction Functions*

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Example

attr1	TO_STRING(attr1)
1234	“1234”
1234.56	“-1234.56”

Date Conversion Functions

Details of the following date conversion functions are available.

- DayOfWeek
- HourOfDay

DayOfWeek Function

DayOfWeek(<eventAttribute>) returns the day of week in the DATE valued *<eventAttribute>*. 0 is returned for Sunday and 6 for Saturday.

Syntax

DayOfWeek (<eventAttribute>)

- <eventAttribute> type must be DATE
- Returned values are
    - 0 for Sunday
    - 1 for Monday
    - 2 for Tuesday
    - 3 for Wednesday
    - 4 for Thursday
    - 5 for Friday
    - 6 for Saturday

Scope

- DayOfWeek() is available in EventDB, ClickHouse and Elasticsearch queries and rules.
- DayOfWeek() can be used in Filter and Group By.

Example

phEventRecvTime	eventType	DayOfWeek(phEventRecvTime)
Monday May 15, 10:37AM	Login-Success	1

phEventRecvTime	eventType	DayOfWeek(phEventRecvTime)
Tuesday May 16, 7:37AM	Login-Success	2

HourOfDay Function

HourOfDay (<field>) returns the hour of day in the DATE valued argument. For times between 12:00AM and 12:59AM, HourOfDay() returns 0; between 1:00AM and 1:59AM, HourOfDay() returns 1, etc.

Syntax

HourOfDay (<eventAttribute>) and eventAttribute type must be DATE.

Scope

HourOfDay() is available in EventDB, ClickHouse and Elasticsearch.

Example

phEventRecvTime	eventType	HourOfDay(phEventRecvTime)
Monday May 15, 10:37AM	Login-Success	10
Monday May 15, 7:37AM	Login-Success	7

Evaluate and Set Function

Details of the following evaluate and set function is available.

- IF

IF Function

IF(<expression>,<trueValue>,<falseValue>) evaluates the <expression> and returns <trueValue> if <expression> is true and <falseValue> if the <expression> is false.

Syntax

IF(<expression>,<trueValue>,<falseValue>)

- <expression> is a Boolean expression that evaluates to true or false. Currently expression can only be the following expressions joined by AND/OR:
  <eventAttribute><Operator><ConstantValue>
- <trueValue> is returned when <expression> evaluates to true – can be a string or an integer
- <falseValue> is returned when <expression> evaluates to false – can be a string or an integer

Note that nested functions is not supported for IF.

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Example

Time	eventType	User	IF(eventType=” Login-Success”,1,0)	IF(eventType=” Login-Failure”,1,0)
T1	Login-Success	User1	1	0
T2	Login-Success	User2	1	0
T3	Login-Failure	User1	0	1
T4	Login-Failure	User1	0	1
T5	Login-Success	User1	1	0

If you group by on User and then apply aggregate on the IF function, then you get the following result:

User	SUM(IF(eventType=” Login-Success”,1,0))	SUM(IF(eventType=” Login-Failure”,1,0
User1	2	2
User2	1	0

Extraction Function

Details of the following extraction function is available.

- EXTRACT

EXTRACT Function

EXTRACT(<field>,<pattern>) extracts a value from <field> after applying regular expression <pattern>, and then returns the extracted value. The returned type is determined from the regular expression. The EXTRACT function helps to parse new fields from the historical raw log which the parser may have missed.

Syntax

EXTRACT(<field>,<pattern>)

- <field> is a string valued eventAttribute. <pattern> is a regular expression pattern for value extraction

EXTRACT(FUNCTION(<field>),<pattern>)

- FUNCTION returns a string value. <pattern> is a regular expression pattern for value extraction.

Elasticsearch does not support nested functions.

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, Evaluate-and-Set Function, Extraction Functions, String Manipulation Functions*

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards. Can extract only one value. Multiple extractions not supported

Example

rawEventMsg	EXTRACT(rawEventMsg,".*\[recvBytes64\]=(\d+).*")
<134>Sep 19 17:55:01 172.30.52.10 java: [PH_DEV_MON_VM_NET_INTF_UTIL]: [eventSeverity]=PHL_INFO, [vmName]=CentOS7-7.2.1, [recvPkts64]=0, [sentPkts64]=0, [**recvBytes64**]=23000, [sentBytes64]=54999	23000
<134>Sep 19 17:55:01 172.30.52.10 java: [PH_DEV_MON_VM_NET_INTF_UTIL]: [eventSeverity]=PHL_INFO, [vmName]=CentOS7-7.2.1, [recvPkts64]=0, [sentPkts64]=0, [**recvBytes64**]= 368640, [sentBytes64]=54999	368640

Lookup Table Functions

Details of the following lookup table functions are available.

- LookupTableGet
- LookupTableHas

LookupTableGet Function

LookupTableGet (<tableName>,<eventAttribute>,<tableColumn>) searches the Lookup Table <tableName> and matches the keys with <eventAttribute>. If a matching row is found then it returns the <tableColumn> from that row. If the Lookup Table has multiple keys then corresponding event attributes must be specified.

Syntax

LookupTableGet (<tableName>,<eventAttribute>,<tableColumn>)

The number of eventAttributes must match the key fields in the Lookup Table.

In Elasticsearch, nesting is not supported.

In ClickHouse, nesting is not supported.

Scope

Available for rules and EventDB, ClickHouse and Elasticsearch queries.

Example

LookupTable: **UserLoc**

User (Key)	Country	Department
Bob	U.S.A	Finance
Alice	Germany	Engineering
John	U.S.A	Marketing

The following table shows the LookupTableGet Function applied to events.

phRecvTime	eventType	user	LookupTableGet (UserLoc, user, Country)	LookupTableGet(User-Loc, user,Department)
T1	Login-Success	John	U.S.A	Marketing
T2	Login-Failure	Alice	Germany	Engineering
T3	Login-Success	Alice	Germany	Engineering

LookupTableHas Function

LookupTableHas (<tableName>,<eventAttribute>) works the following way:

- Returns 1 if there is a row in Lookup table <*tableName*> where the key fields match the specified <*eventAttribute*>.
- Returns 0 if there is no match.

Syntax

LookupTableHas (<tableName>,<eventAttribute>)

The number of eventAttributes must match the key fields in the Lookup Table.

In Elasticsearch, nesting is not supported.

In ClickHouse, nesting is not supported.

Scope

Available for rules and EventDB, ClickHouse and Elasticsearch queries.

Example

LookupTable: **LoginCountry**

User (Key)	Country(Key)
Bob	U.S.A
Alice	Germany
John	U.S.A

The following table shows the LookupTableHas Function applied to events.

phRecvTime	eventType	user	srcGeoCountry	LookupTableHas(LoginCountry, user, srcGeoCountry)
T1	Login-Success	John	U.S.A	1
T2	Login-Failure	Alice	France	0
T3	Login-Success	Alice	Germany	1

String Manipulation Functions

Details of the following string manipulation functions are available.

- LEN
- LTRIM
- REPLACE
- RTRIM
- SUB_STR
- TO_LOWER
- TO_UPPER
- TRIM
- URL_DECODE

LEN Function

LEN(<field>) returns the *length* of a string valued <field>.

Syntax

LEN(<eventAttribute>) - *eventAttribute* must be a STRING type.

LEN(Function(<eventAttribute>)) - The *Function* must return a STRING value.

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

In Elasticsearch, nesting is not supported.

In ClickHouse, these nested function categories are allowed:

- *Evaluate-and-Set Function, Extraction Function, String Manipulation Functions*

Example

eventType	rawEvent	LEN(rawEvent)
Event1	This is a short event	21
Event2	This is a medium event	23
Event3	This is a very very long event	30

LTRIM Function

LTRIM(<field>,<chars>) returns the string valued <field> after trimming characters in <chars> from left side. If *<chars>* is not specified, then only spaces and tabs are removed.

Syntax

LTRIM(<eventAttribute >,<chars>)

- *<eventAttribute>* must be a STRING type
- <chars> is a list of characters

LTRIM(Function(<eventAttribute>), <chars>)

- *Function* must return a STRING value
- <chars> is a list of characters

In Elasticsearch, nesting is not supported.

In ClickHouse, these nested function categories are allowed:

- *Evaluate-and-Set Function, Extraction Function, String Manipulation Functions*

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Example

user	LTRIM(user)	LTRIM(user, “FORTINET\\”)
“ user1”	“user1”	“ user1”
“FORTINET\user3”	" “FORTINET\user3”	"user3”

REPLACE Function

REPLACE(<field>,<pattern>,<replaceWith>) returns a string formed by substituting string *<replaceWith>* for every occurrence of regex string *<pattern>* in string valued *<field>*.

Syntax

REPLACE(<eventAttribute>,<pattern>,<replaceWith>)

- *<eventAttribute>* must be a STRING type
- *<pattern>* must be a regular expression and
- *<replaceWith>* is a STRING type

REPLACE (Function(<eventAttribute>),<pattern>,<replaceWith>)

- *Function* must return a STRING value
- *<pattern>* must be a regular expression and
- *<replaceWith>* is a STRING type

In Elasticsearch, nesting is not supported.

In ClickHouse, these nested function categories are allowed:

- *Evaluate-and-Set Function, Extraction Function, String Manipulation Functions*

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Example

user	REPLACE(user, "FORTINET\\", "")	REPLACE(user, "Administrator", "admin")
Bob	Bob	Bob
FORTINET\John	John	John
alice@fortinet.com	alice@fortinet.com	alice@fortinet.com
Administrator	Administrator	admin

RTRIM Function

RTRIM(<field>,<chars>) returns the string valued *<field>* after trimming characters in *<chars>* from the right side. If *<chars>* is not specified, then only spaces and tabs are removed.

Syntax

RTRIM(<eventAttribute >,<chars>)

- *<eventAttribute>* must be STRING type
- <chars> is a list of characters

RTRIM(Function(<eventAttribute>), <chars>)

- *Function* must return a STRING value
- <chars> is a list of characters

In Elasticsearch, nesting is not supported.

In ClickHouse, these nested function categories are allowed:

- *Evaluate-and-Set Function, Extraction Function, String Manipulation Functions*

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Example

user	RTRIM(user)	RTRIM(user, “@fortinet.com”)
“user1 ”	“user1”	“user1 ”
“user2@fortinet.com”	“user2@fortinet.com”	"user2”

Restrictions

None

SUB_STR Function

SUB_STR(<field>,<start>,<num>) returns a substring of string valued *<field>*, starting at the index specified by *<start>* with the number of characters specified by *<num>*. **If** *<num>* is not specified then the string *<field>* starting at *<start>* to the end is returned.

Syntax

SUB_STR(<eventAttribute>,<start>[,<num>])

- *<eventAttribute>* must be STRING type
- <start> is an integer between 0 and the length of <eventAttribute>
- <num> is an integer and must be less than length of <eventAttribute> minus <start>

SUB_STR(Function(<eventAttribute>),<start>[,<num>])

- *Function* must return a STRING value
- <start> is an integer between 0 and the length of <eventAttribute>
- <num> is an integer and must be less than length of <eventAttribute> minus <start>

SUM(<eventAttribute>) or SUM (Function(<eventAttribute>))

In Elasticsearch, nesting is not supported.

In ClickHouse, these nested function categories are allowed:

- *Evaluate-and-Set Function, Extraction Function, String Manipulation Functions*

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Example

user	SUB_STR(user,2)	SUB_STR(user,2,2)
aabbcc	bbcc	bb
123456	3456	34

TO_LOWER Function

TO_LOWER(<field>) changes the case of a string valued <field> to all lower case.

Syntax

TO_LOWER (<eventAttribute>) - *eventAttribute* must be a STRING type.

TO_LOWER (Function(<eventAttribute>)) - The *Function* must return a STRING value.

In Elasticsearch, nesting is not supported.

In ClickHouse, these nested function categories are allowed:

- *Evaluate-and-Set Function, Extraction Function, String Manipulation Functions*

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Example

eventType	user	TO_LOWER(user)
E1	Bob	bob
E2	ACME/John	acme/john
E3	ALICE	alice

TO_UPPER Function

TO_UPPER(<field>) changes the case of a string valued <field> to all upper case.

Syntax

TO_UPPER (<eventAttribute>) - *eventAttribute* must be a STRING type.

TO_UPPER (Function(<eventAttribute>)) - The *Function* must return a STRING value.

In Elasticsearch, nesting is not supported.

In ClickHouse, these nested function categories are allowed:

- *Evaluate-and-Set Function, Extraction Function, String Manipulation Functions*

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Example

eventType	user	TO_UPPER(user)
E1	Bob	BOB
E2	ACME/John	ACME/JOHN
E3	ALICE	ALICE

TRIM Function

TRIM(<field>,<chars>) returns the string valued <field> after trimming characters in <chars> from both sides. If <chars> is not specified, then only spaces and tabs are removed.

Syntax

TRIM(<eventAttribute >,<chars>)

- *<eventAttribute>* must be a STRING type.
- <chars> is a list of characters

TRIM(Function(<eventAttribute>), <chars>)

- *Function* must return a STRING value
- <chars> is a list of characters

In Elasticsearch, nesting is not supported.

In ClickHouse, these nested function categories are allowed:

- *Evaluate-and-Set Function, Extraction Function, String Manipulation Functions*

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Example

user	TRIM(user)	TRIM(user, “FORTINET\\”)
“ user1”	“user1”	“ user1”
“user2 ”	"user2”	“user2 ”
“FORTINET\user3”	" “FORTINET\user3”	"user3”

URL_DECODE Function

URL_DECODE(<field>) returns a decoded URL string of event attribute <field> which represents an encoded URL.

Syntax

URL_DECODE (<eventAttribute>) - eventAttribute must be a STRING type.

URL_DECODE (Function(<eventAttribute>)) - The *Function* must return a STRING value.

In ClickHouse, these nested function categories are allowed:

- *Evaluate-and-Set Function, Extraction Function, String Manipulation Functions*

Scope

Not available for Elasticsearch.

Available for ClickHouse queries from 7.0.0 onwards.

Example

infoUrl	URL_DECODE(infoUrl)
http://127.0.0.1:8123/? query=SELECT%201%3B	http://127.0.0.1:8123/?query=SELECT 1;
http://127.0.0.1:8123/? SELECT%20%2A%20FROM%20Users%20WHERE%20custId%20%3D%20105%20OR%201%3D1	http://127.0.0.1:8123/?SELECT * FROM Users WHERE custId= 105 OR 1=1

Time Window Functions

Details of the following time window functions are available.

- EMA
- SMA

EMA Function

EMA(N,<field>) returns *Exponential Moving Average* over N previous values of the numerical valued <field> among all events matching the query criteria.

Syntax

EMA(N, <eventAttribute>) - eventAttribute must be a numerical type.

EMA(N,Function(<eventAttribute>)) – The *Function* must return a numerical value and cannot be an aggregate attribute.

Any query using SMA needs to have at least one of the time aggregation fields included. Supported time aggregation fields include

- Hourly (phRecvHour)
- Daily (phRecvDate)
- Weekly (phRecvWeek)
- Monthly(phRecvMonth)

In Elasticsearch, these nested function categories are allowed:

- *Extraction Function, String Manipulation Functions*
  Note: *Only LEN allowed in String Manipulation Functions*

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, String Manipulation Functions*
  Note: *Only LEN allowed in String Manipulation Functions*

Scope

Works for ClickHouse and Elasticsearch queries from release 7.0.0 onwards.

Example

Raw Data

eventRecvTime	hostName	cpuUtil
Apr 19, 2023, 12:00:00 PM	H1	3.00%
Apr 19, 2023, 12:15:00 PM	H1	2.37%
Apr 19, 2023, 12:30:00 PM	H1	2.68%
Apr 19, 2023, 12:45:00 PM	H1	2.72%
Apr 19, 2023, 13:00:00 PM	H1	2.55%
Apr 19, 2023, 13:15:00 PM	H1	2.43%
Apr 19, 2023, 13:30:00 PM	H1	2.50%
Apr 19, 2023, 13:45:00 PM	H1	2.74%
Apr 19, 2023, 14:00:00 PM	H1	2.64%
Apr 19, 2023, 14:15:00 PM	H1	3.74%
Apr 19, 2023, 14:30:00 PM	H1	2.12%
Apr 19, 2023, 14:45:00 PM	H1	3.84%

EMA query response

eventRecvHour	hostName	EMA(2,cpuUtil)
Apr 19, 2023, 12:00:00 PM	H1	2.69
Apr 19, 2023, 13:00:00 PM	H1	2.60
Apr 19, 2023, 14:00:00 PM	H1	2.92

```
alpha = 2/(window size + 1) = 2/(2 + 1) = 0.667
```

```
AVG(cpuUtil) [12:00-12:59:59]  = (3.00 + 2.37+ 2.68+ 2.72)/4 = 2.6925
AVG(cpuUtil) [13:00-13:59:59] = (2.55+2.43+2.50+2.74)/4 = 2.555
AVG(cpuUtil) [14:00- 4:59:59] = (2.64+3.74+2.12+3.84)/4 = 3.085

EMA(2,cpuUtil) [12:00:00] = AVG(cpuUtil) [12:00-12:59:59]
                          = 2.69
EMA(2,cpuUtil) [13:00:00] = alpha * AVG(cpuUtil) [13:00- 13:59:59] +
     (1 - alpha) * AVG(cpuUtil) [12:00-12:59:59]
                          = 0.66 * 2.555 + (0.37)*2.6925
                          = 2.60
EMA(2,cpuUtil) [14:00:00] = alpha * AVG(cpuUtil) [14:00- 14:59:59] +
                            (1 - alpha) * AVG(cpuUtil) [13:00- 13:59:59]
                          = 0.66 * 3.085 + 0.37*2.555
                          = 2.92
```

Restrictions

1. HAVING clause is not supported.

SMA Function

SMA(N,<field>) returns *Simple Moving Average* over N previous values of the numerical valued <field> among all events matching the query criteria.

