RSA Archer GRC

RSA Archer Security Operations Management 1.3 SP1

Installation and Configuration Guide

5.5 SP3 P2 and Later

Revision 2

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers: **http://www.emc.com/support/rsa/index.htm**.

Trademarks

RSA, the RSA Logo, RSA Archer, RSA Archer Logo, and EMC are either registered trademarks or trademarks of EMC Corporation ("EMC") in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to **www.rsa.com/legal/trademarks_list.pdf**.

License agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-party licenses

This product may include software developed by parties other than RSA.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright © 2010-2016 EMC Corporation All Rights Reserved. Published in the USA.
August 2016

Contents

Revision History **6**

Preface **7**
About This Guide 7
RSA Archer GRC Documentation 7
RSA Security Analytics Documentation 7
RSA Archer Security Operations Management Data Dictionary 8
Support and Service 8
Other Resources 8

Chapter 1: RSA Archer Security Operations Management **9**
RSA Archer Security Operations Management 9
RSA Archer Security Operations Management Components 9
RSA Archer Security Operations Management Architecture 10
Integration with RSA Security Analytics 11
RSA Unified Collector Framework Ports 14
RSA Archer Security Operations Management Files 16
RSA Archer Security Operations Management Requirements 17
RSA Archer GRC Requirements 17
RSA Security Analytics or Other SIEM Tools Requirements 19
RSA Unified Collector Framework (UCF) Requirements 19
Prepare to Install or Upgrade and Configure RSA Archer Security Operations Management 1.3 SP1 20

Chapter 2: Installing the RSA Archer Security Operations Management Solution **22**
Download the Solution File from the RSA Archer Community on RSA Link 22
Back Up the Database 22
Import the Install Package 23
Update the License Key 23
Performing Advanced Package Mapping 23
Install the Solution Package 24
Review the Package Installation Log 26
Create the Security Operations Management Group 26
Create a New Crisis Event Status 27
Configure Bing Maps 27
Create a User Account for the RSA Archer Web Service Client 28
RSA Archer Security Operations Management Data Feeds 28
Import a Data Feed 29
Schedule a Data Feed 30
Importing ACD Content 31
Prepare to Import ACD Data 31
Import ACD Data into Incident Response Procedure Library 32
Perform ACD Data Post Import Activities 33
Post-Install Activities 33
Deleting Obsolete Objects 33

Validating Formulas and Calculation Orders 34
Verifying Key Fields 34
Updating Record Permissions Fields to Allow Access to Other Solution Records 35
Verifying the Upgrade from RSA Advanced Incident Management for Security 1.1 35
Test the Solution 36

Chapter 3: Installing the RSA Unified Collector Framework 37

RSA Unified Collector Framework Integrations 37
RSA Security Analytics Incident Management Integration Options 37
Create RSA Archer User Accounts for Push and Pull 38
Set Up the RSA Unified Collector Framework 40
Install the RSA Unified Collector Framework 40
Configure Endpoints 41
(Optional) Set the Maximum Number of Alerts or Events Sent Through the RSA Unified Collector Framework 46

Chapter 4: Upgrading the RSA Unified Collector Framework 47

Upgrading the UCF from RSA Archer Security Operations Management 1.3 47
Upgrade the UCF from RSA Archer Security Operations Management 1.3 47
Upgrading the UCF from RSA Archer Security Operations Management 1.2 48
Upgrade the UCF from RSA Archer Security Operations Management 1.2 48
Upgrade the UCF from RSA Archer Security Operations Management 1.1 or 1.1 SP1 50
Upgrade the UCF from RSA Archer Security Operations Management 1.1 or 1.1 SP1 50
Migrate the RSA Connector Framework 51
Uninstall the RSA Connector Framework (RCF) 52

Appendix A: Configuring Integrations 53

Configure RSA Security Analytics for the Enterprise Management Plug-In 53
Configure RSA Security Analytics Live Feed 53
Update the Concentrator and Decoder Services 55
Create a Recurring Feed Task 56
Configure RSA Security Analytics Incident Management 57
Select the Mode for SA IM 57
Update the Normalization Scripts for RSA Security Analytics Incident Management 58
Forward Security Analytics Alerts to the SA IM Service 59
Forward RSA Enterprise Compromise Assessment Tool (ECAT) Alerts to the SA IM Service 60
Aggregate Alerts into Incidents 60
Configure Splunk 61
Configure IBM QRadar 61
Configure IBM QRadar for Secure TCP Connection 62
IBM QRadar Test Example 63
Configure McAfee Enterprise Security Manager (ESM) 63
McAfee Enterprise Security Manager (ESM) Test Example 64
Configure Syslog Output Action for the Reporting Engine for Security Analytics 65

Configure SA RE SSL for Secure Syslog Server 65
Configure Rules in Security Analytics 66
Add Alert Templates for the Reporting Engine in Security Analytics 66
Configure Alerts in Security Analytics 67
Configure ESA Syslog Notification Settings in Security Analytics 67
Configure SA ESA SSL for Secure Syslog Server 68
Add ESA Alert Templates in Security Analytics 69
Create ESA Rules in Security Analytics 69
Configure a Generic SIEM Tool 70
Generic and SIEM Specific Mappings 72
Mandatory Fields in Generic SIEM 72
Add New Field in SIEM Tool 73
Add Source Field in Alert Source 73
Update the RSA Security Analytics Host File for SSL Mode 74
Manually Copy Enterprise Management Certificates 75

Appendix B: Customizing and Modifying the Integration with RSA Security Analytics for Business Context 76
Include Optional RSA Archer Fields 76
Create a New Context Menu Action 77
Change Feed Settings 78

Appendix C: RSA Unified Collector Framework Administration Tasks 80
Start the RSA Unified Collector Framework 80
Stop the RSA Unified Collector Framework 80
Uninstall the RSA Unified Collector Framework 80
Configure the Syslog Endpoint After Upgrade 81
Manually Copy SA IM Certificates 81
Regenerate Certificates 82
Regenerate Expired SA IM Certificates 83

Appendix D: RSA SecOps Watchdog Service 84
RSA SecOps Watchdog Service Conditions 84
RSA SecOps Watchdog Service Counters 86
Watchdog Configured Cron Time 88
Watchdog Hours Configured For Total Counter 88
Add the Watchdog Service to the Performance Monitor 88
Start the RSA SecOps Watchdog Service 89
Stop the RSA SecOps Watchdog Service 89

Appendix E: Troubleshooting 90
Component Troubleshooting 90
Security Analytics Incident Management Integration Troubleshooting 99
Enterprise Management Plug-In Setup Troubleshooting 104
Package Installation Log Message Examples 108

Revision History

Revision	Date	Description
1	7/28/2016	Updated the required version of RSA Security Analytics to 10.5.x and later. Removed topics related to RSA Security Analytics 10.4.
2	8/2/2016	Updated the required versions of RSA Security Analytics. RSA Security Analytics 10.6 is not supported.

Preface

About This Guide

This guide is for RSA® Archer® GRC administrators who need to install the RSA Archer Security Operations Management 1.3 SP1 solution. For more information, see the RSA Archer GRC Platform Help.

This guide assumes that the reader is knowledgeable about the GRC industry and RSA Archer GRC.

RSA Archer GRC Documentation

You can access the RSA Archer GRC documentation from the RSA Archer GRC Community on RSA Link.

Documentation	Location
Platform, Solutions, Applications, and Content	On the RSA Archer GRC Community on RSA Link at: **https://community.rsa.com/docs/DOC-41227**

RSA continues to assess and improve the documentation. Check the RSA Archer GRC Community on RSA Link for the latest documentation.

RSA Security Analytics Documentation

For information about RSA Security Analytics, see the following documentation:

Guide	Description
RSA Security Analytics Help	The RSA Security Analytics Help provides information needed to understand and use RSA Security Analytics features. It contains topics and tutorials to help you learn the basics of the user interface, system configuration, and analysis concepts. In addition, troubleshooting information for common situations is added on a continuous basis.

You can access this reference material from the RSA Security Analytics Unified Dashboard.

RSA Archer Security Operations Management *Data Dictionary*

The RSA Archer Security Operations Management *Data Dictionary* contains configuration information for the solution.

You can obtain the *Data Dictionary* for the solution by contacting your RSA Archer GRC Account Representative or calling 1-888-539-EGRC.

Support and Service

Customer Support Information	**https://community.rsa.com/community/rsa-customer-support**
Customer Support E-mail	**archersupport@rsa.com**

Other Resources

RSA Archer GRC Community on RSA Link: Our public forum, on the new RSA Link Community platform, brings together customers, prospects, consultants, RSA Archer GRC thought leaders, partners and analysts to talk about GRC as a practice, and includes product demos, GRC videos, white papers, blogs and more. **https://community.rsa.com/community/products/archer-grc**

RSA Archer Community on RSA Link: Our private community, is a powerful governance, risk and compliance online network that promotes collaboration among Archer customers, partners, industry analysts, and product experts. Engaging with the RSA Archer Community on RSA Link enables you to collaborate to solve problems, build best practices, establish peer connections and engage with RSA Archer GRC Thought Leaders. **https://community.rsa.com/community/products/archer-grc/archer-customer-partner-community**

RSA Ready: RSA's Technology Partner Program is where 3rd parties gain access to RSA Software in order to develop an interoperability and have it documented and certified. RSA Ready certifications are posted to an online Community and supported by RSA Support. **https://community.rsa.com/community/products/rsa-ready**

Chapter 1: RSA Archer Security Operations Management

RSA Archer Security Operations Management 9
RSA Archer Security Operations Management Architecture 10
RSA Unified Collector Framework Ports 14
RSA Archer Security Operations Management Files 16
RSA Archer Security Operations Management Requirements 17
Prepare to Install or Upgrade and Configure RSA Archer Security Operations Management 1.3 SP1 20

RSA Archer Security Operations Management

The RSA Archer Security Operations Management solution enables you to aggregate all actionable security alerts, allowing you to become more effective, proactive, and targeted in your incident response and SOC management.

RSA Archer Security Operations Management helps you do the following:

- Prioritize and respond faster to security incidents by leveraging business context and actionable threat intelligence.
- Engage key business and IT stakeholders in the incident management process.
- Simplify incident investigation and breach response procedures through industry best practice methodologies and response procedures.
- Optimize SOC investments through SOC Key Performance Indicators (KPI) monitoring and staff time management tracking.

RSA Archer Security Operations Management Components

RSA Archer Security Operations Management is composed of the following:

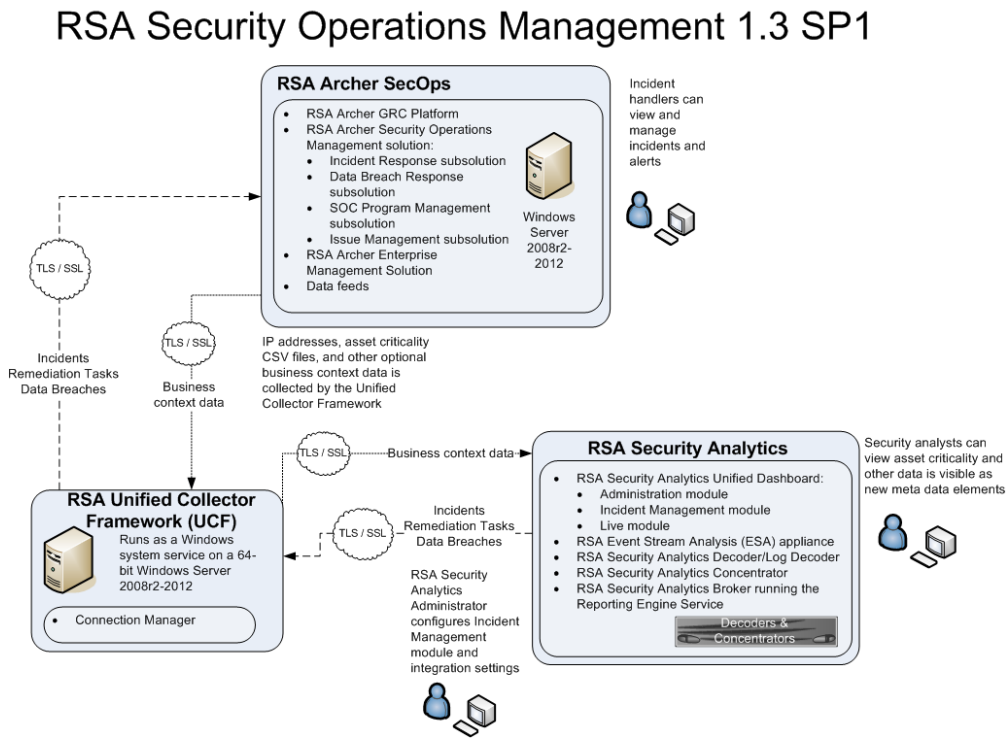
- RSA Archer Security Operations Management solution:
  - Incident Response subsolution
  - Data Breach Response subsolution
  - SOC Program Management subsolution
  - Issue Management subsolution

- Integrations with a Security Information and Event Management (SIEM) tool:
  - RSA Security Analytics. For more information, see **Integrations with RSA Security Analytics**.
  - Other supported third-party SIEM tools. For more information, see the **RSA Archer Community on RSA Link**.
- RSA Unified Collector Framework (UCF):
  - Security Analytics Incident Management (SA IM) Integration Service
  - Enterprise Management Plug-in
  - Syslog Server
  - RSA SecOps Watchdog Service

Important: The RSA Archer Enterprise Management solution is required for RSA Archer Security Operations Management to be fully functional.

RSA Archer Security Operations Management Architecture

The following figure shows the architecture of the integrations between RSA Archer Security Operations Management and RSA Security Analytics and the flow of data.



Note: RSA Archer Security Operations Management can also integrate with other SIEM tools to feed alerts into the solution. For information on supported third-party integrations, see the **RSA Archer Community on RSA Link**.

Integration with RSA Security Analytics

RSA Archer Security Operations Management integrates with RSA Security Analytics using the RSA Unified Collector Framework.

RSA Unified Collector Framework

The RSA Unified Collector Framework (UCF) integrates with all supported SIEM tools and the RSA Archer Security Operations Management solution. When integrating with the RSA Security Analytics Incident Management module, you can choose one of the following integration options:

- Manage the full incident workflow in RSA Archer Security Operations Management. If you select this option, the Unified Collector Framework transports incidents from the Security Analytics Incident Management module into the solution.
- Manage the incident workflow in the Security Analytics Incident Management module and allow analysts the option to escalate remediation tasks and open data breaches for management and remediation in the RSA Archer Security Operations Management solution. If you select this option, the Unified Collector Framework transports remediation tasks (created as Findings), data breaches, or both.

  Important: You must configure the same option in both RSA Security Analytics and the Unified Collector Framework.