Syntax

SMA(N, <eventAttribute>) - *eventAttribute* must be a numerical type.

SMA(N,Function(<eventAttribute>)) – The *Function* must return a numerical value and cannot be an aggregate attribute.

In Elasticsearch, these nested function categories are allowed:

- *Extraction Function, String Manipulation Functions*
  Note: *Only LEN allowed in String Manipulation Functions*

In ClickHouse, these nested function categories are allowed:

- *Conversion Functions, String Manipulation Functions*
  Note: *Only LEN allowed in String Manipulation Functions*

Scope

Available for ClickHouse and Elasticsearch queries from release 7.0.0 onwards.

Example

Raw Data

eventRecvTime	hostName	cpuUtil
Apr 19, 2023, 12:00:00 PM	H1	3.00%
Apr 19, 2023, 12:15:00 PM	H1	2.37%
Apr 19, 2023, 12:30:00 PM	H1	2.68%
Apr 19, 2023, 12:45:00 PM	H1	2.72%
Apr 19, 2023, 13:00:00 PM	H1	2.55%
Apr 19, 2023, 13:15:00 PM	H1	2.43%
Apr 19, 2023, 13:30:00 PM	H1	2.50%
Apr 19, 2023, 13:45:00 PM	H1	2.74%
Apr 19, 2023, 14:00:00 PM	H1	2.64%
Apr 19, 2023, 14:15:00 PM	H1	3.74%
Apr 19, 2023, 14:30:00 PM	H1	2.12%
Apr 19, 2023, 14:45:00 PM	H1	3.84%

SMA Query response

eventRecvHour	hostName	SMA(2,cpuUtil)
Apr 19, 2023, 12:00:00 PM	H1	2.69
Apr 19, 2023, 13:00:00 PM	H1	2.62
Apr 19, 2023, 14:00:00 PM	H1	2.85

```
SMA(2,cpuUtil) [12:00:00] = AVG(cpuUtil) [12:00-12:59:59]
                          = (3.00 + 2.37+ 2.68+ 2.72)/4
                          = 2.6925
SMA(2,cpuUtil) [13:00:00] = (AVG(cpuUtil) [12:00-12:59:59] + AVG(cpuUtil) [13:00-
13:59:59] ) /2
                          = [2.6925 + (2.55+2.43+2.50+2.74)/4] / 2
                          = [ 2.6925 + 2.555 ] / 2
                          = 2.62
SMA(2,cpuUtil) [14:00:00] = (AVG(cpuUtil) [13:00-13:59:59] + AVG(cpuUtil) [14:00-
14:59:59] ) /2
                          = [ 2.555 + (2.64+3.74+2.12+3.84)/4] / 2
                          = [ 2.555 + 3.085 ] / 2
                          = 2.85
```

Restrictions

1. HAVING clause is not supported.

GUI Notes

Flash to HTML5 GUI Mapping

This section describes the mapping between FortiSIEM Flash-based GUI (available for all AccelOps and FortiSIEM versions up to 5.0.0) and FortiSIEM HTML5-based GUI (available from FortiSIEM version 5.0.0). This mapping enables you to familiarize with AccelOps/FortiSIEM Flash-based GUI to quickly find the corresponding functions in FortiSIEM HTML5-based GUI.

FortiSIEM HTML5-based GUI is similar to the earlier Flash-based GUI. In addition to the Dashboard, Analytics, Incidents, CMDB and Admin tabs from Flash-based GUI, the HTML5-based GUI adds two new tabs - CASES and RESOURCES.

The following tables show the mapping for each tab.

Dashboard

Flash Element	HTML5 Element
Executive Summary	DASHBOARD > Network Dashboard > Summary DASHBOARD > Server Dashboard > Summary DASHBOARD > Storage Dashboard > Summary
Incident Dashboard > Table View	INCIDENTS > List View
Incident Dashboard > Fishbone View	*Currently not available*
Incident Dashboard > Topological View	*Currently not available*
Incident Dashboard > Calendar View	*Currently not available*
Incident Dashboard > Location View	INCIDENTS > List View > Action > Locations
My Dashboard	DASHBOARD > New Dashboard (can be imported)
Summary Dashboard > Biz Service Summary	DASHBOARD > Click **+** to add new Dashboard and choose **Type** as 'Business Service Dashboard'.
Summary Dashboard > All Device	DASHBOARD > Network Dashboard > Summary DASHBOARD > Server Dashboard > Summary DASHBOARD > Storage Dashboard > Summary

Flash Element	HTML5 Element
Summary Dashboard > Network Device	DASHBOARD > Network Dashboard > Summary
Summary Dashboard > Servers	DASHBOARD > Server Dashboard > Summary
Summary Dashboard > EC2 Systems	DASHBOARD > Amazon Web Services Dashboard > Summary
Summary Dashboard > Azure Systems	*Currently not available as built-in (user can create their own)*
Summary Dashboard > All VMs	DASHBOARD > VMWare Dashboard > VM DASHBOARD > VMWare Dashboard > ESX
Summary Dashboard > My Devices	DASHBOARD > Any customized summary dashboard can be used to manage devices.
Availability / Performance > Hardware Summary	DASHBOARD > Network Dashboard > Hardware DASHBOARD > Server Dashboard > Hardware
Storage	DASHBOARD > NetApp Dashboard DASHBOARD > VNX Dashboard
Top Monitored Processes	*Currently not available*
Apache Servers	DASHBOARD > Web Server Dashboard
Exchange Servers	*Currently not available as built-in (user can create their own)*
Windows DHCP	*Currently not available as built-in (user can create their own)*
Windows DNS	*Currently not available as built-in (user can create their own)*
IIS Servers	DASHBOARD > Web Server Dashboard
ASP.NET Servers	*Currently not available*
MS Active Directory Servers	*Currently not available*
MS SQL Servers	DASHBOARD > Database Dashboard
Oracle DB Servers	DASHBOARD > Database Dashboard
MySQL Servers	DASHBOARD > Database Dashboard

Flash Element	HTML5 Element
VoIP Summary	*Currently not available as built-in (user can create their own)*
IPSLA Summary	*Currently not available as built-in (user can create their own)*
STM Summary	*Currently not available as built-in (user can create their own)*
Environmental Dashboard	*Currently not available as built-in (user can create their own)*
Dashboard By Function > Network > Generic	DASHBOARD > Network Dashboard > Availability DASHBOARD > Network Dashboard > Performance DASHBOARD > Network Dashboard > Login/Change DASHBOARD > Network Dashboard > Change
Dashboard By Function > Network > Netflow	DASHBOARD > Network Dashboard > Netflow
Dashboard By Function > Network > VoIP	DASHBOARD > Network Dashboard > VoIP
Dashboard By Function > Network > IPSLA	DASHBOARD > Network Dashboard > IPSLA
Dashboard By Function > Server	DASHBOARD > Server Dashboard
Dashboard By Function > Virtualization	DASHBOARD > VMWare Dashboard
Dashboard By Function > Application > Generic	DASHBOARD > Server Dashboard > Availability DASHBOARD > Server Dashboard > Performance
Dashboard By Function > Application > Mail	*Currently not available as built-in (user can create their own)*
Dashboard By Function > Application > Database	*Currently not available as built-in (user can create their own)*
Dashboard By Function > Application > Web	DASHBOARD > Web Server Dashboard
Dashboard By Function > Storage	DASHBOARD > NetApp Dashboard DASHBOARD > VNX Dashboard
Dashboard By Function > Environment	*Currently not available as built-in (user can create their*

Flash Element	HTML5 Element
	own)
Dashboard By Function > Event/Log Mgmt	DASHBOARD > FortiSIEM Dashboard
Dashboard By Function > Fortinet Security Fabric	DASHBOARD > Fortinet Security Fabric

Analytics

Flash Element	HTML5 Element
Real Time Search	ANALYTICS
Historical Search	ANALYTICS
Reports	RESOURCES > Reports
Generated Reports	ANALYTICS > 🗁 ▾
Identity and Location Report	DASHBOARD > Click **+** to add new Dashboard and choose **Type** as 'Identity and Location Dashboard'.
Rules	RESOURCES > Rules
Audit	*Currently not available*
Incident Notification Policy	ADMIN > Settings > General > Notification
Remediations	RESOURCES > Remediations
Display Column Sets	*Currently not available*
Filter Column Sets	*Currently not available*

Incidents

Flash Element	HTML5 Element
Incidents	INCIDENTS > List View
Tickets	CASE
IPS Vulnerability Map	*Currently not available*

CMDB

Flash Element	HTML5 Element
Topology	*Currently not available*
Devices	CMDB > Devices
Applications	CMDB > Applications
Users	CMDB > Users
Business Services	CMDB > Business Services
Networks	RESOURCES > Networks
Watch Lists	RESOURCES > Watch Lists
Protocols	RESOURCES > Protocols
Event Types	RESOURCES > Event Types
Malware Domains	RESOURCES > Malware Domains
Malware IP	RESOURCES > Malware IPs
Malware URLs	RESOURCES > Malware URLs
Malware Processes	RESOURCES > Malware Processes
CMDB Reports	CMDB > CMDB Reports
Country Groups	RESOURCES > Country Groups
Malware Hash	RESOURCES > Malware Hash
Default Password	RESOURCES > Default Password
Anonymity Networks	RESOURCES > Anonymity Networks
User Agents	RESOURCES > User Agents

Admin

Flash Element	HTML5 Element
Admin > Startup	*Not available*

Flash Element	HTML5 Element
Admin > Setup Wizard > Organizations	ADMIN > Setup > Organizations
Admin > Setup Wizard > Windows Agents	ADMIN > Setup > Windows Agents
Admin > Setup Wizard > Credentials	ADMIN > Setup > Credentials
Admin > Setup Wizard > Discovery	ADMIN > Setup > Discovery
Admin > Setup Wizard > Pull Events	ADMIN > Setup > Pull Events
Admin > Setup Wizard > Monitor Change/Performance	ADMIN > Setup > Monitor Performance
Admin > Setup Wizard > Synthetic Transaction Monitoring	ADMIN > Setup > STM
Admin > Device Support > Device/App Types	ADMIN > Device Support > Device/App
Admin > Device Support > Event Attribute Types	ADMIN > Device Support > Event Attribute
Admin > Device Support > Event Types	ADMIN > Device Support > Event
Admin > Device Support > Parsers	ADMIN > Device Support > Parser
Admin > Device Support > Performance Monitoring	ADMIN > Device Support > Monitoring
Admin > Device Support > Custom Properties	ADMIN > Device Support > Custom Property
Admin > Device Support > Dashboard Columns	*Currently not available*
Admin > Collector Health	ADMIN > Health > Collector Health
Admin > Cloud Health	ADMIN > Health > Cloud Health
Admin > Elasticsearch health	ADMIN > Health > Elasticsearch health
Admin > General Settings > System	ADMIN > Settings > System
Admin > General Settings > Analytics	ADMIN > Settings > Analytics
Admin > General Settings > Discovery	ADMIN > Settings > Discovery
Admin > General Settings > Monitoring	ADMIN > Settings > Monitoring
Admin > General Settings > UI	ADMIN > Settings > System > UI

Flash Element	HTML5 Element
Admin > General Settings > Email Template	ADMIN > Settings > System > Email
Admin > General Settings > Event Handling	ADMIN > Settings > Event Handling
Admin > General Settings > Kafka Config	ADMIN > Settings >System > Kafka
Admin > General Settings > External Authentication	ADMIN > Settings > General > Authentication
Admin > General Settings > Integration	ADMIN > Settings > General > Integration
Admin > General Settings > External Lookup	ADMIN > Settings > System > Lookup
Admin > General Settings > Escalation Policy	ADMIN > Settings > General > Escalation
Admin > Discovery Results	ADMIN > Setup > Discovery > History
Admin > License Management	ADMIN > License > License
Admin > Usage Information	ADMIN > License > Usage
Admin > Role Management	ADMIN > Settings > Role
Admin > Maintenance Calendar	ADMIN > Setup > Maintenance
Admin > Event DB Management	*Currently not available*
Admin > Data Update	ADMIN > Data Update

FortiSIEM Charts and Views

FortiSIEM provides a variety of charts and maps to better help you understand and analyze your incident data. You can access these charts and views from the widget dashboard settings (see Modifying widget information display) or by clicking the **TABLE** or 📈 ▾ drop-down icon in the ANALYTICS page (see Viewing Historical Search Results).

Chart/View	Description	Display Settings	Requirements
Table	Displays data in a tabular format.	You can choose to display the bar chart (**Show Bar**), the event type (**Show Event Type**), and the count (**Count**). Set the colors for the	None

Chart/View	Description	Display Settings	Requirements
		bar chart or reverse the color map.	
Link Graph	Displays source, event, and destination relationships. Source nodes appear in light blue, Event nodes are color coded by their severity if event attribute "Event Severity Category" exists in the Display Fields on Table view. A node can be clicked and dragged to be repositioned. If a node can be represented by a recognizable device type from FortiSIEM, the appropriate icon will be displayed, otherwise a default monitor icon will appear. The Rows and Total number represent the number of data items in the table view, not the number of nodes. For example, one representation will consist of 3 nodes (source, event, destination), but if all the data items share the same source, event, and destination, only three nodes will appear. Click on any node and the following options appear: • Quick Info - Select to show more information about the selected node. • Add <*object*> to Filter - Adds the data from the selected node to a filter.	Select the **Source**, **Event**, and **Destination** from the drop - down lists. Auto Layout attempts to show all nodes in an optimal manner. To disable, deselect the **Auto Layout** checkbox.	A source and destination are required.
Bar Chart	Displays data similar to a bar chart.	Select the Aggregate Field (**Column**) to display and their colors. You can also reverse the color map.	At least one numeric column is required.
Chord Chart	A graphical method of displaying the inter-relationships between data in a matrix. The data is arranged radially around a circle with the relationships between the data points typically drawn as arcs connecting the data.	Select the incident **Source**, **Target**, and **Value** from the drop-down lists.	At least two key columns and one numeric column are required.
Choropleth Chart	A thematic map in which areas are shaded or patterned in proportion to the measurement of the statistical variable being displayed on the map.	Select the **Location** and **Value** from the drop-down lists.	At least one numeric column is required. Configure **Google Maps API Key** in **ADMIN > Settings > System**

Chart/View	Description	Display Settings	Requirements
			> UI See UI Settings.
Cluster Bubble Chart	You can use a bubble chart instead of a scatter chart if your data has three data series that each contain a set of values. The sizes of the bubbles are determined by the values in the third data series.	Select the **Column** from the drop-down list.	At least one numeric column is required.
Donut Chart	Displays data similar to a pie chart.	Select the Aggregate Field (**Column**) to display since the report may have multiple Aggregate Fields.	At least one numeric column is required.
GEO Map Chart	Displays the IP addresses in a geographic map.	Public or private IP addresses with location defined in **ADMIN > Settings > Discovery > Location**. See Setting Location.	At least one numeric column is required.
Heat Map Chart	Displays two event attributes and a numerical aggregate value.	Select the Heat map coordinates **X** and **Y**, and an associated **Value**.	At least two key columns and one numeric column are required.
Sankey Chart	A specific type of flow diagram, in which the width of the arrows is shown proportionally to the flow quantity.	Select the **Source**, **Target**, and **Value** from the drop-down lists.	At least two key columns and one numeric column are required.
Scatter Plot Chart	Plots two aggregate fields.	Select two aggregate fields, **X** and **Y**. Select the **Size** of the sample.	At least two numeric columns are required.
Sunburst Chart	Visualizes hierarchical data, depicted by concentric circles. The circle in the center represents the root node, with the hierarchy moving outward from the center.	Select the **Rank1**, **Rank2**, **Rank3** and **Count** from the drop-down lists.	Only one column can be used in one rank.
Tree Map Chart	Displays columns in a Tree Map.	Select the Tree Map **Ranks** and the	Only one column can be

Chart/View	Description	Display Settings	Requirements
		Count attributes from the drop-down lists.	used in one rank.
Trend Line Chart	A "trend" line is superimposed on a chart that reveals the overall direction of the data.		
Trend Area Chart	A graph that shows trend changes over time, by displaying a series of data as different colored lines.		
Trend Bar Chart	Uses bars to track trends over time.		

Knowledge Base

FortiSIEM Event Attribute to CEF Key Mapping

FortiSIEM forwards externally received logs and internally generated events/incidents to an external system via CEF formatted syslog.

FortiSIEM Event Attribute to CEF Key Mappings

FortiSIEM event attributes	CEF key	Notes
appCategory	cat	
appTransportProto	app	
count	cnt	
destAction	act	
destDomain	destinationDnsDomain	
destIntfName	deviceOutboundInterface	
destIpAddr	destinationTranslated Address	

FortiSIEM event attributes	CEF key	Notes
destIpAddr	dst	
destIpPort	destinationTranslatedPort	
destIpPort	dpt	
destMACAddr	dmac	
destName	dhost	
destServiceName	destinationServiceName	
destUser	duser	
destUserId	duid	
destUserPriv	dpriv	
deviceIdentification	deviceExternalId	
deviceTime	rt	
domain	deviceDnsDomain	
endTime	end	
errReason	reason	
extEventId	externalId	
fileAccess	filePermission	
fileId	fileId	
fileModificationTime	fileModificationTime	
fileName	fname	
filePath	filePath	
fileSize	fsize	

FortiSIEM event attributes	CEF key	Notes
fileType	fileType	
hashCode	fileHash	
hostIpAddr	dvc	
hostMACAddr	dvcmac	
hostName	dvchost	
httpCookie	requestCookies	
httpMethod	requestMethod	
httpReferrer	requestContext	
httpUserAgent	requestClientApplication	
infoURL	request	
ipProto	proto	
msg	msg	
postNATHostIpAddr	deviceTranslatedAddress	
postNATSrcIpAddr	sourceTranslatedAddress	
postNATSrcIpPort	sourceTranslatedPort	
procId	dvcpid	
procName	deviceProcessName	
recvBytes	in	
sentBytes	out	
serviceName	sourceServiceName	
srcDomain	sourceDnsDomain	

FortiSIEM event attributes	CEF key	Notes
srcIntfName	deviceInboundInterface	
intfName	deviceInboundInterface	
srcIpAddr	src	
srcIpPort	spt	
srcMACAddr	smac	
srcName	shost	
srcUser	suser	
srcUserPriv	spriv	
startTime	start	
targetProcId	dpid	
targetProcName	dproc	

Mapping to CEF Custom Attributes

FortiSIEM event attributes	CEF key	Notes
supervisorName	cs1Label = SupervisorHostName	
customer	cs2Label = CustomerName	
incidentDetail	cs3Label=IncidentDetail	
ruleName	cs4Label=RuleName	
inIncidentEventIdList	cs5Label=IncidentEventIDList	
phCustId	cn1Label=CustomerID	
incidentId	cn2Label=IncidentID	

FortiSIEM event attributes	CEF key	Notes
	type	0 = base event; 2 = incident

FortiSIEM Event Categories and Handling

This topic provides a brief description of various types of event categories in FortiSIEM.

System Event Category	Description	Counted in EPS License	phstatus -a outout	Stored in DB?
0	External events and not flow events (e.g. syslog, SNMP Trap, Event pulling)	Yes	EPS	Yes
1	Incidents (events that begin with PH_RULE)	No	EPS INTERNAL	Yes
2	FortiSIEM Audit Events (events that begin with PH_AUDIT)	No	EPS INTERNAL	Yes
3	FortiSIEM Internal system logs, free format	No	EPS INTERNAL	Yes
4	External flow events (Netflow, Sflow)	Yes	EPS	Yes
5	FortiSIEM Internal health events for summary dashboards	No	EPS INTERNAL	Yes
6	FortiSIEM Performance Monitoring events (events that begin with PH_DEV_MON)	Yes	EPS PERF	Yes
7	AO Beaconing events	No	EPS INTERNAL	Yes
8	FortiSIEM Real Time Performance Probe Events	No	EPS INTERNAL	No
99	FortiSIEM Internal Rule Engine	No	EPS INTERNAL	No

Public Domain Built-in Rules

The following table shows the public domain built-in rules incorporated into FortiSIEM.

Rules that are adopted from the SIGMA rule set are licensed under the Detection Rule License available here.

FortiSIEM Rule	Author	Source Link
AWS CloudTrail Important Changes	vitaliy0x1	https://github.com/SigmaHQ/sigma/blob/master/rules/cloud/aws_cloudtrail_disable_logging.yml
AWS EC2 Userdata Download	faloker	https://github.com/SigmaHQ/sigma/blob/master/rules/cloud/aws_ec2_download_userdata.yml
Linux: Attempt to Disable Crowdstrike Service	Ömer Günal	https://github.com/SigmaHQ/sigma/blob/master/rules/linux/lnx_security_tools_disabling.yml
Linux: Attempt to Disable CarbonBlack Service	Ömer Günal	https://github.com/SigmaHQ/sigma/blob/master/rules/linux/lnx_security_tools_disabling.yml
Windows: Turla Service Install	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_apt_carbonpaper_turla.yml
Windows: StoneDrill Service Install	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_apt_stonedrill.yml
Windows: Turla PNG Dropper Service	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_apt_turla_service_png.yml
Windows: smbexec.py Service Installation	Omer Faruk Celik	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_hack_smbexec.yml
Windows: Malicious Service Installations	Florian Roth, Daniil Yugoslavskiy, oscd.community (update)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_mal_service_installs.yml
Windows: Meterpreter or Cobalt Strike Getsystem Service Installation	Teymur Kheirkhabarov, Ecco	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_meterpreter_or_cobaltstrike_getsystem_service_installation.yml
Windows: PsExec Tool Execution	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/other/win_tool_psexec.yml
Windows: Local User Creation	Patrick Bareiss	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_user_creation.yml
Windows: Local User Creation Via Powershell	@ROxPinTeddy	https://github.-

FortiSIEM Rule	Author	Source Link
		com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_create_local_user.yml
Windows: Local User Creation Via Net.exe	Endgame, JHasenbusch (adapted to sigma for oscd.community)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_net_user_add.yml
Windows: Suspicious ANONYMOUS LOGON Local Account Created	James Pemberton / @4A616D6573	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_local_anon_logon_created.yml
Windows: New or Renamed User Account with $ in Attribute SamAccountName	Ilyas Ochkov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_new_or_renamed_user_account_with_dollar_sign.yml
Windows: AD Privileged Users or Groups Reconnaissance	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_account_discovery.yml
Windows: Administrator and Domain Admin Reconnaissance	Florian Roth (rule), Jack Croock (method)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_net_recon_activity.yml
Windows: Access to ADMIN$ Share	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_admin_share_access.yml
Windows: Login with WMI	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_wmi_login.yml
Windows: Admin User Remote Logon	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_admin_rdp_login.yml
Windows: RDP Login from Localhost	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_rdp_localhost_login.yml
Windows: Interactive Logon to Server Systems	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_interactive_logons.yml

FortiSIEM Rule	Author	Source Link
Windows: Pass the Hash Activity	Ilias el Matani (rule), The Information Assurance Directorate at the NSA (method)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_pass_the_hash.yml
Windows: Pass the Hash Activity 2	Dave Kennedy, Jeff Warren (method) / David Vassallo (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_pass_the_hash_2.yml
Windows: Successful Overpass the Hash Attempt	Roberto Rodriguez (source), Dominik Schaudel (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_overpass_the_hash.yml
Windows: RottenPotato Like Attack Pattern	@SBousseaden, Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_rottenpotato.yml
Windows: Hacktool Ruler	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_alert_ruler.yml
Windows: Metasploit SMB Authentication	Chakib Gzenayi (@Chak092), Hosni Mribah	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_metasploit_authentication.yml
Windows: Kerberos Manipulation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_kerberos_manipulation.yml
Windows: Suspicious Kerberos RC4 Ticket Encryption	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_rc4_kerberos.yml
Windows: Persistence and Execution at Scale via GPO Scheduled Task	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_GPO_scheduledtasks.yml
Windows: Powerview Add-DomainObjectAcl DCSync AD Extend Right	Samir Bousseaden; Roberto Rodriguez @Cyb3rWard0g; oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_account_backdoor_dcsync_rights.yml
Windows: AD Object WriteDAC Access	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_ad_object_writedac_access.yml
Windows: Active Dir-	Roberto Rodriguez	https://

FortiSIEM Rule	Author	Source Link
ectory Replication from Non Machine Account	@Cyb3rWard0g	github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_ad_replication_non_machine_account.yml
Windows: AD User Enumeration	Maxime Thiebaut (@0xThiebaut)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_ad_user_enumeration.yml
Windows: Enabled User Right in AD to Control User Objects	@neu5ron	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_alert_active_directory_user_control.yml
Windows: Eventlog Cleared	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_eventlog_cleared.yml
Windows: MSHTA Suspicious Execution 01	Diego Perez (@darkquassar), Markus Neis, Swisscom (Improve Rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_mshta_execution.yml
Windows: Dumpert Process Dumper	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_hack_dumpert.yml
Windows: Blue Mockingbird	Trent Liffick (@tliffick)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/win_mal_blue_mockingbird.yml
Windows: Windows PowerShell Web Request	James Pemberton / @4A616D6573	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/win_powershell_web_request.yml
Windows: DNS Tunnel Technique from MuddyWater	@caliskanfurkan_	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/sysmon_apt_muddywater_dnstunnel.yml
Windows: Advanced IP Scanner Detected	@ROxPinTeddy	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_advanced_ip_scanner.yml
Windows: APT29 Detected	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_apt29_thinktanks.yml
Windows: Baby	Florian Roth	https://-

FortiSIEM Rule	Author	Source Link
Shark Activity		github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_babyshark.yml
Windows: Judgement Panda Credential Access Activity	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_bear_activity_gtr19.yml
Windows: Logon Scripts - User-InitMprLogonScript	Tom Ueltschi (@c_APT_ure)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/sysmon_logon_scripts_userinitmprlogonscript_proc.yml
Windows: BlueMash-room DLL Load	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_bluemashroom.yml
Windows: Password Change on Directory Service Restore Mode DSRM Account	Thomas Patzke	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_dsrm_password_change.yml
Windows: Account Tampering - Suspicious Failed Logon Reasons	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_failed_logon_reasons.yml
Windows: Backup Catalog Deleted	Florian Roth (rule), Tom U. @c_APT_ure (collection)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_backup_delete.yml
Windows: Failed Code Integrity Checks	Thomas Patzke	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_codeintegrity_check_failure.yml
Windows: DHCP Server Loaded the CallOut DLL	Dimitrios Slamaris	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_dhcp_config.yml
Windows: Suspicious LDAP-Attributes Used	xknow @xknow_infosec	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_ldap_dataexchange.yml
Windows: Password Dumper Activity on LSASS		https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_lsass_dump.yml
Windows: Generic Password Dumper Activity on LSASS	Roberto Rodriguez, Teymur Kheirkhabarov, Dimitrios Slamaris, Mark Russinovich,	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_lsass_dump_generic.yml

FortiSIEM Rule	Author	Source Link
	Aleksey Potapov, oscd.community (update)	
Windows: Suspicious PsExec Execution	Samir Bousseaden	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_psexec.yml
Windows: Suspicious Access to Sensitive File Extensions	Samir Bousseaden	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_raccess_sensitive_fext.yml
Windows: Secure Deletion with SDelete	Thomas Patzke	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_sdelete.yml
Windows: Unauthorized System Time Modification	@neu5ron	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_time_modification.yml
Windows: Windows Defender Exclusion Set	@Barry-Shooshooga	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/other/win_defender_bypass.yml
Windows: Windows Pcap Driver Installed	Cian Heasley	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/other/win_pcap_drivers.yml
Windows: Weak Encryption Enabled and Kerberoast	@neu5ron	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_alert_enable_weak_encryption.yml
Windows: Remote Task Creation via ATSVC Named Pipe	Samir Bousseaden	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_atsvc_task.yml
Windows: Chafer Activity	Florian Roth, Markus Neis	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_chafer_mar18.yml
Windows: WMIExec VBS Script	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_cloudhopper.yml
Windows: CrackMapExecWin Activity	Markus Neis	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_dragonfly.yml
Windows: Elise Backdoor	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_elise.yml

FortiSIEM Rule	Author	Source Link
Windows: Emissary Panda Malware SLLauncher Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_emissarypanda_sep19.yml
Windows: Empire Monkey Activity	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_empiremonkey.yml
Windows: Equation Group DLL-U Load	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_equationgroup_dll_u_load.yml
Windows: EvilNum Golden Chickens Deployment via OCX Files	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_evilnum_jul20.yml
Windows: GALLIUM Artefacts Via Hash Match	Tim Burrell	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_gallium.yml
Windows: GALLIUM Artefacts Via Hash and Process Match	Tim Burrell	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_gallium.yml
Windows: Windows Credential Editor Startup	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/sysmon_hack_wce.yml
Windows: Greenbug Campaign Indicators	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_greenbug_may20.yml
Windows: Hurricane Panda Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_hurricane_panda.yml
Windows: Judgement Panda Exfiltration Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_judgement_panda_gtr19.yml
Windows: Ke3chang Registry Key Modifications	Markus Neis, Swisscom	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_ke3chang_regadd.yml
Windows: Lazarus Session Highjacker	Trent Liffick (@tliffick), Bartlomiej Czyz (@bczyz1)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_lazarus_session_highjack.yml
Windows: Mustang Panda Dropper Activ-	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_

FortiSIEM Rule	Author	Source Link
ity		creation/win_apt_mustangpanda.yml
Windows: Defrag Deactivation	Florian Roth, Bartlomiej Czyz (@bczyz1)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_slingshot.yml
Windows: Sofacy Trojan Loader Activity	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_sofacy.yml
Windows: Ps.exe Renamed SysInternals Tool	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_ta17_293a_ps.yml
Windows: TAIDOOR RAT DLL Load	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_taidoor.yml
Windows: TropicTrooper Campaign November 2018	@41thexplorer, Microsoft Defender ATP	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_tropictrooper.yml
Windows: Turla Group Commands May 2020	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_turla_comrat_may20.yml
Windows: Unidentified Attacker November 2018 Activity 1	@41thexplorer, Microsoft Defender ATP	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_unidentified_nov_18.yml
Windows: Unidentified Attacker November 2018 Activity 2	@41thexplorer, Microsoft Defender ATP	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_unidentified_nov_18.yml
Windows: Winnti Malware HK University Campaign	Florian Roth, Markus Neis	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_winnti_mal_hk_jan20.yml
Windows: Winnti Pipemon Characteristics	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_winnti_pipemon.yml
Windows: Operation Wocao Activity	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_wocao.yml
Windows: ZxShell Malware	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_zxshell.yml
Windows: Active Dir-	@neu5ron	https://-

FortiSIEM Rule	Author	Source Link
ectory User Backdoors		github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_alert_ad_user_backdoors.yml
Windows: Mimikatz DC Sync	Benjamin Delpy, Florian Roth, Scott Dermott	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_dcsync.yml
Windows: Windows Event Auditing Disabled	@neu5ron	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_disable_event_logging.yml
Windows: DPAPI Domain Backup Key Extraction	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_dpapi_domain_backupkey_extraction.yml
Windows: DPAPI Domain Master Key Backup Attempt	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_dpapi_domain_masterkey_backup_attempt.yml
Windows: External Disk Drive or USB Storage Device	Keith Wright	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_external_device.yml
Windows: Possible Impacket SecretDump Remote Activity	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_impacket_secretdump.yml
Windows: Obfuscated Powershell IEX invocation	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_invoke_obfuscation_obfuscated_iex_services.yml
Windows: First Time Seen Remote Named Pipe	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_lm_namedpipe.yml
Windows: LSASS Access from Non-System Account	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_lsass_access_non_system_account.yml
Windows: Credential Dumping Tools Service Execution	Florian Roth, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_mal_creddumper.yml
Windows: WCE wceaux dll Access	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_mal_wceaux_dll.yml