Supported and Generic SIEM

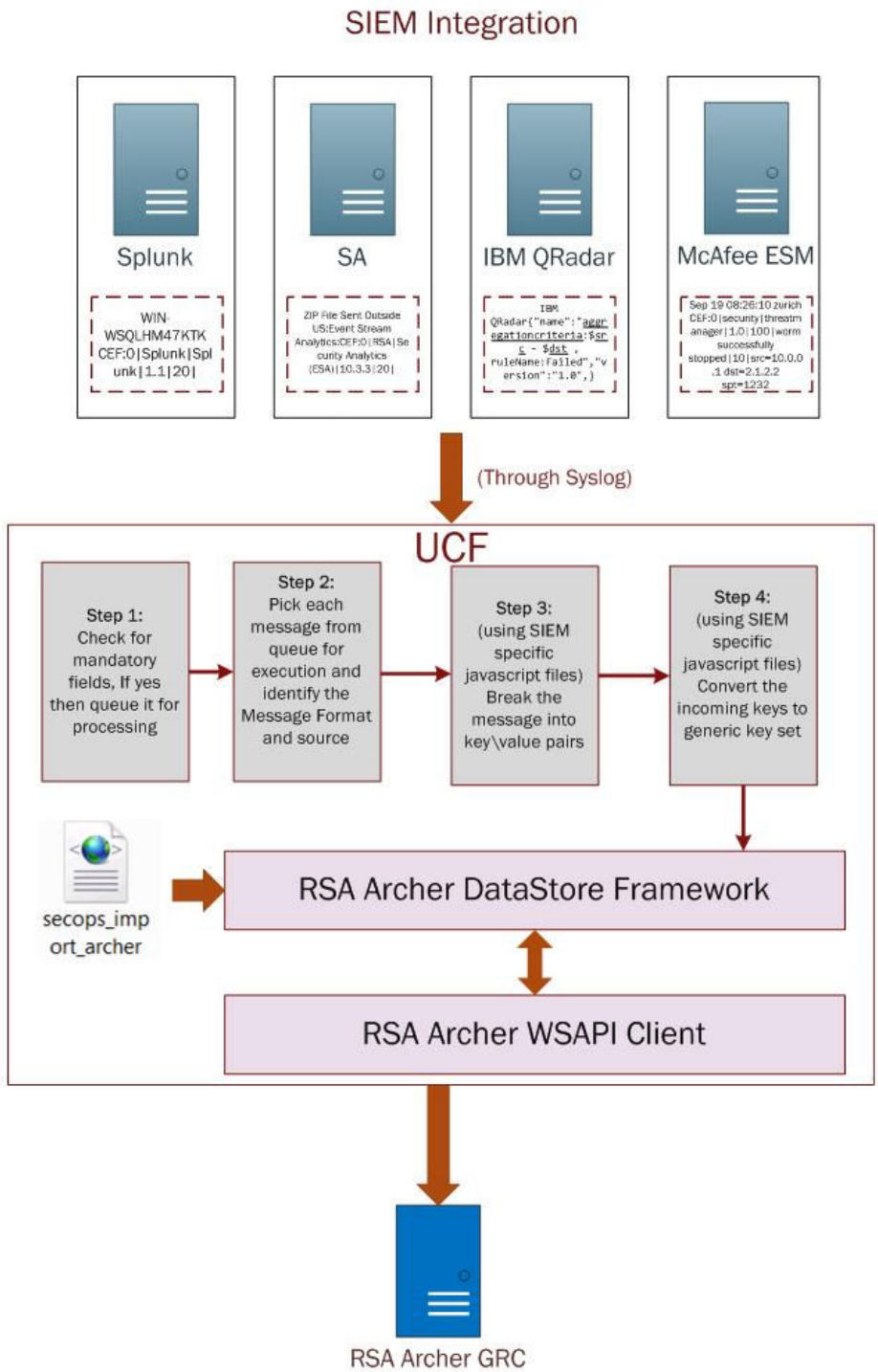
The UCF uses a generic SIEM implementation to integrate with various SIEM tools and provide event forwarding through Syslog. Out of the box, RSA Archer Security Operations Management 1.3 SP1 supports integration with the following tools:

- RSA Security Analytics Reporting Engine (SA RE)
- RSA Security Analytics Event Stream Analysis (SA ESA)
- Splunk
- McAfee Enterprise Security Manager (ESM)
- IBM QRadar

SIEM tools that are not supported out of the box can also be configured to work with RSA Archer Security Operations Management.

Note: If you integrate with the RSA Security Analytics Incident Management module, integrating with SA RE and SA ESA can result in duplicate events and incidents created in RSA Archer GRC.

The UCF supports multiple SIEM tools at the same time, such as supporting SA RE, Slunk, and SA IM. Different instances of the same SIEM tool are not supported, such as running two SA servers connected to the same UCF.


SIEM Integration
Splunk
WIN-WSQLHM47KTK CEF:0|Splunk|Splunk|1.1|20|
SA
ZIP File Sent Outside US:Event Stream Analytics:CEF:0|RSA|Security Analytics|CSA|10.3.3|20|
IBM QRadar
IBM QRadar{"name":"aggregationcriteria:$src - $dst , ruleName:Failed","version":"1.0",}
McAfee ESM
Sep 19 08:26:10 zurich CEF:0|security|threatmanager|1.0|100|worm successfully stopped|10|src=10.0.0.1 dst=2.1.2.2 spt=1232
(Through Syslog)
UCF
Step 1: Check for mandatory fields, If yes then queue it for processing
Step 2: Pick each message from queue for execution and identify the Message Format and source
Step 3: (using SIEM specific javascript files) Break the message into key\value pairs
Step 4: (using SIEM specific javascript files) Convert the incoming keys to generic key set
secops_import_archer
RSA Archer DataStore Framework
RSA Archer WSAPI Client
RSA Archer GRC

Enterprise Management Plug-In for Business Context

The Enterprise Management plug-in provides context around the assets that are most critical to your organization by automatically feeding critical asset information from your RSA Archer Enterprise Management solution through the RSA Unified Collector Framework into RSA Security Analytics as metadata. In Security Analytics, security analysts can prioritize an investigation based on the assets most critical to the organization, using asset criticality and other metadata fed from your RSA Archer GRC system. Security analysts can also use the metadata to create rules and alerts to identify network and log events happening on critical assets.

Important: You must populate the RSA Archer Devices application with the IP addresses, criticality rating information, and the business unit and facilities cross-references that you want to transfer to your RSA Security Analytics system. RSA recommends contacting Professional Services if you need assistance populating your data.

RSA SecOps Watchdog Service

The RSA SecOps Watchdog Service tracks and reports the number of messages read from RabbitMQ or Syslog servers, and the number of messages that have been created or updated in RSA Archer GRC.

The RSA SecOps Watchdog Service is responsible for reading all of the counters from the Windows Performance Counters at every Configured Cron Time, logging the appropriate messages, and performing any actions deemed necessary.

RSA Unified Collector Framework Ports

Note: The recommended protocol is TCP or Secure TCP for all connections except McAfee ESM, which only supports Syslog forwarding through UDP.

RSA recommends creating firewall rules on the UCF machine to only accept incoming connections from known remote and SIEM tool source IP addresses. For example, to integrate with IBM QRadar using TCP, create a firewall rule on the UCF machine to allow incoming TCP connections on port 1514 and limiting the source IP address range to only include the IP address of the IBM QRadar machine forwarding the messages.

Component	Default Port Number	Traffic Direction	UCF Firewall Rule Required	Details
UCF JMX / Connection Manager	9000	Local Machine Only	No	Default JMX port; used when runConnectionmanager.bat is executed.
UCF JMX Dynamic Port Range	40000-64000	Local Machine Only	No	Java JMX enables dynamic ports to be used. The ports change each time service is restarted.
RSA Archer Web Services API HTTPS	443	To RSA Archer Web Server	No	Port used by the UCF for communication with RSA Archer Web Server.
RSA Archer Enterprise Management Plug-in	9090	Incoming	Yes	Required if using the Enterprise Management plug-in.
IBM QRadar - Syslog	1514	Incoming	Yes	Recommended for Syslog when configuring the QRadar endpoint in the UCF and forwarding configuration on the QRadar SIEM.
IBM QRadar - Secure Syslog	1515	Incoming	Yes	Recommended for Secure Syslog when configuring the QRadar endpoint in the UCF, and forwarding configuration on the QRadar SIEM.
McAfee ESM - Syslog	514	Incoming	Yes	Only supported method for connection from McAfee - Syslog is with UDP.
Splunk - Syslog	1514	Incoming	Yes	Recommended for configuring the RSA Security Operations Management Splunk plug-in on the Splunk machine, and when setting up the Splunk endpoint in the UCF.

Component	Default Port Number	Traffic Direction	UCF Firewall Rule Required	Details
Splunk - Secure Syslog	1515	Incoming	Yes	Recommended for configuring the RSA Security Operations Management Splunk plug-in on the Splunk machine, and when setting up the Splunk endpoint in the UCF for Secure Syslog.
SA IM with RabbitMQ	5671	To RSA Security Analytics	No	Default port used for configuring the SA IM endpoint in the UCF. **Note:** If the connection does not work, contact the RSA Security Analytics administrator for the correct RabbitMQ port.
SA RE/ESA - Syslog	1514	Incoming	Yes	Recommended for Syslog when configuring the SA RE/ESA endpoints in the UCF and when configuring forwarding on SA RE/ESA.
SA RE/ESA - Secure Syslog	1515	Incoming	Yes	Recommended for Secure Syslog when configuring the SA RE/ESA endpoints in the UCF and when configuring forwarding on SA RE/ESA.

RSA Archer Security Operations Management Files

RSA Archer Security Operations Management comprises the following .zip files:

- RSA_Archer_Security_Operations_Management_1.3.1.zip
  - RSA_Archer_Security_Operations_Management_1.3.1_Install_Package.zip
  - RSA_Archer_Security_Operations_Management_1.3.1_Data_Feeds.zip
    - Security_Operations_-_Generate_Breach_Tasks.dfx5
    - Security_Operations_-_Generate_Incident_Response_Procedures_and_Tasks.dfx5

    - Security_Operations_-_Not_Applicable_Breach_Tasks.dfx5
    - Security_Operations_-_Not_Applicable_Incident_Response_Tasks.dfx5
- RSA Unified Collector Framework.pdf

  Note: This file contains links to the UCF installers for versions 1.3 and 1.3 SP1.

  - RSA-Unified-Collector-Framework-1.3.1.XXX.zip
    - RSA-Unified-Collector-Framework-1.3.1.XXX.exe

These files can be downloaded from the RSA SecOps 1.3 SP1 landing page on RSA Link at **https://community.rsa.com/docs/DOC-44272**.

Important: If you are upgrading from version 1.2.0.2 or 1.1.1, you must also download RSA_Archer_Security_Operations_Management_1.3.zip from **https://community.rsa.com/docs/DOC-32552**.

To set up the integration between your RSA Archer GRC and SIEM systems, you also need RSA_Unified_Collector_Framework.zip.

Note: The solution also provides Advanced Cyber Defense (ACD) CSV files, which include incident response procedures and tasks that you can import and use.

RSA Archer Security Operations Management Requirements

Before installing the RSA Archer Security Operations Management 1.3 SP1 solution, you must meet the requirements for the following components:

- **RSA Archer GRC**
- **RSA Security Analytics or Other SIEM Tools**
- **RSA Unified Collector Framework**

RSA Archer GRC Requirements

Requirement	Details
RSA Archer GRC Platform 5.5 SP3 P2 and later, or 6.0 and later.	The RSA Archer Security Operations Management solution is designed to work with specific versions of the Platform.
A user account on the RSA Archer Community on RSA Link.	You must have a user account to the Community to download the solution files.

Requirement	Details
An RSA Archer license that gives you access to the most current version of RSA Archer Security Operations Management.	RSA Archer Security Operations Management 1.3 SP1.
RSA Archer Enterprise Management 4 SP1.	This guide assumes that you have installed the RSA Archer Enterprise Management 4 SP1 solution. For installation instructions, see *RSA Archer Enterprise Management 4 SP1 Installation Guide*. **Note:** If you are using an older version of the RSA Archer GRC platform, you must upgrade the platform before upgrading the RSA Archer Enterprise Management solution.
A valid license for Microsoft Bing Maps.	You must have an active license to Microsoft Bing Maps to use the Bing maps iView in the Incident Coordinator dashboard.
For the Enterprise Management SA IM plug-in, your RSA Archer Devices application must be populated with the IP addresses, criticality rating information, and the business unit and facilities cross-references that you want to transfer to your RSA Security Analytics system.	The Enterprise Management plug-in pulls data from your Devices application. **Note:** If you need assistance populating your RSA Archer GRC system with data, RSA strongly recommends that you engage the Professional Services group. Contact your RSA Sales Representative to arrange an engagement.

RSA Security Analytics or Other SIEM Tools Requirements

Requirement	Details
RSA Security Analytics 10.5.x or later, or 10.6.0.1 or later. **Note:** RSA Security Analytics 10.6 is not supported.	TRSA Security Analytics 10.5.x or later, or 10.6.0.1 or later must be installed and running, with the Security Analytics Incident Management module configured. To enable the Command and Control fields to be exported to RSA Archer GRC, you must be running RSA Security Analytics 10.6.0.1 or later.
Other supported third-party SIEM tools	For supported SIEM tools, see the **RSA Archer Community on RSA Link**.

RSA Unified Collector Framework (UCF) Requirements

Requirement	Details
An independent system running any of the following: • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 **Important:** Enable .NET Framework 3.5 using the Add Roles and Features Wizard. RSA also recommends that this system has 8 GB RAM with a dual core processor and minimum of 10GB of available hard drive space. **Important:** You must install the UCF on a separate 64-bit system.	The system needs network connectivity to both your SIEM system and your RSA Archer GRC Platform, and is where you install the UCF. **Important:** Ensure that the time on your UCF system and the RSA Archer GRC Platform are synchronized, or with a difference of no more than one second.

Requirement	Details
64-bit Java Runtime Environment (JRE) 1.8.	The RSA Unified Collector Framework (UCF) requires the use of this software. **Important:** Java Cryptographic extension 8 files (JCE8) files must be replaced in the <*java-install-dir*>\lib\security folder. For more information, see **Upgrade the UCF from RSA Archer Security Operations Management 1.2**.
64-bit Microsoft Visual C++ 2010 Runtime	The UCF installs this software if it is not already installed.
Windows security updates.	Ensure that all Windows security updates are applied to your system before installing the UCF.

Prepare to Install or Upgrade and Configure RSA Archer Security Operations Management 1.3 SP1

Procedure

1. Ensure that you have access to the following:
   - Depending on your RSA Archer GRC version number:
     - (5.x) RSA Archer GRC Platform Help
     - (6.x) RSA Archer GRC Online Documentation
   - RSA Archer GRC Platform Control Panel Help
2. Read and understand the relevant section, based on your RSA Archer GRC version:
   - (5.x) The “Managing Packages” section of the RSA Archer GRC Platform Help.
   - (6.x) The "Packaging" section of the RSA Archer GRC Online Documentation.
3. Obtain the *Data Dictionary* for the solution by contacting your RSA Archer Account Representative, or by calling 1-888-539-EGRC. The *Data Dictionary* contains the configuration information for the solution.

4. Do one of the following:
   - For new installations, do the following:
     a. **Install the RSA Archer Security Operations Management Solution**.
     b. **Install the RSA Unified Collector Framework**.
     c. **Configure Third-Party Tools**.
   - To upgrade from RSA Archer Security Operations Management 1.3, do the following:
     a. **Install the RSA Archer Security Operations Management Solution**.

        Important: If you have customized fields, contact your RSA Professional Services representative.

     b. **Upgrade the RSA Unified Collector Framework**.
     c. **Configure Third-Party Tools**.
   - To upgrade from RSA Archer Security Operations Management 1.2.0.2, do the following:
     a. **Install the RSA Archer Security Operations Management Solution**.

        Important: If you have customized fields, contact your RSA Professional Services representative.

     b. **Upgrade the RSA Unified Collector Framework**.

        Important: You must first upgrade the UCF to version 1.3, then upgrade again to version 1.3 SP1.

     c. **Migrate the RSA Connector Framework**.
     d. **Configure Third-Party Tools**.
   - To upgrade from RSA Archer Security Operations Management 1.1 SP1, do the following:
     a. **Install the RSA Archer Security Operations Management Solution**.
     b. **Upgrade the RSA Unified Collector Framework**.

        Important: You must first upgrade the UCF to version 1.3, then upgrade again to version 1.3 SP1.

     c. **Configure Third-Party Tools**.

Chapter 2: Installing the RSA Archer Security Operations Management Solution

Download the Solution File from the RSA Archer Community on RSA Link 22
Back Up the Database 22
Import the Install Package 23
Update the License Key 23
Performing Advanced Package Mapping 23
Install the Solution Package 24
Review the Package Installation Log 26
Create the Security Operations Management Group 26
Create a New Crisis Event Status 27
Configure Bing Maps 27
Create a User Account for the RSA Archer Web Service Client 28
RSA Archer Security Operations Management Data Feeds 28
Importing ACD Content 31
Post-Install Activities 33
Test the Solution 36

Download the Solution File from the RSA Archer Community on RSA Link

Procedure

Download the RSA_Archer_Security_Operations_Management_1.3.1_Install_Package.zip file for RSA Archer Security Operations Management 1.3 SP1 from the RSA Archer Community on RSA Link at **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange**.

Back Up the Database

After a solution package has been installed, the installation cannot be rolled back (reversed). RSA recommends that you create a backup of your database before installing the new package in case you need to return to a pre-install state.