FortiSIEM Rule	Author	Source Link
Windows: MMC20 Lateral Movement	@2xxeformyshirt (Security Risk Advisors) - rule; Teymur Kheirkhabarov (idea)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_mmc20_lateral_movement.yml
Windows: NetNTLM Downgrade Attack	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_net_ntlm_downgrade.yml
Windows: Denied Access To Remote Desktop	Pushkarev Dmitry	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_not_allowed_rdp_access.yml
Windows: Possible DCShadow	Ilyas Ochkov, oscd.-community, Chakib Gzenayi (@Chak092), Hosni Mribah	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_possible_dc_shadow.yml
Windows: Protected Storage Service Access	Roberto Rodriguez @Cyb3rWard0g	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_protected_storage_service_access.yml
Windows: Scanner PoC for CVE-2019-0708 RDP RCE Vuln	Florian Roth (rule), Adam Bradbury (idea)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_rdp_bluekeep_poc_scanner.yml
Windows: RDP over Reverse SSH Tunnel	Samir Bousseaden	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_rdp_reverse_tunnel.yml
Windows: Register new Logon Process by Rubeus	Roberto Rodriguez (source), Ilyas Ochkov (rule), oscd.-community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_register_new_logon_process_by_rubeus.yml
Windows: Remote PowerShell Sessions	Roberto Rodriguez @Cyb3rWard0g	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_remote_powershell_session.yml
Windows: Remote Registry Management Using Reg Utility	Teymur Kheirkhabarov, oscd.community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_remote_registry_management_using_reg_utility.yml
Windows: SAM Registry Hive Handle Request	Roberto Rodriguez @Cyb3rWard0g	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_sam_registry_hive_handle_request.yml

FortiSIEM Rule	Author	Source Link
Windows: SCM Database Handle Failure	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_scm_database_handle_failure.yml
Windows: SCM Database Privileged Operation	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_scm_database_privileged_operation.yml
Windows: Addition of Domain Trusts	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_add_domain_trust.yml
Windows: Addition of SID History to Active Directory Object	Thomas Patzke, @atc_project (improvements)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_add_sid_history.yml
Windows: Failed Logon From Public IP	NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_failed_logon_source.yml
Windows: Failed Logins with Different Accounts from Single Source System	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_failed_logons_single_source.yml
Windows: Remote Service Activity via SVCCTL Named Pipe	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_svcctl_remote_service.yml
Windows: SysKey Registry Keys Access	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_syskey_registry_access.yml
Windows: Tap Driver Installation	Daniil Yugoslavskiy, Ian Davis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_tap_driver_installation.yml
Windows: Transferring Files with Credential Data via Network Shares	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_transferring_files_with_credential_data_via_network_shares.yml
Windows: User Added to Local Administrators	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_user_added_to_local_administrators.yml
Windows: Failed to Call Privileged Service LsaRegisterLogonProcess	Roberto Rodriguez (source), Ilyas Ochkov (rule), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_user_couldnt_call_privileged_service_lsaregisterlogonprocess.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious Driver Loaded By User	xknow (@xknow_infosec), xorxes (@xor_xes)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_user_driver_loaded.yml
Windows: Suspicious Driver Load from Temp	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/driver_load/sysmon_susp_driver_load.yml
Windows: File Created with System Process Name	Sander Wiebing	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_creation_system_file.yml
Windows: Credential Dump Tools Dropped Files	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_cred_dump_tools_dropped_files.yml
Windows: Detection of SafetyKatz	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_ghostpack_safetykatz.yml
Windows: LSASS Memory Dump File Creation	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_lsass_memory_dump_file_creation.yml
Windows: Microsoft Office Add-In Loading	NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_office_persistence.yml
Windows: QuarksPwDump Dump File	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_quarkspw_filedump.yml
Windows: RedMimicry Winnti Playbook Dropped File	Alexander Rausch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_redmimicry_winnti_filedrop.yml
Windows: Suspicious ADSI-Cache Usage By Unknown Tool	xknow @xknow_infosec	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_susp_adsi_cache_usage.yml
Windows: Suspicious desktop.ini Action	Maxime Thiebaut (@0xThiebaut)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_susp_desktop_ini.yml
Windows: Suspicious PROCEXP152 sys File Created In TMP	xknow (@xknow_infosec), xorxes (@xor_xes)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_susp_procexplorer_driver_created_in_tmp_folder.yml
Windows: Hijack Legit RDP Session to Move Laterally	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_tsclient_filewrite_startup.yml
Windows: Windows Web shell Creation	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_webshell_creation_detect.yml

FortiSIEM Rule	Author	Source Link
Windows: WMI Persistence - Script Event Consumer File Write	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_wmi_persistence_script_event_consumer_write.yml
Windows: Suspicious Desktopimgdownldr Target File	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/win_susp_desktopimgdownldr_file.yml
Windows: In-memory PowerShell	Tom Kern, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_in_memory_powershell.yml
Windows: PowerShell load within System Management Automation DLL	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_powershell_execution_moduleload.yml
Windows: Fax Service DLL Search Order Hijack	NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_fax_dll.yml
Windows: Possible Process Hollowing Image Loading	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_image_load.yml
Windows: .NET DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_office_dotnet_assembly_dll_load.yml
Windows: CLR DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_office_dotnet_clr_dll_load.yml
Windows: GAC DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_office_dotnet_gac_dll_load.yml
Windows: Active Directory Parsing DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_office_dsparse_dll_load.yml
Windows: Active Directory Kerberos DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_office_kerberos_dll_load.yml
Windows: VBA DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_winword_vbadll_load.yml

FortiSIEM Rule	Author	Source Link
Windows: WMI DLL Loaded Via Office Applications	Michael R. (@nahamike01)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_winword_wmidll_load.yml
Windows: Loading dbghelp dbgcore DLL from Suspicious Processes	Perez Diego (@darkquassar), oscd.community, Ecco	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_suspicious_dbghelp_dbgcore_load.yml
Windows: Svchost DLL Search Order Hijack	SBousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_svchost_dll_search_order_hijack.yml
Windows: Unsigned Image Loaded Into LSASS Process	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_unsigned_image_loaded_into_lsass.yml
Windows: Suspicious WMI Modules Loaded	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_wmi_module_load.yml
Windows: WMI Persistence - Command Line Event Consumer	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_wmi_persistence_commandline_event_consumer.yml
Windows: Registry Entries Found For Azorult Malware	Trent Liffick	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/mal_azorult_reg.yml
Windows: Registry Entries Found For FlowCloud Malware	NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/win_mal_flowcloud.yml
Windows: Octopus Scanner Malware Detected	NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/win_mal_octopus_scanner.yml
Windows: Registry Entries For Ursnif Malware	megan201296	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/win_mal_ursnif.yml

FortiSIEM Rule	Author	Source Link
Windows: Dllhost.exe Internet Connection	bartblaze	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_dllhost_net_connections.yml
Windows: Suspicious Typical Malware Back Connect Ports	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_malware_backconnect_ports.yml
Windows: Notepad Making Network Connection	EagleEye Team	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_notepad_network_connection.yml
Windows: PowerShell Network Connections	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_powershell_network_connection.yml
Windows: RDP Over Reverse SSH Tunnel	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_rdp_reverse_tunnel.yml
Windows: Regsvr32 Network Activity	Dmitriy Lifanov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_regsvr32_network_activity.yml
Windows: Remote PowerShell Session	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_remote_powershell_session_network.yml
Windows: Rundll32 Internet Connection	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_rundll32_net_connections.yml
Windows: Network Connections From Executables in Suspicious Program Locations	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_susp_prog_location_network_connection.yml
Windows: Outbound RDP Connections From Suspicious Executables	Markus Neis - Swisscom	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_susp_rdp.yml
Windows: Outbound Kerberos Connection From Suspicious Executables	Ilyas Ochkov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_suspicious_outbound_kerberos_connection.yml ; https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_suspicious_outbound_kerberos_connection.yml

FortiSIEM Rule	Author	Source Link
Windows: Microsoft Binary Github Communication	Michael Haag (idea), Florian Roth (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_win_binary_github_com.yml
Windows: Microsoft Binary Suspicious External Communication	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_win_binary_susp_com.yml
Windows: Data Compressed - Powershell	Timur Zinniatullin, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_data_compressed.yml
Windows: Dnscat Execution	Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_dnscat_execution.yml
Windows: PowerShell Credential Prompt	John Lambert (idea), Florian Roth (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_prompt_credentials.yml
Windows: Powershell Profile ps1 Modification	HieuTT35	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_suspicious_profile_create.yml
Windows: Credentials Dumping Tools Accessing LSASS Memory	Florian Roth, Roberto Rodriguez, Dimitrios Slamaris, Mark Russinovich, Thomas Patzke, Teymur Kheirkhabarov, Sherif Eldeeb, James Dickenson, Aleksey Potapov, oscd.community (update)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_cred_dump_lsass_access.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious In-Memory Module Execution	Perez Diego (@darkquassar), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_in_memory_assembly_execution.yml
Windows: Suspect Svchost Memory Access	Tim Burrell	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_invoke_phantom.yml
Windows: Credential Dumping by LaZagne	Bhabesh Raj	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_lazagne_cred_dump_lsass_access.yml
Windows: LSASS Memory Dump	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_lsass_memdump.yml
Windows: Malware Shellcode in Verclsid Target Process	John Lambert (tech), Florian Roth (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_malware_verclsid_shellcode.yml
Windows: Mimikatz through Windows Remote Management	Patryk Prauze - ING Tech	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_mimikatz_trough_winrm.yml
Windows: Turla Group Lateral Movement	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_turla_commands.yml
Windows: Hiding Files with Attrib exe	Sami Ruohonen	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_attrib_hiding_files.yml
Windows: Modification of Boot Configuration	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_bootconf_mod.yml
Windows: SquiblyTwo	Markus Neis / Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_bypass_squiblytwo.yml
Windows: Change Default File Association	Timur Zinniatullin, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_change_default_file_association.yml
Windows: Cmdkey Cached Credentials Recon	jmallette	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_cmdkey_recon.yml
Windows: CMSTP	Nik Seetharaman	https://

FortiSIEM Rule	Author	Source Link
UAC Bypass via COM Object Access		github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_cmstp_com_object_access.yml
Windows: Cmd exe CommandLine Path Traversal	xknow @xknow_infosec	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_commandline_path_traversal.yml
Windows: Unusual Control Panel Items	Kyaw Min Thein, Furkan Caliskan (@caliskanfurkan_)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_control_panel_item.yml
Windows: Copying Sensitive Files with Credential Data	Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_copying_sensitive_files_with_credential_data.yml
Windows: Fireball Archer Malware Install	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_crime_fireball.yml
Windows: Maze Ransomware	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_crime_maze_ransomware.yml
Windows: Snatch Ransomware	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_crime_snatch_ransomware.yml
Windows: Data Compressed - rar.exe	Timur Zinniatullin, E.M. Anhaus, oscd.-community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_data_compressed_with_rar.yml
Windows: DNS Exfiltration and Tunneling Tools Execution	Daniil Yugoslavskiy, oscd.community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_dns_exfiltration_tools_execution.yml
Windows: DNSCat2 Powershell Detection Via Process Creation	Cian Heasley	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_dnscat2_powershell_implementation.yml
Windows: Encoded FromBase64String	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_encoded_frombase64string.yml
Windows: Encoded IEX	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_encoded_iex.yml
Windows: COMPlus-ETWEnabled Com-	Roberto Rodriguez (Cyb3rWard0g),	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_

FortiSIEM Rule	Author	Source Link
mand Line Arguments	OTR (Open Threat Research)	creation/win_etw_modification_cmdline.yml
Windows: Disabling ETW Trace	@neu5ron, Florian Roth, Jonhnathan Ribeiro, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_etw_trace_evasion.yml
Windows: Exfiltration and Tunneling Tools Execution	Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exfiltration_and_tunneling_tools_execution.yml
Windows: Exploit for CVE-2015-1641	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2015_1641.yml
Windows: Exploit for CVE-2017-0261	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2017_0261.yml
Windows: Droppers Exploiting CVE-2017-11882	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2017_11882.yml
Windows: Exploit for CVE-2017-8759	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2017_8759.yml
Windows: Exploiting SetupComplete.cmd CVE-2019-1378	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2019_1378.yml
Windows: Exploiting CVE-2019-1388	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2019_1388.yml
Windows: Exploited CVE-2020-10189 Zoho ManageEngine	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2020_10189.yml
Windows: Suspicious PrinterPorts Creation CVE-2020-1048	EagleEye Team, Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2020_1048.yml
Windows: DNS RCE CVE-2020-1350	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2020_1350.yml
Windows: File/Folder Permissions Modifications Via Com-	Jakob Weinzettl, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_file_permission_modifications.yml

FortiSIEM Rule	Author	Source Link
mand line Utilities		
Windows: Grabbing Sensitive Hives via Reg Utility	Teymur Kheirkhabarov, Endgame, JHasenbusch, Daniil Yugoslavskiy, oscd.-community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_grabbing_sensitive_hives_via_reg.yml
Windows: Bloodhound and Sharphound Hack Tool	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hack_bloodhound.yml
Windows: Koadic Execution	wagga	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hack_koadic.yml
Windows: Rubeus Hack Tool	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hack_rubeus.yml
Windows: SecurityXploded Tool	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hack_secutyxploded.yml
Windows: HH exe Execution	E.M. Anhaus (originally from Atomic Blue Detections, Dan Beavin), oscd.-community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hh_chm.yml
Windows: CreateMiniDump Hacktool	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hktl_createminidump.yml
Windows: HTML Help Shell Spawn	Maxim Pavlunin	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_html_help_spawn.yml
Windows: Suspicious HWP Sub Processes	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hwp_exploits.yml
Windows: Impacket Lateralization Detection	Ecco	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_impacket_lateralization.yml
Windows: Indirect Command Execution	E.M. Anhaus (originally from Atomic Blue Detections,	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_indirect_cmd.yml

FortiSIEM Rule	Author	Source Link
	Endgame), oscd.community	
Windows: Suspicious Debugger Registration Cmdline	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_install_reg_debugger_backdoor.yml
Windows: Interactive AT Job	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_interactive_at.yml
Windows: Invoke-Obfuscation Obfuscated IEX Invocation when to create process	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_invoke_obfuscation_obfuscated_iex_commandline.yml
Windows: Windows Kernel and 3rd-Party Drivers Exploits Token Stealing	Teymur Kheirkhabarov (source), Daniil Yugoslavskiy (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_kernel_and_3rd_party_drivers_exploits_token_stealing.yml
Windows: MSHTA Spawned by SVCHOST	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_lethalhta.yml
Windows: Local Accounts Discovery	Timur Zinniatullin, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_local_system_owner_account_discovery.yml
Windows: LSASS Memory Dumping Using procdump	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_lsass_dump.yml
Windows: Adwind Remote Access Tool JRAT	Florian Roth, Tom Ueltschi	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mal_adwind.yml
Windows: Dridex Process Pattern	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_dridex.yml
Windows: DTRACK Malware Process Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_dtrack.yml

FortiSIEM Rule	Author	Source Link
Windows: Emotet Malware Process Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_emotet.yml
Windows: Formbook Malware Process Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_formbook.yml
Windows: QBot Process Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_qbot.yml
Windows: Ryuk Ransomware	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/win_mal_ryuk.yml ; https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_ryuk.yml
Windows: WScript or CScript Dropper	Margaritis Dimitrios (idea), Florian Roth (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_script_dropper.yml
Windows: Trickbot Malware Recon Activity	David Burkett, Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_trickbot_recon_activity.yml
Windows: WannaCry Ransomware	Florian Roth (rule), Tom U. @c_APT_ure (collection)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_wannacry.yml
Windows: MavInject Process Injection	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mavinject_proc_inj.yml
Windows: Meterpreter or Cobalt Strike Getsystem Service Start	Teymur Kheirkhabarov, Ecco	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_meterpreter_or_cobaltstrike_getsystem_service_start.yml
Windows: Mimikatz Command Line	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mimikatz_command_line.yml
Windows: MMC Spawning Windows Shell	Karneades, Swisscom CSIRT	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mmc_spawn_shell.yml

FortiSIEM Rule	Author	Source Link
Windows: Mouse Lock Credential Gathering	Cian Heasley	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mouse_lock.yml
Windows: Mshta JavaScript Execution	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.-community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mshta_javascript.yml
Windows: MSHTA Spawning Windows Shell	Michael Haag	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mshta_spawn_shell.yml
Windows: Quick Execution of a Series of Suspicious Commands	juju4	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_multiple_suspicious_cli.yml
Windows: Windows Network Enumeration	Endgame, JHasenbusch (ported for oscd.community)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_net_enum.yml
Windows: Netsh RDP Port Opening	Sander Wiebing	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_allow_port_rdp.yml
Windows: Netsh Port or Application Allowed	Markus Neis, Sander Wiebing	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_fw_add.yml
Windows: Netsh Program Allowed with Suspcious Location	Sander Wiebing	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_fw_add_susp_image.yml
Windows: Network Trace with netsh exe	Kutepov Anton, oscd.community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_packet_capture.yml
Windows: Netsh Port Forwarding	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_port_fwd.yml
Windows: Netsh RDP Port Forwarding	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_port_fwd_3389.yml
Windows: Harvesting of Wifi Credentials Using netsh exe	Andreas Hunkeler (@Karneades)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_wifi_credential_harvesting.yml

FortiSIEM Rule	Author	Source Link
Windows: Network Sniffing	Timur Zinniatullin, oscd.community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_network_sniffing.yml
Windows: New Service Creation via sc.exe	Timur Zinniatullin, Daniil Yugoslavskiy, oscd.community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_new_service_creation.yml
Windows: Non Interactive PowerShell	Roberto Rodriguez @Cyb3rWard0g (rule), oscd.-community (improvements)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_non_interactive_powershell.yml
Windows: Microsoft Office Product Spawning Windows Shell	Michael Haag, Florian Roth, Markus Neis, Elastic, FPT.EagleEye Team	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_office_shell.yml
Windows: MS Office Product Spawning Exe in User Directory	Jason Lynch	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_office_spawn_exe_from_users_directory.yml
Windows: Executable Used by PlugX in Uncommon Location	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_plugx_susp_exe_locations.yml
Windows: Possible Applocker Bypass	juju4	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_possible_applocker_bypass.yml
Windows: Detection of Possible Rotten Potato	Teymur Kheirkhabarov	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_possible_privilege_escalation_using_rotten_potato.yml
Windows: Powershell AMSI Bypass via NET Reflection	Markus Neis	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_amsi_bypass.yml
Windows: Audio Capture via PowerShell	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.-community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_audio_capture.yml
Windows: PowerShell Base64	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_

FortiSIEM Rule	Author	Source Link
Encoded Shellcode		creation/win_powershell_b64_shellcode.yml
Windows: Suspicious Bitsadmin Job via PowerShell	Endgame, JHasenbusch (ported to sigma for oscd.-community)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_bitsjob.yml
Windows: Suspicious PowerShell Execution via DLL	Markus Neis	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_dll_execution.yml
Windows: PowerShell Downgrade Attack	Harish Segar (rule)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_downgrade_attack.yml
Windows: Download via PowerShell URL	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_download.yml
Windows: FromBase64String Command Line	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_frombase64string.yml
Windows: Suspicious PowerShell Parameter Substring	Florian Roth (rule), Daniel Bohannon (idea), Roberto Rodriguez (Fix)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_suspicious_parameter_variation.yml
Windows: Suspicious XOR Encoded PowerShell Command Line	Sami Ruohonen, Harish Segar (improvement)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_xor_commandline.yml
Windows: Default PowerSploit and Empire Schtasks Persistence	Markus Neis, @Karneades	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powersploit_empire_schtasks.yml
Windows: Windows Important Process Started From Suspicious Parent Directories	vburov	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_proc_wrong_parent.yml
Windows: Bitsadmin Download	Michael Haag	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_process_creation_bitsadmin_download.yml
Windows: Process Dump via Rundll32 and Comsvcs dll	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_process_dump_rundll32_comsvcs.yml

FortiSIEM Rule	Author	Source Link
Windows: PsExec Service Start	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_psexesvc_start.yml
Windows: Query Registry	Timur Zinniatullin, oscd.community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_query_registry.yml
Windows: MSTSC Shadowing	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_rdp_hijack_shadowing.yml
Windows: RedMimicry Winnti Playbook Execute	Alexander Rausch	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_redmimicry_winnti_proc.yml
Windows: Remote PowerShell Session for creating process	Roberto Rodriguez @Cyb3rWard0g	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_remote_powershell_session_process.yml
Windows: System Time Discovery	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.-community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_remote_time_discovery.yml
Windows: Renamed Binary	Matthew Green - @mgreen27, Ecco, James Pemberton / @4A616D6573, oscd.community (improvements), Andreas Hunkeler (@Karneades)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_binary.yml
Windows: Highly Relevant Renamed Binary	Matthew Green - @mgreen27, Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_binary_highly_relevant.yml
Windows: Renamed jusched exe	Markus Neis, Swisscom	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_jusched.yml
Windows: Execution of Renamed PaExec	Jason Lynch	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_paexec.yml
Windows: Renamed PowerShell	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_powershell.yml

FortiSIEM Rule	Author	Source Link
Windows: Renamed ProcDump	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_procdump.yml
Windows: Renamed PsExec	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_psexec.yml
Windows: Run PowerShell Script from ADS	Sergey Soldatov, Kaspersky Lab, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_run_powershell_script_from_ads.yml
Windows: Possible Shim Database Persistence via sdbinst exe	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_sdbinst_shim_persistence.yml
Windows: Manual Service Execution	Timur Zinniatullin, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_service_execution.yml
Windows: Stop Windows Service	Jakob Weinzettl, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_service_stop.yml
Windows: Shadow Copies Access via Symlink	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_shadow_copies_access_symlink.yml
Windows: Shadow Copies Creation Using Operating Systems Utilities	Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_shadow_copies_creation.yml
Windows: Shadow Copies Deletion Using Operating Systems Utilities	Florian Roth, Michael Haag, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_shadow_copies_deletion.yml
Windows: Windows Shell Spawning Suspicious Program	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_shell_spawn_susp_program.yml
Windows: SILENTTRINITY Stager Execution	Aleksey Potapov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_silenttrinity_stage_use.yml
Windows: Audio Cap-	E.M. Anhaus (ori-	https://-

FortiSIEM Rule	Author	Source Link
ture via SoundRecorder	ginally from Atomic Blue Detections, Endgame), oscd.-community	github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_soundrec_audio_capture.yml
Windows: Possible SPN Enumeration	Markus Neis, keepwatch	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_spn_enum.yml
Windows: Possible Ransomware or Unauthorized MBR Modifications	@neu5ron	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_bcdedit.yml
Windows: Application Allowlisting Bypass via Bginfo	Beyu Denis, oscd.-community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_bginfo.yml
Windows: Suspicious Calculator Usage	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_calc.yml
Windows: Possible App Allowlisting Bypass via WinDbg CDB as a Shell code Runner	Beyu Denis, oscd.-community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_cdb.yml
Windows: Suspicious Certutil Command	Florian Roth, juju4, keepwatch	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_certutil_command.yml
Windows: Certutil Encode	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_certutil_encode.yml
Windows: Suspicious Commandline Escape	juju4	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_cli_escape.yml
Windows: Command Line Execution with Suspicious URL and AppData Strings	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_cmd_http_appdata.yml
Windows: Suspicious Code Page Switch	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_codepage_switch.yml
Windows: Recon-	Florian Roth,	https://-

FortiSIEM Rule	Author	Source Link
naissance Activity with Net Command	Markus Neis	github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_commands_recon_activity.yml
Windows: Suspicious Compression Tool Parameters	Florian Roth, Samir Bousseaden	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_compression_params.yml
Windows: Process Dump via Comsvcs DLL	Modexp (idea)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_comsvcs_procdump.yml
Windows: Copy from Admin Share	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_copy_lateral_movement.yml
Windows: Suspicious Copy From or To System32	Florian Roth, Markus Neis	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_copy_system32.yml
Windows: Covenant Launcher Indicators	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_covenant.yml
Windows: CrackMapExec Command Execution	Thomas Patzke	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_crackmapexec_execution.yml
Windows: CrackMapExec PowerShell Obfuscation	Thomas Patzke	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_crackmapexec_powershell_obfuscation.yml
Windows: Suspicious Parent of Csc.exe	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_csc.yml
Windows: Suspicious Csc.exe Source File Folder	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_csc_folder.yml
Windows: Suspicious Curl Usage on Windows	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_curl_download.yml
Windows: Suspicious Curl File Upload	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_curl_fileupload.yml
Windows: Curl Start Combination	Sreeman	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_curl_start_combo.yml

FortiSIEM Rule	Author	Source Link
Windows: ZOHO Dctask64 Process Injection	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_dctask64_proc_inject.yml
Windows: Suspicious Desktopimgdownldr Command	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_desktopimgdownldr.yml
Windows: Devtoolslauncher.exe Executing Specified Binary	Beyu Denis, oscd.community (rule), @_felamos (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_devtoolslauncher.yml
Windows: Direct Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_direct_asep_reg_keys_modification.yml
Windows: Disabled IE Security Features	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_disable_ie_features.yml
Windows: DIT Snapshot Viewer Use	Furkan Caliskan (@caliskanfurkan_)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ditsnap.yml
Windows: Application Allowlisting Bypass via Dnx.exe	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_dnx.yml
Windows: Suspicious Double File Extension	Florian Roth (rule), @blu3_team (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_double_extension.yml
Windows: Application Allowlisting Bypass via Dxcap.exe	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_dxcap.yml
Windows: Suspicious Eventlog Clear or Configuration Using Wevtutil or Powershell or Wmic	Ecco, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_eventlog_clear.yml
Windows: Executables Started in Suspicious Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_exec_folder.yml
Windows: Execution in Non-Executable Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_execution_path.yml
Windows: Execution	Florian Roth	https://-

FortiSIEM Rule	Author	Source Link
in Webserver Root Folder		github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_execution_path_webserver.yml
Windows: Explorer Root Flag Process Tree Break	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_explorer_break_proctree.yml
Windows: Suspicious File Characteristics Due to Missing Fields	Markus Neis, Sander Wiebing	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_file_characteristics.yml
Windows: Findstr Launching lnk File	Trent Liffick	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_findstr_lnk.yml
Windows: Firewall Disabled via Netsh	Fatih Sirin	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_firewall_disable.yml
Windows: Fsutil Suspicious Invocation	Ecco, E.M. Anhaus, oscd.community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_fsutil_usage.yml
Windows: Suspicious GUP.exe Usage	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_gup.yml
Windows: IIS Native-Code Module Command Line Installation	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_iss_module_install.yml
Windows: Windows Defender Download Activity	Matthew Matchen	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_mpcmdrun_download.yml
Windows: Suspicious MsiExec Directory	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_msiexec_cwd.yml
Windows: MsiExec Web Install	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_msiexec_web_install.yml
Windows: Malicious Payload Download via Office Binaries	Beyu Denis, oscd.-community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_msoffice.yml
Windows: Net.exe Execution For Discovery	Michael Haag, Mark Woan (improvements), James Pem-	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_net_execution.yml

FortiSIEM Rule	Author	Source Link
	berton / @4A616D6573 / oscd.community (improvements)	
Windows: Suspicious Netsh.DLL Persistence	Victor Sergeev, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_netsh_dll_persistence.yml
Windows: Invocation of Active Directory Diagnostic Tool ntdsutil exe	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ntdsutil.yml
Windows: Application Allowlisting Bypass via DLL Loaded by odbcconf exe	Kirill Kiryanov, Beyu Denis, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_odbcconf.yml
Windows: OpenWith.exe Executing Specified Binary	Beyu Denis, oscd.community (rule), @harr0ey (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_openwith.yml
Windows: Suspicious Execution from Outlook	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_outlook.yml
Windows: Execution in Outlook Temp Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_outlook_temp.yml
Windows: Ping Hex IP	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ping_hex_ip.yml
Windows: Empire PowerShell Launch Parameters	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_empire_launch.yml
Windows: Empire PowerShell UAC Bypass	Ecco	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_empire_uac_bypass.yml
Windows: Suspicious Encoded PowerShell Command Line	Florian Roth, Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_enc_cmd.yml
Windows: PowerShell Encoded Character Syntax	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_encoded_param.yml

FortiSIEM Rule	Author	Source Link
Windows: Malicious Base64 Encoded PowerShell Keywords in Command Lines	John Lambert (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_hidden_b64_cmd.yml
Windows: Suspicious PowerShell Invocation Based on Parent Process	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_parent_combo.yml
Windows: Suspicious PowerShell Parent Process	Teymur Kheirkhabarov, Harish Segar (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_parent_process.yml
Windows: Suspicious Use of Procdump	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_procdump.yml
Windows: Programs starting from Suspicious Location	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_prog_location_process_starts.yml
Windows: PowerShell Script Run in AppData	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ps_appdata.yml
Windows: PowerShell DownloadFile	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ps_downloadfile.yml
Windows: Psr.exe Capture Screenshots	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_psr_capture_screenshots.yml
Windows: Rar with Password or Compression Level	@ROxPinTeddy	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_rar_flags.yml
Windows: Suspicious RASdial Activity	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_rasdial_activity.yml
Windows: Suspicious Reconnaissance Activity via net group or localgroup	Florian Roth, omkar72	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_recon_activity.yml
Windows: Suspicious Regsvr32 Usage	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_regsvr32_anomalies.yml

FortiSIEM Rule	Author	Source Link
Windows: Regsvr32 Flags Anomaly	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_regsvr32_flags_anomaly.yml
Windows: Renamed ZOHO Dctask64	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_renamed_dctask64.yml
Windows: Renamed SysInternals Debug View	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_renamed_debugview.yml
Windows: Suspicious Process Start Locations	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_run_locations.yml
Windows: Suspicious Arguments in Rundll32 Usage	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_rundll32_activity.yml
Windows: Suspicious DLL Call by Ordinal	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_rundll32_by_ordinal.yml
Windows: Scheduled Task Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_schtask_creation.yml
Windows: WSF JSE JS VBA VBE File Execution	Michael Haag	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_script_execution.yml
Windows: Suspicious Service Path Modification	Victor Sergeev, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_service_path_modification.yml
Windows: Squirrel Lolbin	Karneades / Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_squirrel_lolbin.yml
Windows: Suspicious Svchost Process	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_svchost.yml
Windows: Suspect Svchost Activity	David Burkett	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_svchost_no_cli.yml
Windows: Sysprep on AppData Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_sysprep_appdata.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious SYSVOL Domain Group Policy Access	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_sysvol_access.yml
Windows: Taskmgr Created By Local SYSTEM Account	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_taskmgr_localsystem.yml
Windows: Process Launch from Taskmgr	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_taskmgr_parent.yml
Windows: Suspicious tscon.exe Created By Local SYSTEM Account	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_tscon_localsystem.yml
Windows: Suspicious RDP Redirect Using tscon.exe	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_tscon_rdp_redirect.yml
Windows: Suspicious Use of CSharp Interactive Console	Michael R. (@nahamike01)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_use_of_csharp_console.yml
Windows: Suspicious Userinit Child Process	Florian Roth (rule), Samir Bousseaden (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_userinit_child.yml
Windows: Whoami Execution	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_whoami.yml
Windows: Suspicious WMI Execution	Michael Haag, Florian Roth, juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_wmi_execution.yml
Windows: Sysmon Driver Unload	Kirill Kiryanov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_sysmon_driver_unload.yml
Windows: System File Execution Location Anomaly	Florian Roth, Patrick Bareiss	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_system_exe_anomaly.yml
Windows: Tap Installer Execution	Daniil Yugoslavskiy, Ian Davis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_tap_installer_execution.yml
Windows: Tasks Folder Evasion	Sreeman	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_

FortiSIEM Rule	Author	Source Link
		creation/win_task_folder_evasion.yml
Windows: Terminal Service Process Spawn	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_termserv_proc_spawn.yml
Windows: Domain Trust Discovery	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community, omkar72	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_dsquery_domain_trust_discovery.yml ; https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_trust_discovery.yml
Windows: Bypass UAC via CMSTP	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.-community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_uac_cmstp.yml
Windows: Bypass UAC via Fodhelper.exe	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_uac_fodhelper.yml
Windows: Bypass UAC via WSReset exe	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_uac_wsreset.yml
Windows: Possible Privilege Escalation via Weak Service Permissions	Teymur Kheirkhabarov	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_using_sc_to_change_sevice_image_path_by_non_admin.yml
Windows: Java Running with Remote Debugging	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_vul_java_remote_debugging.yml
Windows: Webshell Detection With Command Line Keywords	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_webshell_detection.yml
Windows: Webshell Recon Detection Via CommandLine Processes	Cian Heasley	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_webshell_recon_detection.yml
Windows: Shells	Thomas Patzke	https://-

FortiSIEM Rule	Author	Source Link
Spawned by Web Servers		github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_webshell_spawn.yml
Windows: Run Whoami as SYSTEM	Teymur Kheirkhabarov	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_whoami_as_system.yml
Windows: Windows 10 Scheduled Task SandboxEscaper 0-day	Olaf Hartong	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_win10_sched_task_0day.yml
Windows: WMI Backdoor Exchange Transport Agent	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_wmi_backdoor_exchange_transport_agent.yml
Windows: WMI Persistence - Script Event Consumer	Thomas Patzke	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_wmi_persistence_script_event_consumer.yml
Windows: WMI Spawning Windows PowerShell	Markus Neis / @Karneades	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_wmi_spwns_powershell.yml
Windows: Wmiprvse Spawning Process	Roberto Rodriguez @Cyb3rWard0g	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_wmiprvse_spawning_process.yml
Windows: Microsoft Workflow Compiler	Nik Seetharaman	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_workflow_compiler.yml
Windows: Wsreset UAC Bypass	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_wsreset_uac_bypass.yml
Windows: XSL Script Processing	Timur Zinniatullin, oscd.community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_xsl_script_processing.yml
Windows: Leviathan Registry Key Activity	Aidan Bracher	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_apt_leviathan.yml
Windows: OceanLotus Registry Activity	megan201296	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_apt_oceanlotus_registry.yml
Windows: Pandemic Registry Key	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_apt_pandemic.yml