Important: You must be a database administrator to perform this task.

Procedure

Back up the database according to the standards and procedures of your company.

Import the Install Package

Procedure

1. Click Administration > Application Builder > Install Packages.
2. In the Available Packages section, click Import to open the Select Import File dialog box.
3. Click Add New, then locate and select the package file that you want to import.
4. Click OK.

Update the License Key

Note: You must update the license key if you are installing a new application or questionnaire. If you are updating existing applications or questionnaires, you do not need to update the license key.

The administrator (a web or database administrator) on the server on which the RSA Archer Control Panel resides must update the license key in the RSA Archer Control Panel before the application package is imported in order for the new applications and questionnaires to be available for use.

Procedure

Update the license key. For instructions, see "Update a License Key" in the RSA Archer Control Panel Help.

Important: If you do not update the license key prior to installing the solution package, you may receive package failures.

Performing Advanced Package Mapping

To perform this task, you must be a user with an access role that has rights to install a package. When you install the latest solution package, you must perform Advanced Package Mapping to avoid creating duplicate objects.

Important: Advanced Package Mapping does not update data feeds and Web APIs. If you modify the system ID of an object used by a data feed or Web API, the data feed or Web Service API will not function properly. You must update the data feed and Web Service API to reference the new system ID of the object. Changing the system ID of a field can adversely affect data feeds or calculations that use the field. Before you execute the mapping process, RSA recommends that you back up your database.

As part of Advanced Package Mapping, you can do the following:

- Map objects
- Review the Package Mapping Log
- Export Mapping Settings
- Import Mapping Settings
- Undo Package Mapping Changes

Advanced Package Mapping requires a considerable amount of memory, which can result in loss of data input and IE errors when working with large applications. System performance may vary based on the size of a package file.

Note: To optimize your system for packaging, RSA recommends using Silverlight 5.1.3 or later.

For information about advanced package mapping and its components, see "Advanced Package Mapping" in either the RSA Archer GRC Platform Help (5.x), or the RSA Archer GRC Online Documentation (6.x).

Install the Solution Package

Important: When you install a package that updates a subform, the updates affect all applications, questionnaires, workspaces, and dashboards that use the subform.

Important: If you are upgrading the solution, you must confirm which applications are in use outside of the RSA Archer Security Operations Management solution. Verify that all application versions are compatible.

Procedure

1. Click Administration > Application Builder > Install Packages.
2. In the Available Packages section, locate the package file that you want to install, and click Install.

   Note: Do not update any previously installed applications.

3. Modify the components of the installation package, as follows:

a. In the Configuration section, select the components of the package that you want to install.

   Note: By default, RSA Archer GRC only selects new applications, so you must select all other applications and questionnaires as needed.

b. In the Install Method section, for each component, select one of the following options.

Option	Description
Create New Only	Creates new objects that do not currently exist in the instance. Does not update existing objects. During a solution upgrade, this option preserves any customization made to the objects in a previous version. **Important:** You must manually update any existing items that you want to change. See the *Data Dictionary* for field information.
Create New and Update	Creates new objects and updates existing objects that match objects in the package. **Note:** If you are installing the solution for the first time, ensure that you select Create New and Update.

c. In the Layout section, for each component, select one of the following options.

Option	Description
Override Layout	Replaces the existing layout with the layout in the package. Moves fields that were previously on the layout that are not on the package layout to the Available Fields list. **Important:** If you select this option, you will lose any customization that you have made to your existing layout. **Note:** If you are installing the solution for the first time, ensure that you select Override Layout.
Do Not Override Layout	No changes are made to the existing layout, but you may have to modify the layout after installing the new package.

4. Click Install, and click OK.
   For sample installation log messages, see **Package Installation Log Message Examples**.

Review the Package Installation Log

Procedure

Review the Package Installation Log to determine if you need to take specific action to resolve issues. For more information on the log messages, see "Package Installation Log Messages" in either the RSA Archer GRC Platform Help (5.x), or the RSA Archer GRC Online Documentation (6.x).

For example, you may need to install specific dependent solutions or applications. For information on the dependencies for each solution, see the *Data Dictionary*.

For additional examples and remediation information for common Package Installation Log messages, see **Package Installation Log Message Examples**.

Create the Security Operations Management Group

Once you have installed the RSA Archer Security Operations Management package, you must create a Security Operations Management group to make it the parent group of all the other SOC subgroups that were added during installation.

Procedure

1. Click Navigation > Administration > Access Control > Manage Groups.
2. Click Add New.
3. In the Name field, enter Security Operations Management.
4. In the Members section, locate and select the following groups from the Available list:
   - SOC : Business Manager
   - SOC : CISO/CSO
   - SOC : Compliance/Privacy Officer
   - SOC : HR
   - SOC : Incident Coordinator
   - SOC : IT Helpdesk
   - SOC : L1 Incident Handler
   - SOC : L2 Incident Handler
   - SOC : Legal

- SOC : SOC Manager
- SOC : Solution Administrator

5. Click Save.

Create a New Crisis Event Status

Note: This procedure is only required if you have licensed the RSA Archer Business Continuity Management solution.

The RSA Archer Security Operations Management solution allows users to create a new Crisis Event record from either an incident, investigation, or a data breach record. You must create a new Status field value named Under Review for new Crisis Events created from RSA Archer Security Operations Management, so that when a RSA Archer Security Operations Management user creates a new crisis event, the crisis response team can determine whether to approve or reject the record.

Procedure

1. Click Administration > Application Builder > Manage Applications.
2. Click Crisis Events.
3. Click the Fields tab.
4. Click the Status field.
5. Click the Values tab.
6. Click Add New.
7. In the Text Value field, enter Under Review.
8. Save the field and the application.

Configure Bing Maps

The Incident Coordinator dashboard provides a Bing maps iView, however you must have a Bing maps license and configure the mapping connection for this iView to work. The administrator (a web or database administrator) on the server on which the Archer Control Panel resides must configure the mapping connection in the Archer Control Panel.

Procedure

Configure the mapping connection. For instructions, see "Configure the Mapping Connection" in the RSA Archer GRC Platform Control Panel Help.

Create a User Account for the RSA Archer Web Service Client

You must create a user account for the web service client to use to transfer data into the RSA Archer GRC Platform.

Note: If you are upgrading from RSA Advanced Incident Management for Security 1.1, you can use the same user account that you already created.

Procedure

1. Click Administration > Access Control > Manage Users.
2. In the Manage Users section, click Add New.
3. In the General Information section, enter a first name, last name, and user name.
4. In the Localization section, set the time zone to (UTC) Dublin, Edinburgh, Lisbon, London.
5. In the Localization section, set the locale to English (United States).
6. Click the Groups tab, and do the following:
   a. In the Groups section, click Lookup.
   b. In the Available Groups window, expand Groups.
   c. Expand the Security Operations Management group.
   d. Scroll down and select SOC: Solution Administrator and EM: Read Only.
   e. Click OK.
7. Click Save.

RSA Archer Security Operations Management Data Feeds

RSA Archer Security Operations Management includes the following data feed files:

- Security_Operations_-_Generate_Breach_Tasks.dfx5
- Security_Operations_-_Generate_Incident_Response_Procedures_and_Tasks.dfx5
- Security_Operations_-_Not_Applicable_Breach_Tasks.dfx5
- Security_Operations_-_Not_Applicable_Incident_Response_Tasks.dfx5

The Generate Breach Tasks and Generate Incident Response Procedure and Tasks data feeds automatically create tasks based on the response templates associated with a record. For example, when an Incident Handler selects a category for an incident, the Generate Incident Response Procedures and Tasks data feed copies all incident response procedures that match that category and associates them with the incident. If a task becomes unnecessary due to a change in the related impacted regulation, the Not Applicable data feeds make a copy of that task and list it in the Not Applicable section of a Breach Task record or an Incident Response Task record.

You must import each data feed and schedule it to run as frequently as you need. By default, the feeds are scheduled to run every minute. If you encounter any performance impacts, please contact RSA Archer Professional Services for assistance.

Import a Data Feed

Procedure

1. Click Administration > Integration > Manage Data Feeds.
2. In the Manage Data Feeds section, click Import.
3. Locate and select the .dfx5 file for the data feed.
4. From the General tab in the General Information section, in the Status field, select Active.
5. Click the Transport tab. Complete the fields in the Transport Configuration section as follows:
   a. In the URL field, type: *<YourServerName>*/*<VirtualDirectoryName>*/ws/search.asmx
   b. In the Instance field, type the name of the Platform instance from which the data feed is coming (this is the instance name as you enter it on the Login window).
6. In the Security section, type the username and password of a Platform user that has API access and access to all of the records on the Platform instance (from which the data feed is coming). For instructions on creating a user account, see **Create a User Account for the RSA Archer Web Service Client**.
7. For the Security_Operations_-_Generate_Incident_Response_Procedures_and_Tasks.dfx5 data feed only, do the following:
   a. Click the Navigation tab.
   b. In the XML File Definition section, locate the File tag under the Task_Attachment element and replace C:\ArcherFiles\Repository\ with your file repository location.

Note: This location could be a relative path or an absolute path based on your RSA Archer Control Panel setting. The Absolute Patch is the entire path of the file repository. The Relative Path is the shortened path from the Home Directory configured in Datafeed Settings.

8. For the Security_Operations_-_Generate_Breach_Tasks.dfx5 feed only, do the following:
   a. Click the Source Definition tab and expand the attachment.
   b. In the File field, edit the calculation and replace C:\ArcherFiles\Repository\ with your file repository location.

      Note: This location could be a relative path or an absolute path based on your RSA Archer Control Panel setting.
9. Ensure that all required fields are complete.
10. Click Save.

    Note: After clicking save, you may receive one or more warning messages. Click Ignore and continue installing the solution.

Schedule a Data Feed

Important: A data feed must be active and valid to successfully run.

As you schedule your data feed, the Data Feed Manager validates the information. If any information is invalid, an error message is displayed. You can save the data feed and correct the errors later; but the data feed does not process until you make corrections.

Procedure

1. Click Administration > Integration > Manage Data Feeds.
2. In the Name column, click the data feed that you want to edit.
3. Click the Schedule tab.

   Note: The Schedule tab is available for both Standard and Transport-Only data feed types.
4. In the Frequency drop-down list, set the frequency for the data feed. For example, if you select Minutely and specify 3 in the Every field, the data feed runs every 3 minutes.
5. (Optional) To configure a data feed to run immediately after another data feed, follow these steps:

a. In the Frequency drop-down list, select Reference.

b. In the Reference Feed drop-down list, select the first data feed. Your current data feed would run after this selected one.

6. (Optional) To override the data feed schedule and immediately run your data feed, in the Run Data Feed Now section, click Start.

7. Click Save.

Importing ACD Content

As of version 1.2, the RSA Archer Security Operations Management solution allows you to import RSA Advanced Cyber Defense (ACD) content into each level of the Incident Response Procedure Library application. You can:

- Import ACD Incident Response Procedure content into the Incident Response Procedures level.
- Import ACD Incident Response Task content into the Incident Response Task level.

Note: You can download the Incident_Response_Procedures_OOTB_RSA_ACD.zip from the RSA Archer Community on RSA Link at **https://community.rsa.com/docs/DOC-23985**.

Prepare to Import ACD Data

You must update two fields in the Incident Response Procedure Library application.

Procedure

1. At the Incident Response Procedure level, change the key field to Procedure Name, as follows:

   a. Click Administration > Application Builder > Manage Applications.

   b. In the Manage Applications section, select the Incident Response Procedure Library application.

   c. Click the Fields tab, and in the Incident Response Procedures level, select the Procedure Name field.

   d. Click the Options tab.

   e. In the Options section, in the Key Field field, select the checkbox.

   f. Click Save.

2. At the Incident Response Task level, change the minimum value of the Step Number field.

a. In the Incident Response Task level, select the Step Number field.
b. Click the Options tab.
c. In the Minimum Value field, verify that the minimum value to 0.

   Note: If the minimum value is not 0, set it to 0.

d. Click Save.

3. Click Save.

Import ACD Data into Incident Response Procedure Library

If you are importing data into a leveled application, you must import data into the parent level before importing data into the child level. Do the following procedure to import data specific to the Incident Response Procedures level, and then repeat the steps to import data specific to the Incident Response Tasks level.

Procedure

1. Click Administration > Integration > Manage Data Imports.
2. In the Manage Data Imports section, from the Incident Response Procedure Library application, select one of the following levels:
   - To import incident response procedures, select the Incident Response Procedures level.

     Important: You must import incident response procedures before importing incident response tasks.

   - To import incident response tasks, select the Incident Response Tasks level.
3. In the General Information section, click Browse.
4. From the File Upload window, click Add New. Select the one of the following:
   - If you are importing incident response procedures, select the OOTB ACD Procedures.csv file, and click Open.
   - If you are importing incident response tasks, select the OOTB ACD Tasks.csv file, and click Open.
5. Click OK.
6. In the Format Options section, in the HTML Formatting field, select File Contains HTML Formatting.

   Note: If this option is not selected, and are included in the application fields.

7. From the General Information section, in the Import Type drop-down list, select Create New Records.
8. In the Import Field Mapping section, ensure that all the values in the Application Fields row match the column headers. If a value does not match,

click the drop-down list for the item, and select the appropriate value.

Important: When you import the incident response tasks, map Procedure Name to Incident Response Procedure (Procedure Name).

9. Click Next.
10. Ensure that the summary information from the Data Import Wizard is correct, and click Import.
11. Repeat steps 1 – 10 to import data into the Incident Response Tasks level.

For more information about data imports, see "Data Imports" in the RSA Archer GRC Platform Help (5.x), or the RSA Archer GRC Online Documentation (6.x).

Perform ACD Data Post Import Activities

After completing the data import, you must update the Incident Response Procedure Library key field and add additional values to the Response Phase values list.

1. Change the key field of the Incident Response Procedure Library application to Incident Response Procedure ID, as follows:
   a. Click Administration > Application Builder > Manage Applications.
   b. In the Manage Applications section, select the Incident Response Procedure Library application.
   c. Click the Fields tab, and in the Incident Response Procedures level, select the Incident Response Procedure ID field.
   d. Click the Options tab.
   e. In the Options section, in the Key Field field, select the checkbox.
   f. Click Save.
2. Click Save.

Post-Install Activities

The package installation does not update some attributes of objects, or delete obsolete objects that are not included in the current solution. RSA recommends that you compare the objects in your database with the information in the *Data Dictionary* to determine which objects are obsolete or have been updated.

Deleting Obsolete Objects

Packaging does not delete obsolete objects. RSA recommends that you delete these objects because they may affect how the applications function. Follow these guidelines on deleting obsolete objects:

- If you select Override Layout when you install the solution install package, the Packager does not remove old fields from the layout. You must delete the old

fields.

- Evaluate your need for certain data-driven events (DDE), pre-existing rules, and actions that were not updated through Packaging. Delete any obsolete rules and actions.
- Verify the DDE order and update it if necessary.
- Evaluate pre-existing notifications and reports that Packaging did not update. Delete obsolete notifications and reports.

For more information about objects, see either the “Managing Packages” section of the RSA Archer GRC Platform Help (5.x), or the "Packaging" section of the RSA Archer GRC Online Documentation (6.x).

Validating Formulas and Calculation Orders

Follow these guidelines on validating formulas and calculation orders:

- The packaging process logs an error if a formula does not validate. This error may be caused by a formula that references applications or fields that do not exist in the instance and were not part of the package (for example, fields in applications that are part of a different core solution). Review those fields to determine if they are needed.
  - If a field is needed, modify the formula to remove references to applications or fields that do not existing in your instance. Fields that do not exist in your instance are identified with an exclamation mark.
  - If a field is not needed, delete the field or remove it from the layout. If the field is not deleted, removing the formula prevents errors from being written in the log files when records are saved.
- Verify the order of calculations for each application and sub-form in the solution. See the *Data Dictionary* for calculation orders for each individual application or sub-form.
- Update the order of calculations as needed for each application and subform in the solution.

For more information about deleting objects, see the "Managing Calculations" section of the RSA Archer GRC Platform Help (5.x), or the “Deleting Fields” section of the RSA Archer GRC Online Documentation (6.x).