FortiSIEM Rule	Author	Source Link
Windows: Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, oscd.community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_asep_reg_keys_modification.yml
Windows: Suspicious New Printer Ports in Registry CVE-2020-1048	EagleEye Team, Florian Roth, NVISO	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_cve-2020-1048.yml
Windows: DHCP Callout DLL Installation	Dimitrios Slamaris	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_dhcp_calloutdll.yml
Windows: Disable Security Events Logging Adding Reg Key MiniNt	Ilyas Ochkov, oscd.-community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_disable_security_events_logging_adding_reg_key_minint.yml
Windows: DNS ServerLevelPluginDll Install	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_dns_serverlevelplugindll.yml
Windows: COMPlus-ETWEnabled Registry Modification	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_etw_modification.yml ; https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_etw_disabled.yml
Windows: Windows Credential Editor Install Via Registry	Florian Roth	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_hack_wce_reg.yml
Windows: Logon Scripts User-InitMprLogonScript Registry	Tom Ueltschi (@c_APT_ure)	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_logon_scripts_userinitmprlogonscript_reg.yml
Windows: Narrator s Feedback-Hub Persistence	Dmitriy Lifanov, oscd.community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_narrator_feedback_persistance.yml
Windows: New DLL Added to AppCertDlls Registry Key	Ilyas Ochkov, oscd.-community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_new_dll_added_to_appcertdlls_registry_key.yml
Windows: New DLL Added to AppInit-DLLs Registry Key	Ilyas Ochkov, oscd.-community	https://-github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_new_dll_added_to_appinit_dlls_registry_key.yml

FortiSIEM Rule	Author	Source Link
Windows: Possible Privilege Escalation via Service Permissions Weakness	Teymur Kheirkhabarov	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_possible_privilege_escalation_via_service_registry_permissions_weakness.yml
Windows: RDP Registry Modification	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_rdp_registry_modification.yml
Windows: RDP Sensitive Settings Changed	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_rdp_settings_hijack.yml
Windows: RedMimicry Winnti Playbook Registry Manipulation	Alexander Rausch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_redmimicry_winnti_reg.yml
Windows: Office Security Settings Changed	Trent Liffick (@tliffick)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_reg_office_security.yml
Windows: Windows Registry Persistence COM Key Linking	Kutepov Anton, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_registry_persistence_key_linking.yml
Windows: Windows Registry Persistence COM Search Order Hijacking	Maxime Thiebaut (@0xThiebaut)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_registry_persistence_search_order.yml
Windows: Windows Registry Trust Record Modification	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_registry_trust_record_modification.yml
Windows: Security Support Provider SSP Added to LSA Configuration	iwillkeepwatch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_ssp_added_lsa_config.yml
Windows: Sticky Key Like Backdoor Usage	Florian Roth, @twjackomo	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_stickykey_like_backdoor.yml
Windows: Suspicious RUN Key from Download	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_download_run_key.yml
Windows: DLL Load via LSASS	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_lsass_dll_load.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious Camera and Microphone Access	Den Iuzvyk	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_mic_cam_access.yml
Windows: Registry Persistence via Explorer Run Key	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_reg_persist_explorer_run.yml
Windows: New RUN Key Pointing to Suspicious Folder	Florian Roth, Markus Neis, Sander Wiebing	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_run_key_img_folder.yml
Windows: Suspicious Service Installed	xknow (@xknow_infosec), xorxes (@xor_xes)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_service_installed.yml
Windows: Suspicious Keyboard Layout Load	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_suspicious_keyboard_layout_load.yml
Windows: Usage of Sysinternals Tools	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_sysinternals_eula_accepted.yml
Windows: UAC Bypass via Event Viewer	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_uac_bypass_eventvwr.yml
Windows: UAC Bypass via Sdclt	Omer Yampel	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_uac_bypass_sdclt.yml
Windows: Registry Persistence Mechanisms	Karneades	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_win_reg_persistence.yml
Windows: Azure Browser SSO Abuse	Den Iuzvyk	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_abusing_azure_browser_sso.yml
Windows: Executable in ADS	Florian Roth, @0xrawsec	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_ads_executable.yml
Windows: Alternate PowerShell Hosts Pipe	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_alternate_powershell_hosts_pipe.yml

FortiSIEM Rule	Author	Source Link
Windows: Turla Group Named Pipes	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_apt_turla_namedpipes.yml
Windows: CactusTorch Remote Thread Creation	@SBousseaden (detection), Thomas Patzke (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_cactustorch.yml
Windows: CMSTP Execution	Nik Seetharaman	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_cmstp_execution.yml
Windows: CobaltStrike Process Injection	Olaf Hartong, Florian Roth, Aleksey Potapov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_cobaltstrike_process_injection.yml
Windows: CreateRemoteThread API and LoadLibrary	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_createremotethread_loadlibrary.yml
Windows: Cred Dump Tools Via Named Pipes	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_cred_dump_tools_named_pipes.yml
Windows: Malicious Named Pipe	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_mal_namedpipes.yml
Windows: Password Dumper Remote Thread in LSASS	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_password_dumper_lsass.yml
Windows: Possible DNS Rebinding	Ilyas Ochkov, oscd.community	https://github.

FortiSIEM Rule	Author	Source Link
		com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_possible_dns_rebinding.yml
Windows: Raw Disk Access Using Illegitimate Tools	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_raw_disk_access_using_illegitimate_tools.yml
Windows: PowerShell Rundll32 Remote Thread Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_susp_powershell_rundll32.yml
Windows: Suspicious Remote Thread Created	Perez Diego (@darkquassar), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_suspicious_remote_thread.yml
Windows: WMI Event Subscription	Tom Ueltschi (@c_APT_ure)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_wmi_event_subscription.yml
Windows: Suspicious Scripting in a WMI Consumer	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_wmi_susp_scripting.yml

License Enforcement

This section describes how FortiSIEM enforces CMDB Device license, Agent license and EPS License.

CMDB Device License Enforcement

Customer purchases an overall CMDB Device license, which specifies how many managed devices can be stored in CMDB. Managed devices can send logs and can be monitored. In an MSSP environment, customer can set a device limit for a specific organization in **Admin > Setup > Organizations > Edit** or **New > Max Devices**. The following device types are excluded from license:

- Devices > Mobile
- Devices > VoIP
- Devices > Decommission
- Devices with Status = Unmanaged.

When you try to add a device to the system, either via discovery or manually, then the global device limit and the per-org device limit is enforced. If the limit is reached, then the device is either not added to CMDB or added and set as Unmanaged. If you decommission a managed device, then the license is returned to the pool. If you recommission a device, then a license is consumed.

CMDB Device License is shown in **Admin > License > General** and the usage is shown in **Admin > License > Usage > Device Usage**.

Agent License Enforcement

Customer purchases Agent License, which specifies how many Agents can register and send events. CMDB Device License is shown in **Admin > License > General** and the usage is shown in **Admin > License > Usage > Agent Usage**.

If Agent License limit is reached, then a new Agent cannot register. If Agent license is reduced to lower than the number of registered Agents, then a few agents are randomly unregistered to bring the value lower than licensed limit.

EPS License Enforcement

Mechanism

FortiSIEM is a distributed system consisting of Supervisor, Worker and Collector nodes. Events can be received at any node and the `phParser` module at that node handles the events and enforces EPS license. An Elastic EPS allocation method distributes unused EPS to the node where it is needed the most.

- Every 3 minutes, `phParser` module on every node calculates *Incoming* EPS and sends it to the Supervisor node.
- Every 3 minutes, `phParser` module on Supervisor node collects *Incoming* EPS from all nodes and calculates *Allocated* EPS and *Unused* Events to be used by every node for the next 3 minutes. unused event is the difference between licensed EPS and incoming EPS accumulated since the system is installed. These parameters are sent to the `phParser` modules on every node. The following information is used to calculate *Allocated* EPS:
    - Global Licensed EPS
    - Collector Guaranteed EPS (note the total Guaranteed EPS for all Collectors must be less than Global Licensed EPS).
    - Incoming EPS
- For the next 3 minutes, the `phParser` module enforces license based on *Allocated EPS and Unused Events information received from the Supervisor node*. At the end of 3 minutes, it sends incoming EPS to the Supervisor node and the cycle continues.

Collector enforces Licensed EPS as follows:

- If incoming EPS is *less* than licensed EPS, events are ingested with no event drop.
- If incoming EPS is *more* than licensed EPS, then the following steps are taken.
    - Unused events are allocated.
    - After consuming unused events, if incoming EPS still exceeds (1.1 * Licensed EPS), then incoming events are dropped. For example, if licensed EPS is 5k, so FortiSIEM allows (5000 * 1.1 * 180 = 990000) events in each 3-minute window, after using up unused events. `phParser` will parse the first 990,000 events and drop the others in the 3-minute window.

Events

phParser on every node generates the following PH_SYSTEM_EPS_NODE event every 3 minutes. To query these system events, the Analytics search filter must also include “System Event Category” = 3.

```
[PH_SYSTEM_EPS_NODE]:[eventSeverity]=PHL_INFO,[fileName]=parserProcess.cpp,[lineNumber]=6169,
[role]=Super,[hostName]=FSM-Host,[incomingEventsPerSec]=10.0,[peakIncomingEventsPerSec]=35.0,
[dropPolicyEvents]=0,[dropPolicyEventsPerSec]=0.0,
[peakDropPolicyEventsPerSec]=0.0,[dropLicenseEvents]=0,[dropLicenseEventsPerSec]=0.0,
[peakDropLicenseEventsPerSec]=0.0,[dropLicenseEventRatio]=0
```

Attributes:

- incomingEventsPerSec: Total received events in 3 minutes divided by 180.
- peakIncomingEventsPerSec: The maximum value of incomingEventsPerSec over all 3-minute periods, since phParser started.
- dropPolicyEvents: The number of events that are dropped by Event Dropping rules in last 3 minutes.
- dropPolicyEventsPerSec: dropPolicyEvents divided by 180.
- peakDropPolicyEventsPerSec: The maximum value of dropPolicyEventsPerSec over all 3-minute periods, since phParser started.
- dropLicenseEvents: The number of events that are dropped because of exceeding license in last 3 minutes.
- dropLicenseEventsPerSec: dropLicenseEvents divided by 180.
- peakDropLicenseEventsPerSec: The maximum value of dropLicenseEventsPerSec over all 3-minute periods, since phParser started.
- dropLicenseEventRatio: Ratio of dropped events because of license to total incoming events in last 3 minutes.

phParser on Supervisor node generates the following PH_SYSTEM_EPS_ORG event every 3 minutes. This event provides Organization level EPS information by combining information from every node.

```
[PH_SYSTEM_EPS_ORG]:[eventSeverity]=PHL_INFO,[fileName]=parserProcess.cpp,[lineNumber]=6205,
[phCustId]=1,[customer]=Super,[incomingEventsPerSec]=0.000000,[peakIncomingEventsPerSec]=0.000000,
[dropLicenseEventsPerSec]=0.000000,
[peakDropLicenseEventsPerSec]=0.000000,[phLogDetail]=
```

Attributes:

- customer: name of organization
- incomingEventsPerSec: Total received events in 3 minutes divided by 180 for this Organization.
- peakIncomingEventsPerSec: The maximum value of incomingEventsPerSec over all 3-minute periods for this Organization, since phParser started.
- dropLicenseEvents: The number of events that are dropped because of exceeding license in last 3 minutes.
- dropLicenseEventsPerSec: dropLicenseEvents divided by 180.
- peakDropLicenseEventsPerSec: The maximum value of dropLicenseEventsPerSec over all 3-minute periods, since phParser started.

phParser on Supervisor node generates the following PH_SYSTEM_EPS_GLOBAL event every 3 minutes. This event provides Global EPS information by combining information from every node.

```
[PH_SYSTEM_EPS_GLOBAL]:[eventSeverity]=PHL_INFO,[fileName]=parserProcess.cpp,[lineNumber]=6252,
[licenseEventsPerSec]=13000,[incomingEventsPerSec]=0.000000,
[peakIncomingEventsPerSec]=0.000000,[dropLicenseEventsPerSec]=0.000000,[peak-
DropLicenseEventsPerSec]=0.000000,[unusedEvents]=1897731307,[phLogDetail]=
```

Attributes:

- `licenseEventsPerSec`: Global licensed events per second
- `incomingEventsPerSec`: Total received events in 3 minutes divided by 180.
- `peakIncomingEventsPerSec`: The maximum value of `incomingEventsPerSec` over all 3-minute periods for this Organization, since `phParser` started.
- `dropLicenseEvents`: The number of events that are dropped because of exceeding license in last 3 minutes.
- `dropLicenseEventsPerSec`: `dropLicenseEvents` divided by 180.
- `peakDropLicenseEventsPerSec`: The maximum value of `dropLicenseEventsPerSec` over all 3-minute periods, since `phParser` started.
- `unusedEvents`: difference between `licenseEventsPerSec` and `incomingEventsPerSec` accumulated since system installed.

`phParser` on an event handling node (e.g. a Collector) generates the following `PH_SYSTEM_EVENT_RATE_EXCEED_LICENSE` event when it starts to drop events.

```
<174>Mar 12 11:33:20 PARSER-HOST phParser[1234]: [PH_SYSTEM_EVENT_RATE_EXCEED_
LICENSE]: [eventSeverity]=PHL_INFO,[procName]=phParser,[fileName]=parserProcess.cpp,
[eventsPerSec]=120.49,[phLogDetail]=120.49 events/sec exceeds licensed event rate of
100 events/sec
```

Attributes:

- `eventsPerSec`: Total received events per second

`phParser` on Supervisor node generates the following `PH_PARSER_GLOBAL_LICENSE_EXCEED` event every 3 minutes, when it sees dropped events.

```
[PH_PARSER_GLOBAL_LICENSE_EXCEED]:[eventSeverity]=PHL_ERROR,[fileName]-
]=LicenseEnforce.cpp,[lineNumber]=1098,[phLogDetail]=Elastic EPS: global license has
already exceeded, cannot realloc
```

In this case, the following incidents “FortiSIEM EPS License Exceeded” and “External Event Dropped By License” triggers.

Python Threat Feed Framework

In release 7.0.0, FortiSIEM introduces a Python framework for FortiSIEM threat feed integrations.

Traditionally, customers or technical assistance center (TAC) engineers had to use a Java package framework to build threat feed integrations. However, adoption of the Java based framework was extremely low. This feature uses the Python framework to make custom threat feed integrations more accessible, with a well defined structure for data.

In this framework, FortiSIEM calls a Python module based threat feed, passing it a number of arguments necessary for communication with a threat feed. This framework then writes the threat entries to a CSV file which AppServer will parse. The framework is also extendable. If the customer knows the natural ID of the threat feed, the customer can run a script externally from FortiSIEM, providing their username and password for basic authentication to call AppServer’s API to update the threat feed.

Updating a threat feed via Python can be done in two ways.

- **FortiSIEM Internal Threat Feed Update**: Python integration built into FortiSIEM – Threat feed update schedule passes standard set of arguments to python script, which uses these to obtain threat feed information, and saves it to CSV file for AppServer to process.
- **FortiSIEM External Threat Feed Update**: Python integration is executed externally from FortiSIEM in some customer environment. Provided customer has access to FortiSIEM credential, Threat feed natural ID, Threat feed URL and credentials. Python script collects threat feed data, and does an HTTP POST to FortiSIEM to push the data to Threat feed via API.

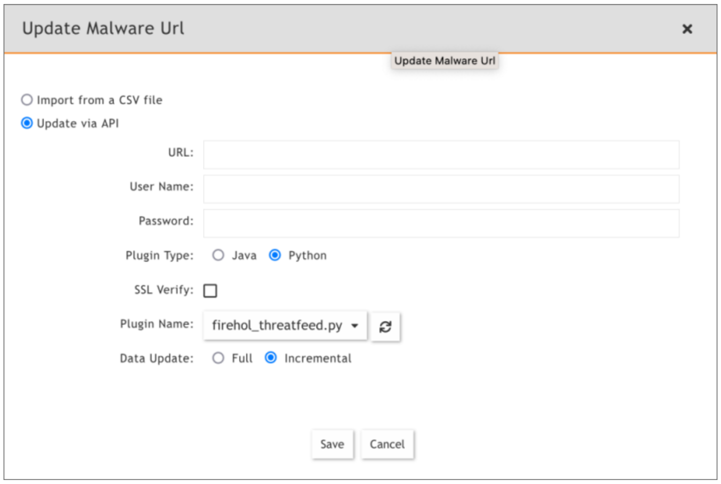
To update a threat feed, you will need to take the following steps.