Verifying Key Fields

Packaging does not change key fields. To verify the key fields in each application, see the RSA Archer Security Operations Management *Data Dictionary*.

Updating Record Permissions Fields to Allow Access to Other Solution Records

The access roles in the RSA Archer Security Operations Management package provide read-access rights to records in the Crisis Events application (in the RSA Archer Business Continuity Management solution) and the Risk Register application (in the RSA Archer Risk Management solution), if you have licensed these solutions.

However, the package does not update any Record Permissions fields in those applications, so users must still be selected in a Record Permissions field in a record in order to view that record.

RSA recommends that you work with your Business Continuity Management and Risk Management solution administrators to determine which RSA Archer Security Operations Management users require access to Crisis Events or Risk Register records and to update any Record Permissions fields necessary to provide default access.

Verifying the Upgrade from RSA Advanced Incident Management for Security 1.1

If you have upgraded from RSA Advanced Incident Management for Security 1.1, the following changes have occured:

- In the Security Incidents application, you have two new tabs: Forensic Analysis and Remediation. The Results tab also has new sections and the Overview tab has a couple new fields.
- In the Incident Response subsolution, you have two new applications: Forensic Analysis and Incident Investigations.
- You have three new subsolutions: Data Breach Response, SOC Program Management, and Issue Management.
- You have six new dashboards for each primary solution user role.
- The Incident Coordinator dashboard provides a Bing maps iView.

  Note: You must have a Bing maps license installed for this iView to work.

- Incident Response Procedures and Tasks can now be created from the Incident Response Procedure Library records that match the selected category.

Test the Solution

Procedure

Test the RSA Archer Security Operations Management 1.3 SP1 solution according to your company standards and procedures, to ensure that the solution works with your existing processes. Some of the items that you may want to include in your testing are:

Item	Action
Customized objects and fields	Ensure that they are present.
Notifications	Ensure that the notifications are firing.
Calculations	Ensure that calculations are functioning.
Workflows	Ensure that workflows are correct.

Chapter 3: Installing the RSA Unified Collector Framework

RSA Unified Collector Framework Integrations 37
RSA Security Analytics Incident Management Integration Options 37
Create RSA Archer User Accounts for Push and Pull 38
Set Up the RSA Unified Collector Framework 40

RSA Unified Collector Framework Integrations

The RSA Unified Collector Framework (UCF) allows you to integrate your RSA Archer Security Operations Management system with the following:

- Security Analytics Incident Management (SA IM)
- Security Analytics Event Stream Analysis (SA ESA)
- Security Analytics Reporting Engine (SA RE)
- Splunk
- McAfee ESM
- IBM QRadar
- Other generic SIEM tools

RSA Security Analytics Incident Management Integration Options

RSA Security Analytics Incident Management integrates with the RSA Archer Security Operations Management solution with different levels of access. You must select the same options in both RSA Security Analytics Incident Management and the RSA Unified Collector Framework (UCF).

The following table describes the different integration options and what data is transported for each option.

Integration option	Data transported into RSA Archer
Manage incidents workflow exclusively in the RSA Archer Security Operations Management solution	Incidents, alerts, and events **Note:** Once incidents are transported into RSA Archer Security Operations Management, incidents and remediation tasks are no longer visible in RSA Security Analytics.
Manage incidents workflow in the RSA Security Analytics Incident Management module	Data breaches Remediation tasks (as Findings), which can be assigned to either the GRC or Operations queues for remediation. **Note:** When updates are made in RSA Archer Security Operations Management, the remediation status is automatically synchronized across the two systems. Incidents (records are read only)

Create RSA Archer User Accounts for Push and Pull

Two RSA Archer user accounts are required to avoid conflicts while sending and receiving data from RSA Security Analytics.

Procedure

1. Click Administration > Access Control > Manage Users > Add New.
2. In the First and Last Name fields, enter a name that indicates that the UCF uses this account to push data into RSA Archer GRC. For example, UCF User, Push.

   Note: When configuring the Pull account, enter a name that indicates that the UCF uses this account to pull data from RSA Archer GRC. For example, UCF User, Pull.

3. (Optional) Enter a user name for this new user account.

   Note: If you do not specify a user name, the RSA Archer GRC Platform creates the user name from the first and last name entered when you save the new user account.

4. In the Contact Information section, in the Email field, enter an email address to associate with this new user account.

5. In the Localization section, change the time zone to (UTC) Coordinated Universal Time.

   Note: The UCF uses UTC time to baseline all the time related calculations.

6. In the Account Maintenance section, enter and confirm a new password for the new user account.

   Important: Note the user name and password for the new user account that you just created. You need to enter these credentials when you set up the UCF to communicate with the RSA Archer GRC Platform through the web service client.

7. Clear the Force Password Change On Next Sign-In option.
8. In the Security Parameter field, select the security parameter that you want to use for this user.

   Note: If you assign a default security parameter with a password change interval of 90 days, you also must update the user account password stored in the SA IM Integration Service every 90 days. To avoid this, you can optionally create a new security parameter for the SA IM Integration Service user account and set the password change interval to the maximum value allowed by your corporate standards.

9. Click the Groups tab, and do the following:
   a. In the Groups section, click Lookup.
   b. In the Available Groups window, expand Groups.
   c. Scroll down and select SOC: Solution Administrator and EM: Read Only.
   d. Click OK.
10. Click Save, then click Apply.
11. If the machine language and regional settings of your RSA Archer GRC system are set to anything other than English-US, do the following:
    a. Open the user account you just created, and in the Localization section, in the Locale field, select English (United States), and click Save.
    b. On the Windows system hosting your RSA Archer GRC Platform, open Internet Information Services (IIS) Manager.
    c. Expand your RSA Archer GRC site, click .Net Globalization, in both the Culture and UI Culture fields, select English (United States), and click Apply.
    d. Restart your RSA Archer GRC site.
12. Repeat steps 1 – 11 to create a second user account for the UCF to pull data from RSA Archer GRC.

Set Up the RSA Unified Collector Framework

Procedure

1. **Install the RSA Unified Collector Framework.**
2. **Configure Endpoints.**
3. **Set the Maximum Number of Alerts or Events Sent Through the SA IM Integration Service.**

Install the RSA Unified Collector Framework

Procedure

1. Verify which version of RSA Archer Security Operations Management is installed. If the solution is not installed, see **Installing the RSA Archer Security Operations Management Solution**. If any version other than 1.2 or later is installed, see **Upgrade the UCF from RSA Archer Security Operations Management 1.1 or 1.1 SP1**.
2. Download and install JRE 8 from Oracle's website.
3. Replace the Java Cryptography Extension (JCE) files with the JCE 8 files as follows:
   a. Download the JCE 8 files from Oracle's website.
   b. Replace the files in the <*install_dir*>\java\jre1.8.0_xx\lib\security folder.
4. Double-click RSA-Unified-Collector-Framework-1.3.1.XXX.exe.
5. Read and accept the license agreement,.
6. Click Next.
7. Complete the InstallShield Wizard, as follows:
   a. Click Next.
   b. Read and accept the license agreement.
   c. Click Next.
   d. (Optional) To change the destination path, do the following:
      i. Click Change.
      ii. Select your destination, and click OK.
   e. Click Next.
   f. Click Install.
   g. Click Finish.

8. Once installation is complete, verify that the following folders were created:
   - C:\Program Files\RSA\SA IM integration service. The RSA Unified Collector Framework automatically starts.
   - C:\Program Files\RSA\SecOps Watchdog Service. The RSA SecOps Watchdog service automatically starts.

Configure Endpoints

Endpoints provide the connection details required for the UCF to reach both your RSA Security Analytics and RSA Archer GRC systems. For port information, see **RSA Unified Collector Framework Ports**.

Important: Some endpoints are necessary to use different integrations. The following table shows the mandatory endpoints.

Mandatory Endpoint	Integration
RSA Archer Push	Syslog endpoint Security Analytics Incident Management (SA IM)
RSA Archer Pull	Enterprise Management plug-in endpoint SA IM
Security Analytics Incident Management	SA IM Mode selection: SecOps or Non-SecOps mode. **Note:** If Non-SecOps mode is selected, incidents are managed in SA IM instead of RSA Archer Security Operations Management.
Enterprise Management	Asset content from RSA Archer GRC to RSA Security Analytics.
Syslog Server	Any supported and generic SIEM **Note:** You must configure the TCP, secure TCP, and UDP ports.

Note: Ensure the certificate subject name for your RSA Archer GRC server matches the hostname.

Important: To install certificates, port 22 must be open.

Procedure

1. On your UCF system, open the Connection Manager, as follows:
   a. Open a command prompt.
   b. Change directories to <*install_dir*>\SA IM integration service\data-collector.
   c. Type:

      ```
      runConnectionManager.bat
      ```
2. In the Connection Manager, enter 1 for Add Endpoint.
3. Add an endpoint for pushing data to RSA Archer Security Operations Management, as follows:
   a. Enter the number for RSA Archer.

      Note: SSL must be enabled to add the RSA Archer endpoints.

   b. For the endpoint name, type push.
   c. Enter the URL of your RSA Archer GRC system.
   d. Enter the instance name of your RSA Archer GRC system.
   e. Enter the user name of the user account you created to push data into your RSA Archer GRC system.
   f. Enter the password for the user account you created to push data into your RSA Archer GRC system, and confirm the password.
   g. When asked whether this account is used for pulling data, enter False.
4. Add an endpoint for pulling data from RSA Archer Security Operations Management, as follows:
   a. Enter the number for RSA Archer.

      Note: SSL must be enabled to add the RSA Archer endpoints.

   b. For the endpoint name, type pull.
   c. Enter the URL of your RSA Archer GRC system.
   d. Enter the instance name of your RSA Archer GRC system.
   e. Enter the user name of the user account you created to pull data from your RSA Archer GRC system.
   f. Enter the password for the user account you created to pull data from your RSA Archer system, and confirm the password.
   g. When asked whether this account is used for pulling data, enter True.

5. Add an endpoint for RSA Security Analytics Incident Management, as follows:
   a. Enter the number for Security Analytics IM.
   b. Enter a name for the endpoint.
   c. Enter the SA Host IP address.
   d. For SA Port, enter 5671.
   e. Enter the target queue for remediation tasks. Selecting All processes both the RSA Archer Integration (GRC) and IT Helpdesk (Operations).
   f. To automatically add certificates to the Security Analytics trust store, do the following:
      i. Enter Yes.
      ii. Enter the SA Host username and password.

      Note: If you receive an error that the CA trust store failed to set, see **Security Analytics Incident Management Integration Troubleshooting**.

6. In UCF connection manager, select the mode, as follows:
   a. Enter the number for Mode Selection.
   b. Select one of the following options:
      - Manage incident workflow in RSA Security Analytics.
      - Manage incident workflow exclusively in RSA Archer Security Operations Management.

      Note: For more information on the integration options, see **Security Analytics Incident Management Integration Options**.

7. Add the RSA Archer Enterprise Management Endpoint, as follows:
   a. Enter the number for Enterprise Management.
   b. Complete the following fields:

Field	Description
Endpoint Name	Optional endpoint name.
Web Server Port	Defaults to 9090. Can be configured to host the web server url. The URL with the port number should be provided as the URL in SA Live feed: http(s)://hostname:port/archer/sa/feed

Field	Description
Criticality	Criticality of the assets to be pulled from RSA Archer GRC. If false, pulls assets with any criticality. If true, pulls assets with only high criticality. To configure this manually, edit the em.criticality property in the collector-config properties file to provide a comma-separated list of criticalities: LOW, MEDIUM, HIGH. See **Change Feed Settings**.
Feed Directory	Directory where the assets CSV file from RSA Archer GRC are saved. **Note:** The directory path provided must exist.
Web Server Username	Username for authenticating to the EM web server. **Note:** This is provided while configuring the SA live feed.
Web Server Password	Password for authenticating to the EM web server. **Note:** This is provided while configuring the SA live feed.
SSL Mode	Defaults to No. If No, the URL uses http mode: http://hostname:port/archer/sa/feed If Yes, the URL uses https mode: https://hostname:port/archer/sa/feed **Note:** If you have not updated the host file, see **Update the RSA Security Analytics Host File for SSL Mode**.

c. If you selected Yes for SSL mode, complete the following fields:

- Copy certs to SA box. Enter Yes to have the certificates automatically copied from RSA Archer Security Operations Management to RSA Security Analytics.
- SA Host. Enter the hostname or IP address of the SA server
- SA Host Username. Enter the username for logging in to the SA server to copy the certificates.
- SA Host Password. Enter the password for logging in to the SA server to copy the certificates.

Note: If copying the certificates fails and adding the endpoint failed, manually copy the certificates. See **Manually Copy Enterprise Management Certificates**. After copying the certificates, you must add the Enterprise Management plug-in without automatically copying the certificates.

d. To configure the Enterprise Management web server as a Security Analytics live feed, **configure the SA Live Feed.**

8. To use third-party integrations, add the Syslog Server Endpoint, as follows:

   a. Enter the number for Syslog Server Endpoint.

   b. Enter the following:

Field	Description
SSL configured TCP port	Secure TCP port if the Syslog client sends the Syslog message in secure TCP mode. **Note:** Defaults to 1515. If you do not want to host the Syslog server in this mode, enter 0.
TCP port	Enter the TCP port if the Syslog client sends the Syslog message in TCP mode. **Note:** Defaults to 1514. If you do not want to host the Syslog server in this mode, enter 0.
UDP port	Enter the UDP port if the Syslog client sends the Syslog message in UDP mode. **Note:** Defaults to 514. If you do not want to host the Syslog server in this mode, enter 0.

Note: By default, the Syslog server runs in the above three modes, unless it is disabled by entering 0.

   c. To test the Syslog client, enter the number for Test Syslog Client. Use the Test Syslog client with the files from <*install_dir*>\SA IM integration service\config\mapping\test-files\.

9. In Connection Manager, enter 5 to test each endpoint.

(Optional) Set the Maximum Number of Alerts or Events Sent Through the RSA Unified Collector Framework

By default, the UCF sends all the alerts associated with an incident and all the events associated with an alert into the RSA Archer Security Operations Management solution. If this is more data than you need, you can set limits on the number of alerts or events sent.

Procedure

1. Stop the UCF, as follows:
   a. Click Control Panel > Administrative Tools > Services.
   b. Select RSA Unified Collector Framework.
   c. Click Stop.
2. Open the <*ucf_intall_dir*>\config\collector-config.properties file.
3. Do one or both of the following:
   - In the sa.alertsInIncident property, enter a valid integer. To allow all alerts, enter a value of 0.
   - In the sa.eventsInAlert property, enter a valid integer. To allow all events, enter a value of 0.
4. Save the <*ucf_intall_dir*>\config\collector-config.properties file.
5. Start the UCF, as follows:
   a. Click Control Panel > Administrative Tools > Services.
   b. Select RSA Unified Collector Framework.
   c. Click Start.

Chapter 4: Upgrading the RSA Unified Collector Framework

Upgrading the UCF from RSA Archer Security Operations Management 1.3 47
Upgrading the UCF from RSA Archer Security Operations Management 1.2 48
Upgrade the UCF from RSA Archer Security Operations Management 1.1 or 1.1 SP1 50
Migrate the RSA Connector Framework 51
Uninstall the RSA Connector Framework (RCF) 52

Upgrading the UCF from RSA Archer Security Operations Management 1.3

If you are upgrading from RSA Archer Security Operations Management 1.3, you must upgrade the middleware. Through the UCF and Connection Manager, all endpoints configured in 1.3 are migrated to RSA Archer Security Operations Management 1.3 SP1. If the Syslog server and EM plug-in were configured to use Secure TCP in 1.3, the secure connection is migrated to 1.3 SP1. Using the RSA SecOps Watchdog Service, you can monitor the UCF.

Important: Before upgrading the UCF, ensure that you fulfill the requirements found at RSA Archer Security Operations Management Requirements.

Upgrade the UCF from RSA Archer Security Operations Management 1.3

Prerequisites

- Install the RSA Archer Security Operations Management Solution
- Ensure that you have upgraded RSA Security Analytics to version 10.5.x or later, or 10.6.0.1 or later.

  Note: RSA Security Analytics 10.6 is not supported.

Procedure

1. Stop the RSASAIMDC and RSA Connector Framework services.

   Note: If RSASAIMDC Service cannot be completely stopped, force close the process.

2. Close any open applications or processes, including any open Connection Manager sessions.
3. Run the RSA-Unified-Collector-Framework-1.3.1.XXX.exe installer.
4. Once installation is complete, verify the following folders were created:
   - C:\Program Files\RSA\SA IM integration service. The RSA SA IM Data collector automatically starts.
   - C:\Program Files\RSA\SecOps Watchdog Service. The RSA SecOps Watchdog service automatically starts.
5. Verify that the RSA SA IM and RSA SecOps Watchdog services are running.
6. Test the existing endpoints or configure additional endpoints. For instructions, see **Configure Endpoints**.

   Once endpoint configuration is complete, you are notified about whether the certificates were successfully verified.

   Note: After upgrading to 1.3.1, the UCF uses the existing certificates. To regenerate certificates, see **Regenerate Certificates**.

Upgrading the UCF from RSA Archer Security Operations Management 1.2

If you are upgrading from RSA Archer Security Operations Management 1.2, you must first upgrade the middleware to version 1.3, then upgrade again to version 1.3 SP1. Through the UCF and Connection Manager, all endpoints configured in 1.2 are migrated to RSA Archer Security Operations Management 1.3 SP1. If the Syslog server and EM plug-in were configured to use Secure TCP in 1.2, the secure connection is migrated to 1.3 SP1 through the RCF migration. Using the RSA SecOps Watchdog Service, you can monitor the UCF.

Important: Before upgrading the UCF, ensure that you fulfill the requirements found at **RSA Archer Security Operations Management Requirements**.

Upgrade the UCF from RSA Archer Security Operations Management 1.2

Important: You must first upgrade the UCF to version 1.3, then upgrade again to version 1.3 SP1.

Prerequisites

- **Install the RSA Archer Security Operations Management Solution**
- Ensure that you have upgraded RSA Security Analytics to version 10.5.x or later, or 10.6.0.1 or later.

Note: RSA Security Analytics 10.6 is not supported.

- Ensure that you have downloaded RSA_Archer_Security_Operations_Management_1.3.zip from **https://community.rsa.com/docs/DOC-32552**.

Procedure

1. Stop the RSASAIMDC and RSA Connector Framework services.

   Note: If the RSASAIMDC Service cannot be completely stopped, force close the process.

2. Close any open applications or processes, including any open Connection Manager sessions.
3. Download and install JRE 8 from Oracle's website.
4. Replace the Java Cryptography Extension (JCE) files with the JCE 8 files as follows:
   a. Download the JCE 8 files from Oracle's website.
   b. Replace the files in the <*install_dir*>\java\jre1.8.0_xx\lib\security folder.
5. Run the RSA-Unified-Collector-Framework-1.3.XXX.exe installer.
6. After the 1.3 installation completes, stop the RSA SecOps Watchdog and RSA Unified Collector Framework services.
7. Run the RSA-Unified-Collector-Framework-1.3.1.XXX.exe installer.
8. Once installation is complete, verify the following folders were created:
   - C:\Program Files\RSA\SA IM integration service. The RSA SA IM Data collector automatically starts.
   - C:\Program Files\RSA\SecOps Watchdog Service. The RSA SecOps Watchdog service automatically starts.
9. Verify that the RSA SA IM and RSA SecOps Watchdog services are running.
10. To test existing endpoints or configure additional endpoints, see **Configure Endpoints**.
    Once endpoint configuration is complete, you are notified about whether the certificates were successfully verified.

    Note: After upgrading to 1.3.1, the UCF uses the existing certificates. To regenerate certificates, see **Regenerate Certificates**.

11. If you used the RCF in the previous version, do the following:
    a. Add the RSA Archer GRC push and pull accounts. See steps 3 to 4 in **Configure Endpoints**.
    b. **Migrate the RSA Connector Framework**.

c. If migration was successful and the configuration functions, **Uninstall RSA Connector Framework**

Upgrade the UCF from RSA Archer Security Operations Management 1.1 or 1.1 SP1

After upgrading the RSA Archer Security Operations Management solution, you must first upgrade the middleware to version 1.3, then upgrade again to version 1.3 SP1. Through the RSA Unified Collector Framework (UCF) and Connection Manager, all endpoints configured in 1.1 or 1.1 SP1 are migrated to RSA Archer Security Operations Management 1.3 SP1. If the Syslog server and Enterprise Management plug-in were configured to use Secure TCP in 1.1 or 1.1 SP1, the secure connection is migrated to 1.3 SP1 through the RCF migration. Using the RSA SecOps Watchdog Service, you can monitor the UCF.

Note: RSA strongly recommends contacting Professional Services for assistance upgrading and migrating your data.

Custom modifications made to the solution are not automatically preserved during the upgrade process. For example, if you modified a packaged field to make it required in RSA Archer Security Operations Management 1.1, your changes may be overwritten when you upgrade to version 1.3 SP1 if you select Create New and Update during the installation. If you have made extensive modifications to your existing solution, RSA recommends contacting your Sales representative to engage Professional Services prior to upgrading.

Important: Before upgrading the UCF, ensure that you fulfill the requirements found at **RSA Archer Security Operations Management Requirements**.

Upgrade the UCF from RSA Archer Security Operations Management 1.1 or 1.1 SP1

Important: You must first upgrade the UCF to version 1.3, then upgrade again to version 1.3 SP1.

Prerequisites

- **Install the RSA Archer Security Operations Management Solution**
- Ensure that you have upgraded RSA Security Analytics to version 10.5.x or later, or 10.6.0.1 or later.

  Note: RSA Security Analytics 10.6 is not supported.

- Ensure that you have downloaded RSA_Archer_Security_Operations_Management_1.3.zip from **https://community.rsa.com/docs/DOC-32552**.

Procedure

1. Stop the RSA Connector Framework service.
2. Close any open applications or processes, including any open Connection Manager sessions.
3. Download and install JRE 8 from Oracle's website.
4. Replace the Java Cryptography Extension (JCE) files with the JCE 8 files as follows:
   a. Download the JCE 8 files from Oracle's website.
   b. Replace the files in the <*install_dir*>\java\jre1.8.0_xx\lib\security folder.
5. Run the RSA-Unified-Collector-Framework-1.3.XXX.exe installer.
6. After the 1.3 installation completes, stop the RSA SecOps Watchdog and RSA Unified Collector Framework services.
7. Run the RSA-Unified-Collector-Framework-1.3.1.XXX.exe installer.
8. Once installation is complete, verify the following folders were created:
   - C:\Program Files\RSA\SA IM integration service. The RSA SA IM Data collector automatically starts.
   - C:\Program Files\RSA\SecOps Watchdog Service. The RSA SecOps Watchdog service automatically starts.
9. Add the RSA Archer GRC push and pull accounts. See steps 3 to 4 in **Configure Endpoints**.
10. To test existing endpoints or configure additional endpoints, see **Configure Endpoints**.
11. If you used the RCF in the previous version, do the following:
    a. **Migrate the RSA Connector Framework**.
    b. **Uninstall the RSA Connector Framework (RCF)**.

Migrate the RSA Connector Framework

If you are upgrading from a previous version of RSA Archer Security Operations Management and used the RSA Connector Framework (RCF), complete this task. All of the previous mapping files for the old RCF components have been migrated to now use secops_import_archer.xml, and secops_export_archer.xml for the Enterprise Management plug-in. All of the old components are now configured using a single Connection Manager endpoint.

Procedure

1. Open a new Command Prompt.
2. Change directories to <*install_dir*>\SA IM integration service\data-collector.
3. Type:

   `runConnectionManager.bat`
4. Enter the number for RCF Migration.
5. Enter the number for each endpoint to migrate.
6. To migrate Security Analytics ESA, do the following:
   a. Enter the number for Security Analytics Event Stream Analysis.
   b. Enter TRUE for migrating the mapping file.
   c. Enter the RCF keystore and RCF truststore passwords.
7. To migrate the EM plug-in, do the following:
   a. Enter the number for Enterprise Management.
   b. Enter TRUE for migrating the mapping file.
   c. Enter the username and password for authenticating the URL from the SA feed.
   d. Enter the RCF keystore password.
8. If the mapping file customizations have been migrated from the RCF, restart the RSA Unified Collector Framework service.
9. Test each endpoint.
10. Verify that alerts from Security Analytics are received by RSA Archer GRC.
11. Verify that Business Context is received by Security Analytics through the EM plug-in.

Uninstall the RSA Connector Framework (RCF)

When you uninstall the RCF, all of the Framework components are uninstalled.

Note: Uninstalling the RCF does not remove the RSA Connector Framework folder, the logs subdirectory, or any files in the logs subdirectory. To remove these files, manually delete them.

Procedure

1. Click Start > Programs > EMC > RSA Connector Framework > Uninstall.
2. When prompted to uninstall, click Yes.
3. Click Finish.

Appendix A: Configuring Integrations

This appendix provides additional tasks for configuring and managing integrations.

Configure RSA Security Analytics for the Enterprise Management Plug-In 53
Configure RSA Security Analytics Incident Management 57
Configure Splunk 61
Configure IBM QRadar 61
Configure McAfee Enterprise Security Manager (ESM) 63
Configure Syslog Output Action for the Reporting Engine for Security Analytics 65
Configure ESA Syslog Notification Settings in Security Analytics 67
Configure a Generic SIEM Tool 70
Update the RSA Security Analytics Host File for SSL Mode 74
Manually Copy Enterprise Management Certificates 75

Configure RSA Security Analytics for the Enterprise Management Plug-In

To configure RSA Security Analytics for the Enterprise Management (EM) plug-in, you must add new metadata keys so that RSA Archer GRC asset criticality data is visible as a new metadata element in RSA Security Analytics. Next you must also create a recurring feed task to define the feed that RSA Security Analytics must download from the SA IM Integration Service and push to the Decoders.

Procedure

1. If you selected SSL mode for the Enterprise Management plug-in, **Update the RSA Security Analytics Host File for SSL Mode**.
2. (Optional) **Configure RSA Security Analytics Live Feed**.
3. **Update the Concentrator and Decoder Services.**
4. **Create Recurring Feed Task.**

Configure RSA Security Analytics Live Feed

You can configure the Enterprise Management web server as a Security Analytics live feed and get asset information.

Important: If you selected SSL mode for the Enterprise Management plug-in, see **Update the RSA Security Analytics Host File for SSL Mode** before configuring the live feed.

Procedure

1. Log in to RSA Security Analytics.
2. From the dashboard, select Live > Feeds.
3. Click Add New Feed.
4. Select Custom Feed.
5. Define the feed, as follows:
   a. Select Recurring.
   b. Enter a name for the feed.
   c. Enter the URL: http(s)://<*hostname:port*>/archer/sa/feed
   d. Select authenticated.
   e. Enter the username and password that was used to add the Enterprise Management endpoint.
   f. In the Recur Every field, enter the period of time after which data from RSA Archer GRC has to be refreshed.

      Note: The job to pull the RSA Archer GRC asset information runs immediately after the EM endpoint is configured. By default, it is scheduled to run at 1 AM everyday. Users can change this by modifying the em.getArcherAsset.schedule and emJobSchedule properties in the collector-config.properties file.

   g. To configure the fields in the CSV file, select Advanced Options and select the XML file from the feed directory.

      Note: You can also configure the column names instead of providing the XML feed information. For more information, see **Create a Recurring Feed Task**.
6. Select the services to get the feed data.
7. Review the feed configuration.
8. Click Finish.
9. **Update the Concentrator and Decoder Services**.

Update the Concentrator and Decoder Services

The SA IM Integration Service manages the files for a custom feed and deposits these files in a local folder that you specify when you configure the SA IM Integration Service. The Live module of RSA Security Analytics retrieves the feed files from this folder. Live then pushes the feed to the Decoders, which start creating metadata based on captured network traffic and the feed definition. To make each Concentrator aware of the new metadata created by the Decoders, you must edit the index-concentrator-custom.xml, and index-logdecoder-custom.xml, and index-decoder-custom.xml files.

Procedure

1. In the Security Analytics Menu, click Administration > Services.
2. Select your Concentrator, and in the Device Grid toolbar, select View > Config.
3. Click the Files tab.
4. From the drop-down list, select index-concentrator-custom.xml.
   - Do one of the following:
     - If content already exists in the file, add a key for the new meta data element as follows:

       <key description="Criticality" format="Text" level="IndexValues" name="criticality" defaultAction="Open"/>

       Important: If you copy and paste this text, ensure that it is formatted on a single line.
     - If the file is blank, add the following content:

       <?xml version="1.0" encoding="utf-8"?>
       <language level="IndexNone" defaultAction="Auto">
       <key description="Criticality" format="Text" level="IndexValues" name="criticality" defaultAction="Open"/>
       </language>
5. Click Apply.
6. If no devices are listed, click Apply.
7. To add multiple devices, do the following:
   a. Click Push.
   b. Select the devices to which you want to push this file.
   c. Click OK.
8. Repeat steps 1-7 for the Log Decoders and Index Decoders, using index-logdecoder-custom.xml and index-decoder-custom.xml.
9. Stop and start the Concentrator and Decoder services.

Create a Recurring Feed Task

In order for RSA Security Analytics to download feed files from the SA IM Integration Service and push the feeds to Decoders, you must create a recurring feed task and define the feed settings.

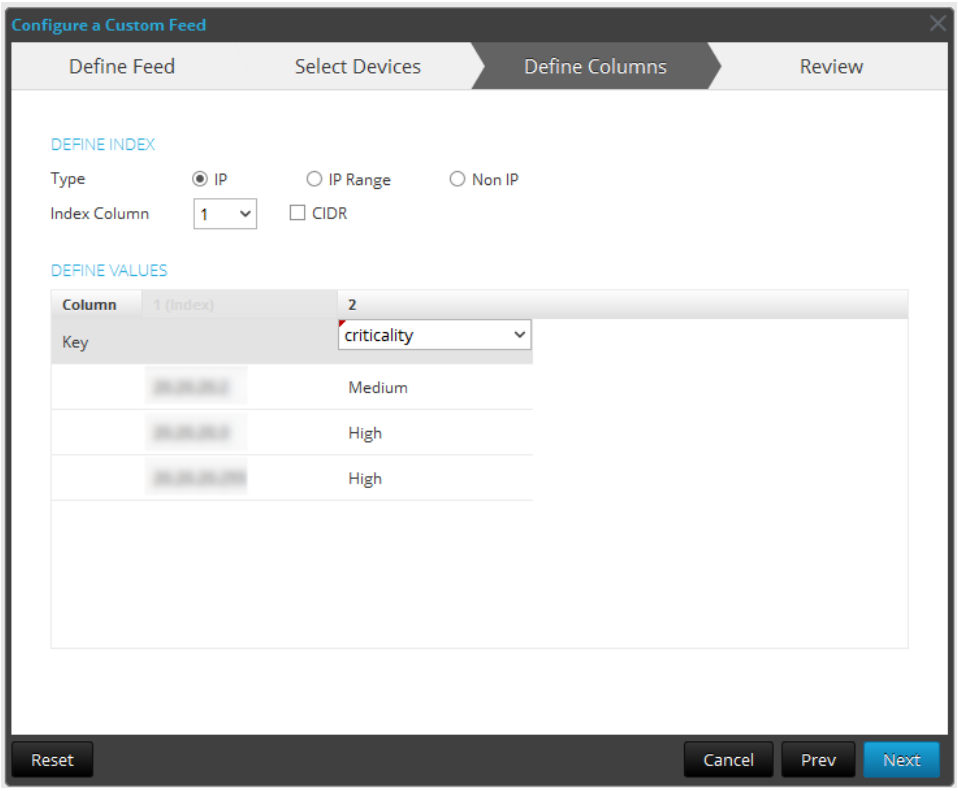
Procedure

1. In the Security Analytics Menu, click Live > Feeds.
2. Click **+**.
3. Select Custom Feed, and click Next.
4. Select Recurring.
5. Enter a name for the feed.
6. In the URL field, enter one of the following:
   - *http*://*ucf_hostname*/archer/sa/feed
   - *https*://*ucf_hostname_or_ip*:*port*/archer/sa/feed

   where *http(s)*://*ucf_hostname_or_ip*:*port* is the address of your SA IM Integration Service system. Use https if you have enabled SSL communication with RSA Security Analytics. For example: http://10.10.10.10:9090 or https://10.10.10.10:8443.