1. From the new threat feed, obtain the URL endpoint, and credentials, if applicable.
2. Create your custom Python threat feed integration by taking the following steps.
   a. Obtain a copy of the Firehol and/or Anomail (TAXII2.x) threat feed integration script.
   b. Place your Python script in the `/opt/phoenix/data-definition/threatfeedIntegrations/` folder on the FortiSIEM Supervisor.
3. From the FortiSIEM Supervisor GUI, navigate to **RESOURCES**, and from the left pane, select **Malware Domains**, **Malware IPs**, **Malware Hash**, or **Malware URLs**.
4. In the same left pane, click **+** to create a new Malware Threat Feed Group.
5. From the Create New Malware Group Window, take the following steps.
   a. In the **Group** field, enter a name for the Malware Group threat feed.
   b. In the **Description** field, enter any information you wish to make available about the Malware Group threat feed.
   c. If Malware IPs was selected, from the Value Type drop-down list, select **IP** or **IP Range**.
   d. Click **Save**.
6. Select your malware threat feed group from the left pane, and from the main pane, click on **More**, and select **Update**.
7. From the Update Malware window, take the following steps.
   a. Select **Update via API**.
   b. From the **URL** row, click the Edit icon.
   c. In the **URL** field, enter the threat feed endpoint being used by your custom threat feed service.
   Note: Ensure you enter the http:// or https:// prefix.
   d. In the **User Name** field, if required, enter the user name associated with the API access.
   Note: Your script can manipulate these fields. If the threat feed requires an API key, you can simply place that in the password field, and dummy value in the username field.
   e. In the **Password** field, enter the password associated with the user name.
   f. For **Plugin Type**, select **Python**.
   g. In the **Plugin Class** row, click the refresh button next to plugin class to refresh the list of python integrations available. This enumerates all .py files in the `/opt/phoenix/data-definition/threatfeedIntegrations/` folder.
   h. Select your Python file from the drop-down list.
   Note: You can click the refresh icon to refresh the drop-down list after copying your .py file to the `/opt/phoenix/data-definition/threatfeedIntegrations/` folder.

i. For **Data Update**, select **Full** or **Incremental**.

Option	Description
Full	Each time a scheduled trigger occurs, your threat feed data will be completely replaced with a new copy. In most cases, select “Full” to prevent accumulation of ineffective/aged threat indicators.
Incremental	Preserves existing data, and adds to it.

j. Click **Save**.



Update Malware Url

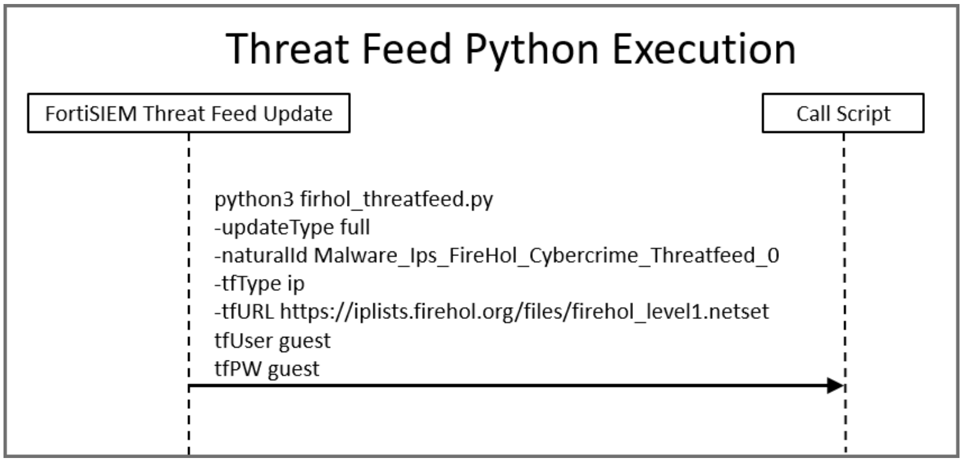
○ Import from a CSV file
● Update via API

URL:
User Name:
Password:
Plugin Type: ○ Java ● Python
SSL Verify: □
Plugin Name: firehol_threatfeed.py
Data Update: ○ Full ● Incremental

8. To create a schedule, see Specifying a Schedule.
After the first schedule has been executed, confirm that the entries are populated.

Threat Feed Workflow

In this scenario, FortiSIEM’s threat feed update schedule will gather the threat feed configuration data you provided during setup, and pass those as arguments to your custom python script. If you use Fortinet's provided framework, the threat feed data can be passed to a function which will store the data in the appropriate cache folder to update FortiSIEM.

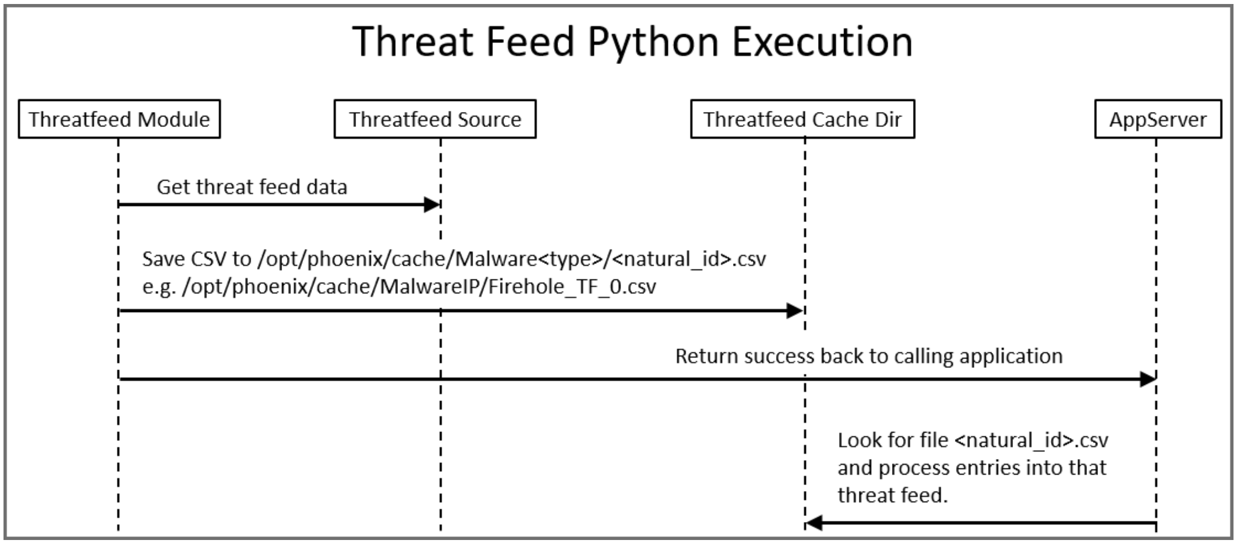


```
python3 firhol_threatfeed.py
-updateType full
-naturalId Malware_Ips_FireHol_Cybercrime_Threatfeed_0
-tfType ip
-tfURL https://iplists.firehol.org/files/firehol_level1.netset
tfUser guest
tfPW guest
```

Internal/Scheduled by FortiSIEM Execution Scenario:

In this scenario, the python script, when called by FortiSIEM, obtains the threat feed data from the remote source, parses the data into a list of dictionary objects, and passes that to a framework function which will save it to a local CSV file on the FortiSIEM Supervisor.

Remember that your custom python script must exist on the Supervisor, and be placed in this folder: `/opt/phoenix/data-definition/threatfeedIntegrations/`


Threat Feed Python Execution
Threatfeed Module
Threatfeed Source
Threatfeed Cache Dir
AppServer
Get threat feed data
Save CSV to /opt/phoenix/cache/Malware<type>/<natural_id>.csv
e.g. /opt/phoenix/cache/MalwareIP/Firehole_TF_0.csv
Return success back to calling application
Look for file <natural_id>.csv and process entries into that threat feed.

External Execution Scenario:

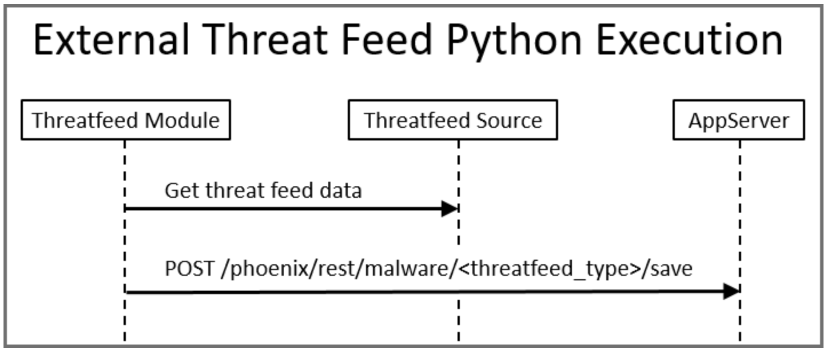
For Advanced Users Only: In this scenario, you can download all these python scripts to a remote location (not on FortiSIEM Supervisor), and execute the threat feed update. This however, requires that you securely store all the required arguments needed, and pass them to the script on execution. In addition, you need to provide the script 3 extra arguments (FortiSIEM base URL, a FortiSIEM user account with authorization (org/user), and FortiSIEM password)

In this scenario, the script uses the FortiSIEM public API to POST threat feed data in a defined JSON format.

Note: The naturalId of the threat feed you created is the most difficult item to obtain here, you must obtain it via Postgres in order to run it externally to FortiSIEM.

Listing available threat feeds to update:

```
select display_name,natural_id from ph_group where type=27;
        display_name          |             natural_id
------------------------------+-------------------------------------
 Emerging Threat Malware IP  | PH_SYS_EMER_THREAT
 ThreatStream Malware IP     | PH_SYS_THREATSTREAM_BLOCKED_IP
 FortiGuard Malware IP       | PH_SYS_FORTIGUARD_BLOCKED_IP
 TruSTAR Malware IP          | PH_SYS_TRUSTAR_BLOCKED_IP
 ThreatConnect Malware IP    | PH_SYS_THREATCONNECT_BLOCKED_IP
 Dragos Worldview Malware IP | PH_SYS_DRAGOSWORLDVIEW_BLOCKED_IP
```


External Threat Feed Python Execution
Threatfeed Module
Threatfeed Source
AppServer
Get threat feed data
POST /phoenix/rest/malware/<threatfeed_type>/save

Threatfeed Module

The threat feed package is located here: `/opt/phoenix/data-definition/threatfeedIntegrations/`

Directory Structure

The Threatfeed module directory consists of the following files and folders.

Directory File/Folder	Description
anomaly_threatfeed.py	An example working threat feed file implementing TAXII2.0 and TAXII2.1 threat feed integration. This is actually implemented in the helper modules “threat-feed_integration”.
firehol_threatfeed.py	An example working threat feed file implementing Firehol IP threat feeds.
fsiem_utils/	This is the package directory for the “fsiem_utils” python package.
fsiem_utils/__init__.py	Empty, simply the designated directory for package.
fsiem_utils/threatfeed_integration.py	Helper module defining the classes representing a threat feed integration and data objects.

Overview of Threat Feed Integrations

Required import: from fsiem_utils.threatfeed_integration import

All custom threat feeds inherit from the parent class ThreatfeedIntegration using the following statement:

class MyCustomThreatFeed(ThreatfeedIntegration):

This parent class handles a lot of the internals of handling input arguments and handling format of data that FortiSIEM can understand.

Script Input Arguments

The sample threat feeds have built in handling for the expected script input, so do not deviate from them. You can merely replace your custom class name with the existing example.

- Required Input Arguments: updateType,naturalId,tfType,tfURL
- (Optional) Input Arguments: tfUser,tfPW, appUser = None, appPW = None, appHost = 'https://127.0.0.1')

Data Object Classes

For ease of formatting data to FortiSIEM expected format, Fortinet has a number of helper classes for representation of an IP object, URL object, Domain object,, or Hash object.

Data Object Class Member Functions

<data_obj>.get_dict() – Returns dictionary form of object

Each of the classes representing a threat feed object (IP_entry, URL_entry, Domain_entry, and Hash_entry) have a function called get_dict() that returns the dictionary representation of the object, which is on the format that AppServer expects. This can be dumped to JSON, which will be in AppServer's public API json format, or it can be dumped to CSV where the field order is preserved.

Class IP_entry()

Creates an object representing a single IP and/or contiguous network range indicator

Example Definition

IP_entry(name="Test IP",low_ip="1.1.1.1",high_ip="2.2.2.2",description="This is ransomware C2 server",date_found-d=now)

Required Arguments

- name
- low_ip

Optional Arguments

- high_ip
- malware_type
- confidence
- severity
- asn
- org
- country
- description
- date_found – datetime object
- lastSeen – datetime object

Class Domain_entry()

Creates an object representing a single domain indicator.

Example Definition

Domain_entry(domainName="google.com",ip="9.9.9.9")

Required Arguments

- domainName

Optional Arguments

- ip
- reverseLookup
- malware_type
- confidence
- severity
- asn
- org
- country
- description
- date_found – datetime object
- lastSeen – datetime object

Class URL_entry()

Creates an object representing a single URL indicator.

Example Definition

URL_entry(url="google.com/test2.xml",origin="https://google.com",description="Test URL")

Required Arguments

- url

Optional Arguments

- origin
- malware_type
- confidence
- description
- lastSeen – datetime object

Class Hash_entry()

Creates an object representing a single hash indicator.

Example Definition

Hash_entry(name="REvil Hash1",algorithm="SHA256",hashcode="XXXXXXXXX",description="test")

Required Arguments

- names
- algorithm
- hashcode

Optional Arguments

- controller_ip
- malware_type
- confidence
- severity
- asn
- org
- country
- description
- date_found – datetime object
- lastSeen – datetime object

Important Member Variables of the ThreatfeedIntegration Class

If you properly follow the example threat feeds by inheriting from the ThreatfeedIntegration class, these are automatically populated by the scripts input arguments.

```
        self.updateType = updateType #full or incremental, indicates if threatfeed
    does a full replace or append
        self.appserverUsername = appUser #Optional if run external to FortiSIEM
        self.appserverPassword = appPW #Optional if run external to FortiSIEM
        self.threatfeed_natural_id = naturalId #Threatfeed natural ID to update
        self.threatfeed_type = tfType #Threatfeed type (ip,site,url,hash,proc)
        self.threatfeed_url = tfURL #Threatfeed source URL
        self.threatfeed_username = tfUser #Threatfeed optional user
        self.threatfeed_password = tfPW #Threatfeed optional pw
        self.appserver_host = appHost #FortiSIEM super IP if script run externally
```

Important Member Functions of the ThreatfeedIntegration Class

Member Function	Description
getThreatFeedData (self)	You must override this function in your script's child class. It references the above member variables to authenticate to your given threat feed source, and calls the save function to send to FortiSIEM.
saveThreatFeedData (self,post_data)	Call this function once you have retrieved your threat feed data. It accepts a python list of dictionary objects, which represent either IP, URL, Domain, or Hash objects. You only call this function, you do not override it.

Instructions on Creating a New Python Integration

Take the following steps to create a new python integration.

1. Copy an existing example file.
   For example:

```
cp firehol_threatfeed.py my_example.py
```

2. Rename the class “FireHolThreatFeed” to your new class name. It is referenced in 3 locations in this file.
3. Override the `getThreatFeedData` function, as this is where all your work will be done. You will build a list of dictionary objects using the existing integrations as an example.
4. Call `saveThreatFeedData(post_data)`. This will convert the list of dictionary objects into a CSV file (if run locally on Supervisor) or call AppServer save API if run externally to Supervisor.
   You can review the file `example_threatfeed.py` to see an example of how to convert data ingested from a threat feed into a representation that the framework can convert to a CSV file.

Python Script

The python script which is user defined e.g. “threatfeed_script_name.py” is called with the input arguments listed in the following table.