   Note: If EM is running in SSL mode, the hostname must be used in the URL.
7. Select Authenticated.
8. In the User Name and Password fields, enter the credentials of the user account you created for RSA Security Analytics to use to access files on the SA IM Integration Service system.
9. Define the recurrence interval for the feed.
10. In the Date Range section, define a start and end date for the feed.
11. Click Next.
12. Select each Decoder to which you want to push this feed.
13. Click Next.
14. In the Type field, ensure that IP is selected.
15. In the Index Column field, select 1.

16. In the second column, set the Key value to criticality.



17. Click Next.
18. Review your feed configuration details, and click Finish.

Configure RSA Security Analytics Incident Management

Procedure

1. Select the Mode for SA IM
2. Forward Security Analytics Alerts to the SA IM Service
3. Forward RSA Enterprise Compromise Assessment Tool (ECAT) Alerts to the SA IM Service
4. Aggregate Alerts into Incidents

Select the Mode for SA IM

Procedure

1. In the Security Analytics menu, click Incidents > Configure.
2. Click the Integration tab.

3. Select from the given options.
   - Manage incident workflow in RSA Security Analytics.
     - Allow analysts to escalate remediation tasks for the Operations target queue as tickets.
     - Allow analysts to escalate remediation tasks for the GRC target queue as Findings.
     - Allow analysts to report data breaches and trigger the breach response process in the RSA Archer Security Operations Management solution.
   - Manage incident workflow exclusively in RSA Archer Security Operations Management.
4. Click Apply.

Update the Normalization Scripts for RSA Security Analytics Incident Management

Users of RSA Security Analytics Incident Management can update the normalization scripts to enable the new fields

Procedure

1. Open normalize_core_alerts.js located in opt/rsa/im/scripts/normalize.
2. Type:

   ```
   cd /opt/rsa/im/scripts/normalize
   ```

3. Click Enter.
4. Type:

   ```
   vi normalize_core_alerts.js.
   ```

5. Click Enter.
6. In the generateEventInfo method, insert the following JSON code lines at the beginning of the function:

   ```
   category: Utils.stringValue(event.category),
   action: Utils.stringValue(event.action),
   event_source: Utils.stringValue(event.event_source),
   level: Utils.intValue(event.level),
   did: Utils.stringValue(event.did),
   risk_info: Utils.stringValue(event.risk_info),
   risk_warning: Utils.stringValue(event.risk_warning),
   risk_suspicious: Utils.stringValue(event.risk_
   suspicious),
   client: Utils.stringValue(event.client),
   ```

```
threat_source : Utils.stringValue(event.threat_source),
threat_desc : Utils.stringValue(event.threat_desc),
service : Utils.stringValue(event.service),
```

7. Save the file.
8. Restart the Incident Management Service in RSA Security Analytics. Type:

```
service rsa-im restart
```

Forward Security Analytics Alerts to the SA IM Service

Procedure

1. To forward Security Analytics Event Stream Analysis alerts to SA IM, do the following:
   a. In Security Analytics, click Administration > Services > ESA service.
   b. Click Actions > View > Config for the ESA service.
   c. Click the Advanced tab.
   d. Verify that Forward Alerts on Message Bus is selected. If it is not select, select the checkbox.
   e. (Version 10.6.0.1 only) If you want to enable Command and Control field exports, select Enable Automated Threat Detection.
   f. Click Apply.
2. To forward Security Analytics Reporting Engine alerts to SA IM, do the following:
   a. In Security Analytics, click Administration > Services > Reporting Engine service.
   b. Click Actions > View > Config for the RE service.
   c. Click the General tab.
   d. Click System Configuration section, and verify that Forward Alerts to IM is selected. If it is not selected, select the checkbox, and click Apply.
3. To forward Security Analytics Malware Analysis alerts to SA IM, do the following:
   a. In Security Analytics, click Administration > Services > Malware Analysis service
   b. Click Actions > View > Config for the MA service.
   c. Click the Auditing tab.
   d. In the Incident Management Alerting section, verify that Enabled Config Value is selected. If it is not selected, select the checkbox, and click Apply.

Forward RSA Enterprise Compromise Assessment Tool (ECAT) Alerts to the SA IM Service

RSA ECAT alerts can be sent to RSA Archer GRC through SA IM.

Procedure

1. In RSA ECAT, click Configure > Monitoring and External Components.
2. In the External Components Configuration window, select the Incident Message Broker.
3. Click Add (+).
4. Complete the following fields:
   - Instance Name
   - Server Hostname/IP. Enter the Host DNS or IP address of the RSA Security Analytics Server.
   - Port Number. The default port is 5671
5. Click Save.
6. See the *RSA Enterprise Compromise Assessment Tool 4.1 User Guide* to set up SSL for ECAT and SA IM communication.

Aggregate Alerts into Incidents

Alerts coming into SA IM can be automatically aggregated into incidents and forwarded to RSA Archer Security Operations Management. Aggregation rules are automatically run every minute and aggregate the alerts into incidents based on the match conditions and grouping options selected. For more information on aggregating alerts, see the RSA Security Analytics Online Documentation.

Procedure

1. In Security Analytics, go to Incidents > Configure > Aggregation Rules.
2. To enable the rules provided out of the box, do the following:
   a. Double-click the rule.
   b. Select Enabled.
   c. Click Save.
   d. Repeat steps a-c for each rule.
3. To add a new rule, do the following:
   a. Click Add (+).
   b. Select Enabled.

c. Complete the following fields:
   - Rule Name
   - Action
   - Match Conditions
   - Grouping Options
   - Incident Options
   - Priority
   - Notifications

d. Click Save.

Configure Splunk

To configure Splunk, see the *RSA Archer Security Operations Management Splunk Implementation Guide*, located on the RSA Archer GRC Community on RSA Link at: **https://community.rsa.com/community/products/grc/overview**.

Configure IBM QRadar

Procedure

1. In IBM QRadar, go to the Offenses tab, and click Rules.
2. In the Group drop-down, select Suspicious.
3. In the Actions drop-down, click New Event Rule.
4. In the Rule Wizard, define the rule, as follows:

Field	Description
When the destination IP is one of the following:	IP address
An account failed to log on in the when the event matches:	Event Name
N events are seen with the same Event Name in *N* minute.	1

5. In the Groups list, select Suspicious.
6. Select the following:
   - Severity
   - Credibility
   - Relevance
   - Ensure the detected event is part of an offense

- Include detected events by Source IP from this point forward, in the offense, for: 60 second(s)
- Annotate event
- Send to Forwarding Destinations

7. In the Forwarding Destination Properties dialog, do the following:
   a. Enter the Name, IP address, and Destination Port of the forwarding destination.
   b. In the Event Format drop-down, select JSON.
   c. In the Protocol drop-down, select TCP.
   d. In the Profile field, upload the template.
   e. Click Save.
8. Complete the Forwarding Profile Properties dialog, as follows:
   a. Enter the profile name.

      Note: The profile name should hold the string containing the dynamic keys, which will be replaced with the correct value by the javascript parser in the UCF when breaking the message into key/value pairs.

      Example: Profile name = aggregationcriteria:QRadar-$src - $dst , ruleName:Failed

      This will be broken into two keys: aggregationcriteria and ruleName. The value for aggregationcriteria will populated with the value of src key and dst key value by the javascript parser to the following: QRadar-10.7.22.102 - 10.7.227.103. Due to limitation of 55 characters for the profile name, the ruleName will be truncated.
   b. In the Preamble field, enter IBM QRadar.
   c. In the ISO Date Format field, select MM-dd-yyyy hh:mm:ss.
   d. In the Selected Properties section, select the checkbox next to Type to select all properties.
   e. Click Save.
9. Verify the rule properties on the Rule Summary page, and click Finish.
10. Test the rule. See **IBM QRadar Test Example.**

Configure IBM QRadar for Secure TCP Connection

Procedure

1. Add the event forwarding destination to the rule in IBM QRadar with the UCF server details.
2. Select SSL over TCP.

3. Enter the destination address and port number.
4. Copy the rootcastore.ctr.der file from the C:\Program Files\RSA\SA IM integration service\cert-tool\certs folder.
5. On the IBM QRadar host, paste the file in the /opt/qradar/conf/trusted_ certificates folder.
6. Configure the UCF Syslog endpoint over a secure TCP connection. See step 8 in **Configure Endpoints**.

IBM QRadar Test Example

Procedure

1. Purposely fail three attempts to login to the IP address.
2. In IBM QRadar, click the Offenses tab.
3. Click All Offenses.
4. Verify that the offense is listed for the new rule.

Configure McAfee Enterprise Security Manager (ESM)

Procedure

1. In McAfee Enterprise Security Manager (ESM), load the templates, as follows:
   a. Click System Properties > Alarms > Settings > Templates.
   b. Select Basic Syslog Template, and click Add.
   c. Copy the templates from the C:\Program Files\RSA\SA IM integration service\config\mapping\templates\SecOps_McAfee_Template.txt file.
   d. Paste the templates into the Message Body field.
   e. Click OK.
2. Identify the correlation rule ID, as follows:
   a. In the navigation pane, click Correlation Engine > Correlation.
   b. Select the rule.
   c. At the bottom of the Policy Editor window, copy the Signature ID.

      Note: The Signature ID is used as a condition for forwarding the events through Syslog.

3. Create an alarm for forwarding the events through Syslog, as follows:
   a. Click System Properties > Alarms > Add.
   b. Click the Summary tab, and do the following:
      i. In the Assignee field, select a user.
      ii. Select Enabled.
   c. On the Condition tab, paste the Signature ID into the Value(s) field.
   d. On the Devices tab, select the relevant devices.
   e. Click the Actions tab, and do the following:
      i. Select Send Message, and click Configure.
      ii. In the Message Template window, in the Syslog drop-down, select Group By DestinationIP.
      iii. In the Date Format drop-down, select mm/dd/yyyy hh:mm:ss.
      iv. Click OK.
   f. Add a recipient, as follows:
      i. Click Add recipient.
      ii. Click Syslog.
      iii. Select the Syslog Recipients, and click Add.

      Note: The recipient must be the UDP port that was configured in the UCF.

      iv. Complete the fields in the Add Syslog Recipient window.
      v. Click OK.
   g. Ensure the alarm is present on the Alarms tab.
4. Generate alerts for testing. See **McAfee Enterprise Security Manager (ESM) Test Example**.

McAfee Enterprise Security Manager (ESM) Test Example

Procedure

1. Purposely fail to connect to the McAfee machine.
2. After 3-5 minutes, check for the Syslog message in the UCF.
3. In McAfee ESM, click Alarms to verify the event details.

Configure Syslog Output Action for the Reporting Engine for Security Analytics

Procedure

1. In Security Analytics, go to Administration > Services.
2. Select your Reporting Engine Service, and click System > Config.
3. Click the Output Actions tab.
4. In the SA Configuration section, in the Host Name field, enter the host name or IP address of your Reporting Engine server.

   Important: If you do not enter a value in this field, the link in the RSA Archer Security Alerts application back to Security Analytics will not work.

5. Add the Syslog Configuration as follows:
   a. In the Server Name field, enter the hostname of the UCF.
   b. In the Server Port field, enter the port that you selected in the UCF Syslog configuration.
   c. In the Protocol field, select the transport protocol.

      Note: If you select Secure TCP, SSL must be configured.

6. Click Save.

Configure SA RE SSL for Secure Syslog Server

If the Syslog server is configured with Secure TCP, configure the SSL.

Procedure

1. Copy the certificate keystore.crt.der from the UCF machine at <*install_dir*>\RSA\SA IM integration service\cert-tool\certs to the Security Analytics server at /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.31-1.b13.el6_6.x86_64/jre/lib/security.
2. Run the following command:

   ```
   keytool -import -file keystore.crt.der -alias ucf-syslog -
   keystore cacerts -storepass changeit
   ```

3. Restart the RE service.

Configure Rules in Security Analytics

In RSA Security Analytics, rules are filters that you create for specific metadata, which result in defined actions when matches are found. For configuring RSA Security Analytics Reporting Engine (SA RE), you must create rules to define the conditions that trigger an alert to be escalated to your RSA Archer GRC Platform. You can create network and application rules. For more information about rules, see the *RSA Security Analytics User Guide*.

Procedure

1. Click Reports > Manage.
2. In Groups, click Rules.
3. Click Add (+).
4. Enter a name for the new group.
5. Select the group you created, and in the Rule toolbar, click Add (+).
6. In the Syslog Name field, enter a name for the SecOps syslog configuration to be used to configure alerts.
7. In the Rule Type field, select NetWitness DB.
8. Enter a name for the rule.
9. Enter values in the Select and Where fields based on the rule that you want to create.

   Note: Add the Syslog configuration with the Syslog name set above.

10. Click Save.

    Note: To see the same number of alerts in SA RE and RSA Archer GRC, ensure that you've selected Once for execute in both the Syslog and Record tabs.

Add Alert Templates for the Reporting Engine in Security Analytics

The UCF syslog configuration comes with out-of-the-box alert templates that you can use when you create an alert with a syslog output action. These templates define the criteria used to aggregate alerts into incidents in your RSA Archer GRC Platform.

The sample templates are located in the following location on the UCF system:

<*install_dir*>\SA IM integration service\config\mapping\templates\SecOps_SA_Templates

Procedure

1. Click Reports > Manage > Alerts.
2. Click the Template tab.
3. Click Add (+).
4. In the Name field, enter a name for the alert template.
5. In the Message field, enter the alert message.
6. Click Create.
7. Repeat steps 3 to 6 for each alert template that you want to add.

Configure Alerts in Security Analytics

In RSA Security Analytics Reporting Engine, an alert is a rule that you can schedule to run on a continuous basis and log its findings to several different alerting outputs.

Procedure

1. Click Reports > Manage > Alerts.
2. Click Add (+).
3. Select Enable.
4. Select the rule you created.
5. Select Push to Decoders.

   Important: If you do not enter a value in this field, the link in the RSA Archer Security Alerts application to RSA Security Analytics will not work.

6. From the Data Sources list, select your data source.
7. In the Notification section, select Syslog.
8. Click Add (+).
9. Complete the Syslog configuration fields.
10. In the Body Template field, select the template that you want to use for this Syslog alert.
11. Click Save.

Configure ESA Syslog Notification Settings in Security Analytics

Procedure

1. Click Administration > System > Global Notifications.
2. Click the Output tab.
3. Define and enable an ESA Syslog notification.

4. Click the Servers tab.
5. Define and enable a Syslog notification server.
6. In the Syslog Server Configuration section, enter the following:

Field	Description
Server Name	Specify the hostname or IP Address of the system on which you installed the UCF.
Server Port	Specify the port number on which you want the UCF to listen for Syslog alert messages.
Facility	Specify the Syslog facility.
Protocol	Select the protocol.

7. Click Save.

Configure SA ESA SSL for Secure Syslog Server

If the Syslog server is configured with Secure TCP, configure the SSL.

Procedure

1. Copy the certificate keystore.crt.der from the UCF machine at <*install_dir*>\SA IM integration service\cert-tool\certs to the ESA box at /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.31-1.b13.el6_6.x86_64/jre/lib/security.
2. Run the following command:

   ```
   keytool -import -file keystore.crt.der -alias ucf-syslog -
   keystore cacerts -storepass changeit
   ```

3. On the ESA machine, replace the /opt/rsa/esa/conf/wrapper.conf trustStore with trustStoreIgnored, as follows:

   ```
   wrapper.java.additional.4=-
   Djavax.net.ssl.trustStoreIGNORED=/opt/rsa/esa/esa_
   truststore
   ```

   ```
   wrapper.java.additional.5=-
   Djavax.net.ssl.trustStoreIGNOREDPassword=netwitness
   ```

4. Restart the ESA service.

Add ESA Alert Templates in Security Analytics

The UCF syslog configuration comes with out-of-the-box alert templates that you can use when you create an alert with a syslog output action. These templates define the criteria used to aggregate alerts into incidents in your RSA Archer GRC Platform.

The sample templates are located in the following location on the UCF system:

<*install_dir*>\SA IM integration service\config\mapping\templates\SecOps_SA_Templates\SecOps_SA_ESA_templates.txt

Procedure

1. Click Administration > System > Global Notifications.
2. Click the Templates tab.
3. Click Add (+).
4. In the Template Type field, select Event Stream Analysis.
5. In the Name field, enter the name for the template.
6. (Optional) In the Description field, enter a brief description for the template.
7. In the Template field, enter the alert message.
8. Click Save.
9. Repeat steps 3 – 8 for each alert template that you want to add.

Create ESA Rules in Security Analytics

Procedure

1. Click Alerts > Configure.
2. Select your ESA device.
3. Click Select.
4. In the ESA Rules toolbar, click **+**.
5. Select Rule Builder.
6. In the Name field, enter a name for the rule.
7. In the Description field, enter a description for the rule.
8. Select a Severity.
9. In the Condition section, do the following:
   a. Click **+** to build a statement.
   b. Enter a name, select a condition type, and add meta data/value pairs for your statement.

c. Click Save.

d. Repeat steps a – c until you have built all your statements for the rule.

10. In the Notifications section, select Syslog.
11. Select the notification, Syslog server, and template that were created previously.
12. Click Save and Close.
13. Click Alerts > Configure > Deployments.
14. Click + for ESA Services section.
15. Select the ESA Service.
16. Click Deploy Now.
17. In the ESA Rules section, click + to choose the ESA Rule that you created, and click Deploy Now.

Configure a Generic SIEM Tool

Important: SIEM tools need to send the formatted dates in UTC format for the correct timestamps to appear in RSA Archer GRC.

Procedure

1. Edit the message-script-identifier.js file in the <*install_dir*>\SA IM integration service\config\mapping\scripts folder as follows:

   a. Compare and map the messages for each SIEM.

   Note: The following is a sample of a CEF message format: <*Date*><*Time*>host CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|[Extension]

   b. If the format is not CEF, add code to link the corresponding javascript parser to parse the message. For example:

   ```
   else{ if(message.indexOf('IBM QRadar')>=0){
   scriptResponse = buildReponse("ibm-
   qradar.js","IBMQRADAR","2"); } }
   ```

   c. For a CEF format, add an else condition to the script. For example:

   ```
   else{
   if(siemVendor == "McAfee" && siemProduct ==
   "ESM"){
   scriptResponse = buildReponse("mcafee-
   esm.js","McAfeeESM","2");
   ```

}

}

d. Build the response definitions with the following arguments:

- Argument 1 - Script file name. This file contains the logic and specific handling to a SIEM message parsing.
- Argument 2 - Unique name which identifies the SIEM. The same prefix that is used if SIEM specific mappings are using instead of generic mappings.
- Argument 3 - Because there are three sets of applications in RSA Archer GRC, Security Events, Security Alerts and Security Incidents, the integration and the data present in the message can be a two-level or three-level integration.

  Note: A two-level integration pushes the message as a Security Alert and Security Incident when the alerts are aggregated to the incident. A three-level integration pushes the message as a Security Event, Security Alert, and Security Incident.

2. Create a new SIEM specific parsing javascript file as follows:

   a. Create a new javascript file for each SIEM tool with the name defined in step 1. For example: (<*install_dir*>\SA IM integrationservice\config\mapping\scripts\mcafee-esm.js).

   b. Copy and paste the content from any of the existing CEF standard parsing code. For example: saesa.js or sare.js.

   c. If using generic mappings, update the generic key to the incoming key mapping as defined in the var init=function() in the javascript file. For example:

```
if(siemProduct == "Security Analytics (ESA){
    scriptResponse == buildResponse("saesa.js","SAESA","3");
}else if(siemProduct == "Splunk"){
    scriptResponse == buildResponse("splunk.js","SPLUNK","2");
}else if(siemProduct == "Security Analytics (RE)"){
    scriptResponse == buildResponse("sare.js","SARE","2");
}else if(siemVendor == "McAfee" && siemProduct == "ESM"){
    scriptResponse == buildResponse("mcafee-esm.js","McAfeeESM","2");
}
```

   d. If using SIEM specific mappings, remove or comment all lines of code present in the var init=() function.

   e. Save the javascript file.

3. Update the mapping file as follows:

   a. Open the mapping file that pushes data to RSA Archer GRC located at <*install_dir*>\RSA\SA IM integration service\config\mapping\secops_

import_archer.xml.

Note: If using generic mappings with no new field additions, no changes are required to the mapping file.

b. If using SIEM specific mappings, verify that the name attribute in all of the new application tag contains the same prefix and is equal to the value given in step 1 for Argument 2. For example:

```
<application CRUDOptions="INSERT" name="McAfeeESM_Security_Alerts" cacheEnable="true">
<application CRUDOptions="UPDATE_IF_EXIST" name="McAfeeESM_Security_Incident" processAtLast="true">
<application CRUDOptions="IGNORE" name="McAfeeESM_Log_Devices">
<application CRUDOptions="IGNORE" name="McAfeeESM_Source_Devices">
<application CRUDOptions="IGNORE" name="McAfeeESM_Destination_Devices">
```

c. If using generic mappings and adding new fields, ensure that the new fields are added in the corresponding javascript file with the incoming key set to the generic key. For example:

i. In the macafee-esm.js file, to add the testField field, the var init function uses genericKeySet['testField']='generic.newkey'.

ii. In the secops_import_archer.xml file, the new field mapping reads:

```
<field name="New Field">
<UUID>New Archer GUID</UUID>
<fieldType>Field Type</fieldType>
<keyName>generic.newkey</keyName>
</field>
```

d. Save the mapping file.

Generic and SIEM Specific Mappings

For Generic SIEM, each script file has the mapping key set which maps the incoming keys present in the message to the generic key set. For Specific SIEM, specific mappings must be appended. SIEM specific mapping files can automatically be appended during the RCF migration.

Mandatory Fields in Generic SIEM

Using mandatory fields in generic SIEM ensures all incoming Syslog messages are delivered. Messages without the mandatory fields are dropped and not picked up for processing. All the mandatory fields are part of the Security Incident application in RSA Archer Security Operations Management. You can configure mandatory fields in the syslog-beans.xml file.

Important: For a Syslog message to be valid, it must have aggregationcriteria as the mandatory field.

In order to push the message to RSA Archer GRC, the following fields are mandatory for the javascript parser to populate:

- generic.aggregationcriteria
- generic.msg
- generic.summary

The summary field comes as part of the CEF header in CEF standard format as shown below:

> *<Date><Time>*host CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|[Extension]

Add New Field in SIEM Tool

Important: For adding additional fields from RSA Security Analytics, see the customization document at: **https://community.rsa.com/docs/DOC-32552**.

Procedure

1. Add the new field in RSA Archer GRC and note the GUID.
2. To add the new field in the SIEM tool configuration, do one of the following:
   - To use generic mappings, do the following:
     a. Update the key set in the SIEM specific javascript file.
     b. Add the mapping for the new field in the Generic Mapping file.
   - To use SIEM specific mappings, update the corresponding mapping file with the new field details.

Add Source Field in Alert Source

Procedure

1. Add a new value in the Source field in RSA Archer GRC, as follows:
   a. On the Administration tab, click Application Builder > Manage Applications.
   b. Open the respective application (example: Security Alerts).
   c. On the Field tab, click the Source field.
   d. On the Values tab, click Add New.
   e. Enter the Text Value with the respective value (example: SourceX).
   f. Click Save.
   g. Click Save for the field and the application to commit the new value to the field and application.
2. Extract the GUID of the newly created Source value from RSA Archer GRC as follows:

a. On the Administration tab, click Integration > Obtain API Resources > Generate API Code.

b. Select the respective application (for e.g., Security Alerts).

c. Click Download Source File.

d. Open the Security_Alerts.cs file.

e. Search for the newly created Source value.

Note: The value has a corresponding GUID (for reference: %GUID%) associated with it, which is used to configure the mapping file.

Example: public static readonly Guid SourceX = new Guid("aba5af52-0242-46cf-9df9-212e4dd32c14");

3. Add the value in the Source field of the mapping file in the UCF, as follows:

a. In the <*install_dir*>/SA IM integration service/config/mapping folder, open the secops_import_archer.xml file.

b. Navigate to the Source field under the xxxxxxx_Security Alerts application mappings.

c. In <valueFieldUUIDs> for Source field, add another element.

Example: <valueFieldUUID name="*SourceX*">%GUID%</valueFieldUUID>

Important: The element must be added wherever the Source field for Security Alerts exist in the mapping file.

d. Restart the UCF.

Update the RSA Security Analytics Host File for SSL Mode

Procedure

1. Edit the host file on the SA server at the following location:
vi /etc/hosts

2. Enter the following for the UCF host IP address:

```
<ucf-host-ip> <ucf-fqdn> <ucf-host-name>
```

3. Restart SA server by running the following command:

```
restart jettysrv
```

4. While configuring the SA live feed, enter the hostname for the URL instead of the IP address and the port number configured for Enterprise Management endpoint in the UCF:

```
https://<ucf-host-name>:<EM_Port>/archer/sa/feed.
```

5. Verify that the connection works.

Manually Copy Enterprise Management Certificates

If certificates were not automatically copied, you can manually copy the certificates.

Procedure

1. Copy the certificate keystore-em.crt from the UCF machine at the following location:

   <*install_dir*>\SA IM integration service\cert-tool\certs to the Security Analytics server at /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.31-1.b13.el6_6.x86_64/jre/lib/security.

2. Log on to the machine that has RSA Security Analytics installed.
3. Go to the location where the SA truststore certificate is copied:

   ```
   cd /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.31-1.b13.el6_6.x86_64/jre/lib/security
   ```

4. Run the following command:

   ```
   keytool -import -alias ucfcert -keystore cacerts -file keystore-em.crt.der
   ```

   Important: If you copied the certificates because adding the Enterprise Management endpoint failed, you must add the endpoint again without automatically copying the certificates. See **Configure Endpoints**.

Appendix B: Customizing and Modifying the Integration with RSA Security Analytics for Business Context

This appendix provides additional tasks for customizing and modifying the integration with RSA Security Analytics for business context.

Include Optional RSA Archer Fields 76
Create a New Context Menu Action 77
Change Feed Settings 78

Include Optional RSA Archer Fields

By default, only the IP Address and Criticality Rating fields in the RSA Archer Devices application are fed into RSA Security Analytics by the SA IM Integration Service. You can customize the Enterprise Management plug-in to include the Business Unit and Facility fields that are cross-referenced in the Devices application in the feed.

Note: If you also plan to feed Business Unit and Facility information from your RSA Archer GRC Platform into Live, you must also add keys for these fields to the index-concentrator-custom.xml file.

Procedure

1. Open <*install_dir*>\SA IM integration service\config\mapping\secops_export_archer.xml.
2. For Device Application, uncomment the businessunit and facility lines by removing <!-- and --> from the ends of the line.
3. Save and close the file.
4. Restart the UCF.
5. In the Security Analytics menu, click Administration > Devices.
6. Select your Concentrator, and in the Device Grid toolbar, select View > Config.
7. Click the Files tab.
8. From the drop-down list, select index-concentrator-custom.xml.
9. To include Business Unit meta data, add the following:

```
<key description="Business Unit" format="Text"
level="IndexValues" name="businessunit"
defaultAction="Open"/>
```

Note: If you copy and paste this text, ensure that it is formatted on a single line.

10. To include Facilities meta data, add the following:

```
<key description="Facility" format="Text"
level="IndexValues" name="facility" defaultAction="Open"/>
```

Note: If you copy and paste this text, ensure that it is formatted on a single line.

11. Click Apply.
12. Click Push, select the devices to which you want to push this file, and click OK.
13. Stop and start the Concentrator and Decoder services.
14. Open the task that you created in **Create a Recurring Feed Task**.
15. Add two additional Key values as follows.

Note: You can use the assets.xml file in the feed directory while configuring the live feed.

Column	Key
3	businessunit
4	facility

16. Click Save.
17. Restart each Decoder to which you pushed these feeds and each Concentrator to which one of these Decoders is assigned.

Create a New Context Menu Action

If you want security analysts to have the option of opening an RSA Archer GRC session to create a blank incident directly from the RSA Security Analytics interface, you can create a new context menu action to perform this action.

Procedure

1. In the Security Analytics menu, click Administration > System.
2. In the left navigation panel, click Plugins.
3. Click Add (+).
4. In the Configuration field, copy and paste the following:

```
{
 "groupName": "externalLookupGroup",
 "openInNewTab": "true",
 "urlFormat": "http://yourarcherhostname/context_
base/GenericContent/Record.aspx?id=0&moduleID=75",
 "moduleClasses": [
 "UAP.investigation.InvestigationValuesApplication"
 ],
 "type":"UAP.common.contextmenu.actions.URLContextAction",
 "version": "1",
 "id": "archerIncidentAction",
 "order": "5",
 "description": "",
 "local": "false",
 "displayName": "CreateArcherIncident",
 "modules": [
 "investigation"
 ],
 "disabled": "",
 "cssClasses": [
 "meta-value-name-link"
 ]
}
```

where *yourarcherhostname/context_base* is the hostname and context base of your RSA Archer GRC system.

5. Click OK.

Change Feed Settings

After you have set up the Enterprise Management plug-in, if you find that you are creating too much meta data or decide to include optional fields or change criticality, you may need to modify your feed settings.

Procedure

1. Open the collector-config.properties file, located in the <*install_dir*>\SA IM integration service\config\ directory.

   Note: This file contains some properties that do not apply to the Enterprise Management plug-in and can be ignored. Only the properties listed below are relevant to the Enterprise Management plug-in.

2. To change the feed frequency, enter a new value for the em.getArcherAsset.schedule property.

Note: This property uses a spring quartz scheduler cron expression to pull asset information from RSA Archer GRC. The job to pull asset information runs at start up using the RSA Archer pull account.

3. To change the criticality filter, set the em.criticality property to high, medium, or low.

   Note: To pull all devices without a criticality filter, set the em.criticality property to FALSE.

4. To change the folder location on your SA IM Integration Service system where feed files are stored, enter a value or comma-separated values for the em.filePath property.

   For example, to store the feed in your <*install_dir*>\UCF\feeds\ folder, set the property, as follows:

   `em.filePath=<install_dir>\UCF\feeds\`

5. Save and close the file.
6. Restart the UCF.

Appendix C: RSA Unified Collector Framework Administration Tasks

This appendix provides additional tasks for configuring and managing the RSA Unified Collector Framework.

Start the RSA Unified Collector Framework 80
Stop the RSA Unified Collector Framework 80
Uninstall the RSA Unified Collector Framework 80
Configure the Syslog Endpoint After Upgrade 81
Manually Copy SA IM Certificates 81
Regenerate Certificates 82
Regenerate Expired SA IM Certificates 83

Start the RSA Unified Collector Framework

Procedure

1. Click Control Panel > Administrative Tools > Services.
2. Select RSA Unified Collector Framework.
3. Click Start.

Stop the RSA Unified Collector Framework

Procedure

1. Click Control Panel > Administrative Tools > Services.
2. Select the RSA SecOps Watchdog Service. Click Stop.
3. Select RSA Unified Collector Framework. Click Stop.

   Note: If the service takes too long to shutdown, use the Task Manager to end the RSASAIMDCService.

Uninstall the RSA Unified Collector Framework

Procedure

1. Click Control Panel > Programs and Features
2. Select RSA Unified Collector Framework.

3. Click Uninstall.

Configure the Syslog Endpoint After Upgrade

Procedure

1. Open a new Command Prompt.
2. Change directories to <*install_dir*>\SA IM integration service\data-collector.
3. Type:

   ```
   runConnectionManager.bat
   ```

4. Add the Syslog Server Endpoint as follows:
   a. Enter the number for Syslog Server Endpoint.
   b. Enter the Syslog TCP Port, Secure TCP Port, and UDP Port properties. For more information, see **Mandatory Fields in Generic SIEM**.
5. To test the endpoint, enter the number for Test Syslog Client. Use the Test syslog client with the files from Installation directory\SA IM integration service\config\mapping\test-files\.