Argument Number	Argument	Argument Type	Description
Arg1	updateType	String	Either "full" or "incremental". If script is externally run, calls to the save API can override whether the threat feed does a full replace of data ("full") or an append ("incremental").
Arg2	naturalId	String	String literal of the threat feed (to update)s’ natural ID.
Arg3	tfType	String	Threat feed type, which will be one of the following: ip, hash, site, or url. This allows a single script to add handling for the type of threat feed if the service provides multiple types of threat feeds.
Arg4	tfURL	String	URL endpoint for the threat feed service.
Arg5	tfUser	String	(Optional) Username value for basic authentication to threat feed service.
Arg6	tfPW	String	(Optional)Password value for threat feed basic authentication. In other cases, it can be used for holding the API secret key instead. The script can manipulate these values as desired.
Arg7	appUser	String	(Optional) Username for FortiSIEM in the format (org/user) e.g. super/admin. This is only needed if the script is executed externally from FortiSIEM and not executed via AppServer schedule.
Arg8	appPW	String	(Optional) Password for FortiSIEM user. This is only needed if the script is executed externally from FortiSIEM and not executed via AppServer schedule.
Arg9	appHost	String	(Optional) If script is run externally to FortiSIEM, this can override the app server (Supervisor) URL. It normally defaults to https://127.0.0.1 as it is only executed programmatically on the FortiSIEM Supervisor.

Example Adhoc Script Run Locally on FortiSIEM

Caution: Script must only be run as user "admin", **never** as root.

```
python3 /opt/phoenix/data-definition/threatfeedIntegrations/firehol_threatfeed.py -
updateType full -naturalId Malware_IPs_FireHol_Cybercrime_Threatfeed_0 -tfType ip -
tfURL https://iplists.firehol.org/files/firehol_level1.netset -tfUser guest -tfPW
guest
```

This generates a CSV file for AppServer to consume: `/opt/phoenix/cache/MalwareIP/Malware_IPs_FireHol_Cybercrime_Threatfeed_0.csv`

Note: When you manually run the script, you'll notice that it doesn't actually update in the GUI. This is because normally, FortiSIEM is the one executing the script, and will only look for this CSV file after it executes. You can manually run this to test for errors and ensure the CSV file is populated appropriately. Afterward, you can try an end to end test by configuring FortiSIEM to call your new threat feed script.

Example Adhoc Script Run Externally to FortiSIEM (e.g. remote customer machine) – This assumes you have a FortiSIEM user account and know the threat feed's natural ID.

```
python3 /opt/phoenix/data-definition/threatfeedIntegrations/firehol_threatfeed.py -
updateType full -naturalId Malware_IPs_FireHol_Cybercrime_Threatfeed_0 -tfType ip -
tfURL https://iplists.firehol.org/files/firehol_level1.netset -tfUser guest -tfPW
guest -appUser 'super/admin' -appPW 'xxxxx' –appHost 'https://192.168.1.25'
```

The only difference here is the addition of appUser, appPW, and appHost, indicating to the script that it must call the app server API which is on a remote system using HTTP POST with basic authentication. If run locally, the script will merely generate a CSV file in the `/opt/phoenix/cache` directory for AppServer to consume (removing the need for app server credentials).

Save Imported Data to Database

Normally the details of the CSV file location, and its format are completely abstracted and handled by the parent class "ThreatfeedIntegration". The content here is for informational purposes only.

- Python script has to save data in following directories depending on threat feed type.
  - /opt/phoenix/cache/MalwareDomain
  - /opt/phoenix/cache/MalwareIP
  - /opt/phoenix/cache/MalwareHash
  - /opt/phoenix/cache/MalwareUrl
- Supported file type is CSV
- File Name: <natural_id>.csv e.g. Malware_IPs_FireHol_Cybercrime_Threatfeed_0.csv
- CSV structure:
  - IPs: name, malwareType, lowIp, highIp, description, confidence ,severity, org, country, asn, dateFound, lastSeen
  - Domains: domainName, malwareType, description, ipAddr, reverseLookup, asn, confidence, severity, org, country, dateFound, lastSeen
  - Hash: botnetName, algorithm, hash, controllerIp, confidence, country, malwareType, severity, asn, org, description, dateFound, lastSeen
  - URL: url, description, malwareType, confidence, lastSeen

Performance Considerations

There are no performance concerns a this time. When selecting the threat feed update type in the GUI, in almost all cases you want to select “Full”. FortiSIEM has been enhanced to handle massive threat feed lists. Only in exceedingly rare cases would you choose update type of “Incremental”. Doing "Incremental" can create problems as threat lists quickly become exceedingly large (not truncated), and often contain stale, and non-effective indicators.

Custom python scripts can be either configured to do either of the following:

- **Incremental** (append only) - Updates to the threat feed, new calls are append only, and does not delete and re-enter the same data. Care should be taken to periodically do a full replace on a maintenance schedule to replace stale entries.
- **Full** - Updates to the threat feed, each call to the script does a complete replace of the threat feed data with the latest copy from the source threat feed source. **This should be considered the default option even in really large threat feeds in the hundreds of thousands of entries**.

Public APIs

These public APIs are only important if you plan to execute this script outside of FortiSIEM as part of your own custom application. Normally FortiSIEM will hold all these scripts locally and execute them on a schedule, removing the need for these public APIs.

AppServer provides the following two public REST APIs to import or delete malware data. These are only needed if the python script is executed external to FortiSIEM. This allows external systems to integrate with FortiSIEM threat feeds, as opposed to having FortiSIEM execute an update on a schedule.

- Import API
- Delete API

Import API

API Endpoint: `POST phoenix/rest/malware/{type}/save`

Query Parameters

1. groupNaturalId : String [*required field]
2. updateType : String [full | incremental]

Path Parameters

1. type: String [*required field]
   a. Accepted values for type - [hash, site, url, ip]

POST Body

Example for IP:

```
[
{
    "name":"RansomwareIP",
    "lowIp":"1.1.1.1",
                "highIp":"1.1.1.1"
            },
            {
                "name":"RansomwareIP2",
                "lowIp":"2.1.1.1",
                "highIp":"2.1.1.1"
            },
            {
                "name":"RansomwareIP3",
                "lowIp":"3.1.1.1",
                "highIp":"3.1.1.1"
            }
        ]
```

Example 2 for Domain:

```
    [
    {
    "domainName":"",
    "ip":"",
    "name":""
    } //This JSON Object keys are defined in ThreatFeedDTO
    ]
```

JSON Structure: Array of Objects: ThreatFeedDTO

See the following tables for their **ThreatFeedDTO JSON Object Structure**.

Malware Domain Threat Feed Parameter	Value Type
domainName	String
ip	String
reverseLookup	String

Malware IP Threat Feed Parameter	Value Type
name	String
lowIp	String

Malware IP Threat Feed Parameter	Value Type
highIp	String

Malwre Hash Threat Feed Parameter	Value Type
botnetName	String
algorithm	String
hash	String
controllerIp	String

Malware Url Threat Feed Parameter	Value Type
url	String
origin	String

Common Malware Threat Feed Parameter	Value Type
active	Boolean
malwareType	String
confidence	String
severity	String
asn	String
org	String
country	String
description	String
dateFound	String
lastSeen	String

Delete API

API Endpoint: `POST phoenix/rest/malware/threatfeed/deleteall`

Query Parameter

1. groupNaturalId : String [*required field]

Return: Success | Error

Notes about Threat Feed Authentication

The python threat feed GUI still only has the ability to pass basic authentication credentials to the Python script (e.g. username and password). You can place values such as an API key in one of these fields and manipulate that data in your custom threat feed integration. So although the UI only displays an optional user/pw fields, you can still put anything you want in these fields and manipulate accordingly. Note that only the password field is encrypted, so try not to place sensitive data in the username field if overriding them for a different authentication type.

Installing New Python Packages

Using new packages not already installed on the Supervisor need to be manually installed with care. Fortinet uses the requests API which covers the most common use cases. The system python3 install already contains many useful packages such as requests and urllib3.

Here are recommended steps to help keep your system secure.

1. Follow your organization’s change control procedures
2. Backup your FortiSIEM Supervisor prior to making the change
3. Ensure you have a rollback/revert plan
4. Document the time of the change and the purpose
5. Make the change only on the Supervisor appliances

UEBA Information

The following UEBA content is available.

Comparing UEBA Sources

- Windows UEBA vs Log Based UEBA
- UEBA Rules Trigger Based on Log Source

Windows UEBA vs Log Based UEBA

The following table provides details on Windows UEBA Agent versus log based UEBA.

Scenario	Windows UEBA Agent	Windows Security Log	Windows Sysmon	Linux Agent	Linux Log
File create	Yes	No	Yes	No	No
File delete	Yes	Yes	Yes	No	No

Scenario	Windows UEBA Agent	Windows Security Log	Windows Sysmon	Linux Agent	Linux Log
File read	Yes	No	No	No	No
File write	Yes	No	No	No	No
File move	Yes	No	No	No	No
File rename	Yes	No	No	No	No
File print	Yes	No	No	No	No
Process stop	Yes	Yes	Yes	No	No
Process create	Yes	Yes	Yes	Yes	No
File upload	Yes	No	No	No	No
File download	Yes	No	No	No	No
Machine on	Yes	Yes	No	No	No
Machine off	Yes	Yes	No	No	No
Drive mount	Yes	No	No	No	No
Drive unmount	Yes	No	No	No	No
Host logon	Yes	Yes	No	No	Yes
Host logoff	Yes	Yes	No	No	Yes

UEBA Rules Trigger Based on Log Source

Rule Name	Windows UEBA Agent	Win Log (Win Security AND/OR Sysmon)	Linux Agent	Linux Log
UEBA AI detects unusual drive unmounted	Yes	No	No	No

Rule Name	Windows UEBA Agent	Win Log (Win Security AND/OR Sysmon)	Linux Agent	Linux Log
UEBA AI detects unusual file creation	Yes	Yes (Sysmon)	No	No
UEBA AI detects unusual file deletion	Yes	Yes (Win Security OR Sysmon)	No	No
UEBA AI detects unusual file download	Yes	No	No	No
UEBA AI detects unusual file movement	Yes	No	No	No
UEBA AI detects unusual file printed	Yes	No	No	No
UEBA AI detects unusual file reading	Yes	No	No	No
UEBA AI detects unusual file renamed	Yes	No	No	No
UEBA AI detects unusual file upload	Yes	No	No	No
UEBA AI detects unusual file writing	Yes	No	No	No
UEBA AI detects unusual host logon	Yes	Yes (Win Security)	No	Yes
UEBA AI detects unusual machine off	Yes	Yes (Win Security)	No	No
UEBA AI detects unusual machine on	Yes	Yes (Win Security)	No	No
UEBA AI detects unusual new drive mounted	Yes	No	No	No
UEBA AI detects unusual process created	Yes	Yes (Win Security OR Sysmon)	Yes	No
UEBA AI detects unusual process not restarted	Yes	No	No	No
UEBA AI detects unusual process started	Yes	Yes (Win Security OR Sysmon)	No	No
UEBA AI detects unusual process stopped	Yes	Yes (Win Security OR Sysmon)	No	No
UEBA AI detects unusual user logoff	Yes	Yes (Win Security)	No	Yes
UEBA Policy detects antivirus not started	Yes	No	No	No
UEBA Policy detects antivirus stopped	Yes	No	No	No
UEBA Policy detects backup applications	Yes	No	No	No
UEBA Policy detects browser download	Yes	No	No	No
UEBA Policy detects browser upload	Yes	No	No	No

Rule Name	Windows UEBA Agent	Win Log (Win Security AND/OR Sysmon)	Linux Agent	Linux Log
UEBA Policy detects cloud upload	Yes	No	No	No
UEBA Policy detects email download	Yes	No	No	No
UEBA Policy detects email upload	Yes	No	No	No
UEBA Policy detects encryption tools	Yes	No	No	No
UEBA Policy detects file archiver application	Yes	No	No	No
UEBA Policy detects file printed	Yes	No	No	No
UEBA Policy detects files copied over remote desktop	Yes	No	No	No
UEBA Policy detects gaming application	Yes	No	No	No
UEBA Policy detects hacking tool and footprints	Yes	No	No	No
UEBA Policy detects hacking tool usage	Yes	No	No	No
UEBA Policy detects malicious powershell execution	Yes	No	No	No
UEBA Policy detects MTP read	Yes	No	No	No
UEBA Policy detects MTP write	Yes	No	No	No
UEBA Policy detects NFS read	Yes	No	No	No
UEBA Policy detects nfs write	Yes	No	No	No
UEBA Policy detects potential leaver editing a CV at work	Yes	No	No	No
UEBA Policy detects potential pirated media	Yes	No	No	No
UEBA Policy detects ransomware	Yes	No	No	No
UEBA Policy detects ransomware file names	Yes	No	No	No
UEBA Policy detects ransomware file types	Yes	No	No	No
UEBA Policy detects removable media read	Yes	No	No	No
UEBA Policy detects removable media write	Yes	No	No	No

Rule Name	Windows UEBA Agent	Win Log (Win Security AND/OR Sysmon)	Linux Agent	Linux Log
UEBA Policy detects snipping tool	Yes	No	No	No
UEBA Policy detects software installation	Yes	No	No	No
UEBA Policy detects suspicious applications	Yes	No	No	No
UEBA Policy detects Tor client usage	Yes	No	No	No
UEBA Policy detects uncommon VPN client	Yes	No	No	No

UEBA Based on Log

In earlier releases, User Entity Behavior Analytics (UEBA) was done based on proprietary logs collected by the FortiSIEM Windows UEBA Agent. Now, the analytics is extended to the following regular logs. Note that regular logs only cover a subset of the user activities compared to the FortiSIEM UEBA Agent.

Windows Security logs

- Unusual machine on activity based on Win-Security-4608 log
- Unusual machine off activity based on Win-Security-4609 log
- Unusual host logon activity based on Win-Security-4624 log
- Unusual host logoff activity based on Win-Security-4634 log
- Unusual file deletion based on Win-Security-4660 log
- Unusual process created based on Win-Security-4688 log
- Unusual process stopped based on Win-Security-4689 log

Windows Sysmon

- Unusual process created based on Win-Sysmon-1-Create-Process log
- Unusual process stopped based on Win-Sysmon-5-Process-Terminated log
- Unusual file creation based on Win-Sysmon-11-FileCreate log
- Unusual file deletion based on Win-Sysmon-23-File-Delete-archived and Win-Sysmon-26-File-Delete-logged log

Linux Agent

- Unusual process created based on LINUX_PROCESS_EXEC log
- Unusual machine off activity based on Generic_Unix_System_Shutdown log
- Unusual host logon activity based on Generic_Unix_Successful_SSH_Login log

For detailed comparison of Windows UEBA Agent versus log based UEBA, see Appendix - Comparing UEBA Sources.

UEBA Sample Logs

UEBA Events File Interaction sample logs are provided here.

FINS-Windows-new-drive-mounted

```
2022-06-24T19:06:58Z CD-DESK-S 0.0.0.0 [phCustId]="1" [customer]="super" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="38ba7825-34a2-41b8-8e3d-0548878bef5b" [timeZone]="-0500" FortiInsight-Windows-Agent msg = {"ac":"new drive mounted","ap":"ntoskrnl.exe","d":"2022-06-24T15:06:57.128-04:00","r":"\\\\?\\swd#wpdbusenum#_??_usbstor#disk&ven_samsung&prod_flash_drive_fit&rev_1100#0374216040008546&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}#{6ac27878-a6fa-4155-ba85-f98f491d4f33} -> samsung usb","u":"__"}
```

FINS-Windows-file-written

```
2022-06-24T19:25:06Z CD-DESK-S 192.168.1.147  [phCustId]="1" [customer]="super" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="38ba7825-34a2-41b8-8e3d-0548878bef5b" [timeZone]="-0500"  FortiInsight-Windows-Agent msg = {"ac":"file written","ap":"explorer.exe","d":"2022-06-24T15:25:00.992-04:00","r":"rm:\\d:\\agenttest\\wireshark-win64-3.6.6.exe","u":"cd-desk-s__durki"}
```

FINS-Windows-file-created

```
2022-06-24T19:25:00Z CD-DESK-S 192.168.1.147  [phCustId]="1" [customer]="super" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="38ba7825-34a2-41b8-8e3d-0548878bef5b" [timeZone]="-0500"  FortiInsight-Windows-Agent msg = {"ac":"file created","ap":"explorer.exe","d":"2022-06-24T15:25:00.215-04:00","r":"rm:\\d:\\agenttest\\wireshark-win64-3.6.6.exe","u":"cd-desk-s__durki"}
```

FINS-Windows-file-deleted

```
2022-06-24T19:23:57Z CD-DESK-S 192.168.1.147  [phCustId]="1" [customer]="super" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="38ba7825-34a2-41b8-8e3d-0548878bef5b" [timeZone]="-0500"  FortiInsight-Windows-Agent msg = {"ac":"file deleted","ap":"explorer.exe","d":"2022-06-24T15:23:56.794-04:00","r":"rm:\\d:\\agenttest\\winscp-5.17.8-setup.zip","u":"cd-desk-s__durki"}
```

FORTINET®

www.fortinet.com