Manually Copy SA IM Certificates

If certificates were not automatically copied, you can manually copy the certificates.

Procedure

1. Copy the certificate keystore.crt.pem from the UCF machine at *install_dir*\SA IM integration service\cert-tool\certs to the Security Analytics server at a path /tmp.
2. Log on to the machine that has RSA Security Analytics installed.
3. Go to /tmp.
4. To append the UCF certificate to Security Analytics RabbitMQ, enter the following:

   ```
   cat keystore.crt.pem >>
   /etc/puppet/modules/rabbitmq/files/truststore.pem
   ```

5. Enter the following:

   ```
   >puppet agent -t
   ```

6. Once the agent completes, exit the connection manager.
7. Restart RSA Unified Collector Framework service from services.msc.
8. Run Connection Manager again to continue with the SA endpoints configuration.

Regenerate Certificates

From Connection Manager, you can regenerate certificates as needed.

Procedure

1. In Command Prompt, go to <*install_dir*>\SA IM integration service\data-collector.
2. Type:

   `runConnectionManager.bat`
3. Enter the number for Regenerate SA IM Integration Service Certificate.
4. For SA RE, SA ESA, and EM integrations migrated from RCF, rerun one of the integrations to copy the RCF keystore certificates.
5. After the certificates regenerate, verify that the following files have been updated in the <*install_dir*>\SA IM integration service\config folder:
   - keystore.p12
   - keystore-em.p12
6. Restart the RSA SA IM Integration service.
7. After generating certificates, redeploy the certificates for the following endpoints that are already configured with SSL as follows:
   a. To redeploy SA IM certificates, do the following:
      i. Edit the SA IM endpoint in Connection Manager.
      ii. Enter Yes to copy the certificates automatically to the Security Analytics trust store.
      iii. Enter the SSH credentials for the Security Analytics host.

      Note: If certificates fail to copy, manually copy the certificates. See **Manually Copy SA IM Certificates**.

   b. To redeploy certificates for the Enterprise Management plug-in, do the following:
      i. Edit the Enterprise Management Plug-in endpoint in Connection Manager.
      ii. Enter Yes to copy the certificates automatically to the Security Analytics trust store.
      iii. Enter the SSH credentials for the Security Analytics host.

      Note: If certificates fail to copy, manually copy the certificates. See **Manually Copy Enterprise Management Certificates**.

c. To manually redeploy certificates for all SIEM tools configured through Syslog with Secure TCP, do the following:

   i. If SA Event Stream Analysis (ESA) Syslog is configured in Secure TCP Mode, see **Configure SA ESA SSL for Secure Syslog Server**.

   ii. If SA Reporting Engine (RE) Syslog is configured in Secure TCP Mode, see **Configure SA RE SSL for Secure Syslog Server**.

   iii. If IBM QRadar Syslog is configured for Secure TCP connection, see **Configure IBM Qradar for Secure TCP Connection**.

Regenerate Expired SA IM Certificates

SA IM certificates are valid for two years. If the SA IM certificates are expired, you can regenerate and copy the certificates.

Procedure

1. In Command Prompt, go to <*install_dir*>\SA IM integration service\data-collector.
2. Type:

   ```
   runConnectionManager.bat
   ```

3. Enter the number for Regenerate SA IM Integration Service Certificate.
4. In the SA IM endpoint in Connection Manager, enter the number for Edit Endpoint.
5. Enter Yes to copy the certificates automatically to the Security Analytics trust store.

   Note: If certificates fail to copy, manually copy the certificates. See **Manually Copy Certificates**.

Appendix D: RSA SecOps Watchdog Service

This appendix provides information about the RSA SecOps Watchdog Service counters and conditions.

RSA SecOps Watchdog Service Conditions 84
RSA SecOps Watchdog Service Counters 86
Watchdog Configured Cron Time 88
Watchdog Hours Configured For Total Counter 88
Add the Watchdog Service to the Performance Monitor 88
Start the RSA SecOps Watchdog Service 89
Stop the RSA SecOps Watchdog Service 89

RSA SecOps Watchdog Service Conditions

Condition	Action	Result	Sample Log Entry
None of the endpoints (SA or Syslog) are configured.	Do nothing.		1 Watchdog.log No endpoints are configured currently.
No records created/updated in RSA Archer GRC in Last *N* Hours (TOTAL_NUM_MESSAGES_UCF_TO_ARCHER).	Restart the UCF.	The UCF shuts down and starts up.	2 Watchdog.log 0 Records written to RSA Archer GRC in the configured limit. Restarting Windows Service.

Condition	Action	Result	Sample Log Entry
No records created/updated in RSA Archer GRC (NUM_MESSAGES_UCF_TO_ARCHER) in the hour prior to when Watchdog runs, but there are messages waiting in the RabbitMQ queue in that hour (TOTAL_NUM_OF_MESSAGES_IN_INCIDENT_QUEUE).	Restart the UCF.	The UCF shuts down and starts up.	3 Watchdog.log 0 Records written to RSA Archer GRC in the last hour, while 15 record(s) are waiting to be processed from RabbitMQ. Restarting Windows Service.

Condition	Action	Result	Sample Log Entry
The UCF service is down.	Watchdog service checks if the UCF service is down at the scheduled time and starts the UCF if it is down.	The UCF service starts.	5 Watchdog.log <*Date*><*Time*>,408 | INFO - WatchdogContainerApplication.performUcfServiceOperations(193) | RSASAIMDC service The service has not been started. <*Date*><*Time*>,408 | INFO - WatchdogContainerApplication.performUcfServiceOperations(193) | RSASAIMDC service <*Date*><*Time*>,408 | INFO - WatchdogContainerApplication.doServiceWaitRestart(143) | Waiting 40 seconds to stop the RSASAIMDC service... <*Date*><*Time*>,424 | INFO - WatchdogContainerApplication.performUcfServiceOperations(182) | Attempting to start RSASAIMDC service. <*Date*><*Time*>,408 | INFO - WatchdogContainerApplication.performUcfServiceOperations(193) | RSASAIMDC service The service has not been started. <*Date*><*Time*>,408 | INFO - WatchdogContainerApplication.performUcfServiceOperations(193) | RSASAIMDC service <*Date*><*Time*>,408 | INFO - WatchdogContainerApplication.doServiceWaitRestart(143) | Waiting 40 seconds to stop the RSASAIMDC service... <*Date*><*Time*>,424 | INFO - WatchdogContainerApplication.performUcfServiceOperations(182) | Attempting to start RSASAIMDC service.

RSA SecOps Watchdog Service Counters

The parameters are configured in the collector.config.properties file.

Name	Description
TOTAL_NUM_OF_ MESSAGES_IN_ INCIDENT_QUEUE	Number of messages present in the RabbitMQ "im.archer_ incident_queue" queue every hour.
NUM_MESSAGES_ FROM_QUEUE	Number of events read from the RabbitMQ queue every hour.
NUM_MESSAGES_ FROM_SYSLOG	Number of messages read from Syslog every hour. **Note:** For SA ESA, events are counted with messages. For other SIEM integrations, the alerts are counted with the messages.
NUM_MESSAGES_UCF_ TO_ARCHER	Number of records created or updated in RSA Archer GRC every hour.
TOTAL_NUM_ MESSAGES_FROM_ QUEUE	Number of events read from the RabbitMQ queue in the last *N* hours.
TOTAL_NUM_ MESSAGES_FROM_ SYSLOG	Number of messages read from Syslog in the last *N* hours.
TOTAL_NUM_ MESSAGES_UCF_TO_ ARCHER	Number of records created or updated in RSA Archer GRC in the last *N* hours.

Note: The default for *N* is 24 hours. Two parameters, watchdog.configuredCronTime and watchdog.hoursConfiguredForTotalCounter, establish how often the monitor runs in a specific period of time. Watchdog.configuredCronTime, a spring quartz cron expression, sets the interval of monitoring. Watchdog.hoursConfiguredForTotalCounter sets the period of time (last *N* hours) during which the watchdog counters are maintained.

By default, these properties are set to the following:

watchdog.configuredCronTime = 0 0 0/24 * * *

watchdog.hoursConfiguredForTotalCounter = 24

The monitor runs every day at 12AM maintaining watchdog counters for the last 24 hours.

Important: If the interval is updated to every few seconds in the saim-beans.xml file, some counters might not be recorded properly. To record every few seconds, modify the startup properties of the WMI Performance Adapter service to Automatic and start the service.

Important: The performance counters are reset when the RSA Unified Collector Framework is restarted.

Watchdog Configured Cron Time

The watchdog.configuredCronTime property is the spring quartz cron timing that is used to determine how often the RSA SecOps Watchdog Service reads all of the performance counters from the Windows Performance Monitoring Tool and perform any restart action based on them. By default, the cron time is set to: 0 0 0/24 * * * which means it runs every day at midnight.

Watchdog Hours Configured For Total Counter

The watchdog.hoursConfiguredForTotalCounter property dictates how many hours of counters are kept in memory. By default, it is set to 24. The total counters keep track of the last 24 hours of data since the UCF was started.

Add the Watchdog Service to the Performance Monitor

You can view information about each performance counter through the Performance Monitor.

Procedure

1. Click Start > Performance Monitor > Monitoring Tools > Performance Monitor.
2. Click the Add (+).
3. Select the counters from RSA_SECOPS.

   Note: The RSA_SECOPS counters are updated by the RSA Unified Collector Framework after an hour of service startup.

4. Click Add.
5. Click OK.

Start the RSA SecOps Watchdog Service

Procedure

1. Click Control Panel > Administrative Tools > Services.
2. Select RSA SecOps Watchdog.
3. Click Start.

Stop the RSA SecOps Watchdog Service

Procedure

1. Click Control Panel > Administrative Tools > Services.
2. Select RSA SecOps Watchdog.
3. Click Stop.

Appendix E: Troubleshooting

This appendix provides resolutions to common problems that you may encounter while configuring the solution.

Component Troubleshooting 90
Security Analytics Incident Management Integration Troubleshooting 99
Enterprise Management Plug-In Setup Troubleshooting 104
Package Installation Log Message Examples 108

Component Troubleshooting

Configuration

Problem	Resolution
Default log files do not provide RSA Archer Webservice API calls.	Open <*install_dir*>\SA IM integration serviceconfig\collector-log4j.xml, and change the log level for CXF to warn from info: <logger name="org.apache.cxf"> <level value="info" /> </logger>

Enterprise Management Plug-In

Problem	Resolution
The feed cannot be accessed in the SA host for Enterprise Management when automatically configured with SSL.	1. Verify that the host entry for the UCF host is present in SA hosts file (/etc/hosts). 2. Restart SA server by running the following command: `restart jettysrv` 3. If you still cannot access the feed URL, reboot the SA host.

RabbitMQ

Problem	Resolution
When the RabbitMQ connectivity is lost, an error in the collector log occurs that begins similarly to the following: <*Date*> <*Time*>| WARN - SimpleMessageListenerContainer$AsyncMessageProcessing Consumer.logConsumerException(1208) | Consumer raised exception, processing can restart if the connection factory supports it com.rabbitmq.client.ShutdownSignalException: connection error; protocol method:.	Check the status of RabbitMQ on the SA server.

RSA Archer GRC Platform

Problem	Resolution
Password for an RSA Archer WebServices user account is about to expire.	To change the password for the RSA Archer WebServices user account, do the following: 1. Click Administration > Access Control > Manage Users. 2. Select the WebServices user account. 3. In the Account Maintenance section, click Change Password. 4. Enter a new password, confirm the password, and click OK. 5. Click Save. 6. Change the password for the Push and Pull user in Connection Manager. 7. Change the password for the Datafeed jobs through the data feed settings.
During the package import process, the following warning message may appear: Field {0} was not found and removed from a collection.	These errors are benign and can be ignored.

Problem	Resolution
The Incident Status dashboard still appears in your workspace after upgrading from RSA Advanced Incident Management for Security 1.1. This dashboard is not required for RSA Security Operations Management.	Remove the dashboard from your workspace, as follows: 1. Click Administrations > Workspaces and Dashboards > Manage Workspaces. 2. Open the Security Operations Management workspace. 3. Click the Dashboards tab. 4. For the Incident Status dashboard, click Remove in the Actions column. 5. Click Save.
In the collector.log file, an error occurs when a corresponding field from SIEM sources is required, but not populated. Example: <*Date*> <*Time*> | ERROR - SyslogIncidentAddedTasklet.execute(127) | Message cannot be executed, exception while pushing the message com.rsa.connector.framework.components.datastore.archer.exception.ArcherComunicationException: javax.xml.ws.soap.SOAPFaultException: Server was unable to process request. ---> The Title field is a required field. The Title field is mapped to the Alert field in secops_import_archer.xml. The alert name is required in the incoming message. If the alert name is empty, the UCF cannot process it as it is a required field in RSA Archer GRC, so the errors are thrown in the collector.log file.	Verify the SIEM configurations to ensure the corresponding field is populated when messages are received.

RSA Archer Endpoints

Problem	Resolution
Adding an RSA Archer endpoint in the Connection Manager fails.	In the <*install_dir*>\SA IM integration service\logs\connectionManager.log file, verify the following: • RSA Archer GRC is in SSL Mode. • The Common Name present in the RSA Archer SSL Certificate matches the host name of the RSA Archer web server and is resolvable by the UCF machine. • The password for the user is valid. • User account is not locked. • Password is not expired.
When adding RSA Archer endpoints, the connection appears to work but the endpoint fails to add and the following error message appears: Failed to connect to endpoint In connectionmanager.log, the following error appears: ERROR - SAIMArcherEndpoint.testEndpointConnection (103) | Failed to test the Archer Endpoint connection java.lang.StringIndexOutOfBoundsException: String index out of range: -37"	Verify the base URL for the RSA Archer web server. **Note:** Not all RSA Archer installs are configured to use /RSAarcher. If using SaaS or if RSA Archer is installed directly to wwwroot, retry adding the endpoint without /RSAarcher in the URL. Enter https://hostname:port for the URL.

RSA Archer Security Operations Management

Problem	Resolution
In RSA Archer Security Operations Management, the Raw Alert field is truncated.	1. Check SIEM tool forwarding parameters for payload size option. **Note:** Some SIEM tools automatically limit long alert messages when forwarding. 2. Verify that the message received in the collector log is identical to the alert contained in the RSA Archer Security Operations Management Raw Alert field. If the data matches, then the SIEM tool is truncating the message before forwarding it.

RSA Archer SecOps Watchdog Service

Problem	Resolution
The UCF or RSA SecOps Watchdog services do not run.	Verify that the user has the following permissions: • Full permissions for both UCF and RSA SecOps Watchdog installation directories and all child items. • Logon As Service Right • Administrator privileges to the local machine. Counters are stored on the local machine in the HKLM\Software\RSA\PerfCounters registry.

RSA Unified Collector Framework

Problem	Resolution
After installing the RSA Unified Collector Framework, the service does not start automatically.	Open the <*install_dir*>\SA IM integration service\logs\collector.log file and check for errors.
RSA Unified Collector Service cannot be started and the following errors are seen in the collector.log: • <*Date*> <*Time*> | ERROR - CollectorApplication.initializeCollector(158) | Unlimited strength Java JCE extension files are not detected. • <*Date*> <*Time*> | ERROR - CollectorApplication.initializeCollector(159) | Shutting down the Service . Please install Unlimited strength Java JCE extension files 8 and start the service.	1. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for JDK/JRE 8 from **http://www.oracle.com/technetwork/java/javase/downloads/index.html** 2. Extract the downloaded zip file. 3. Move the extracted US_export_policy.jar and local_policy.jar files to the following JRE install directory: *JRE_install_dir*/lib/security (Overwrite the existing files) 4. **Start the RSA Unified Collector Framework**.
After upgrading to a JRE version other than JRE 1.8, the service does not start.	1. Go to <C:\Program Files\EMC\RSA\SA IM integration service\. 2. Run RSASAIMDC as administrator. 3. On the Java tab, select Default or enter the location of JRE 1.8.

Splunk

Problem	Resolution
After upgrading the Splunk mapping file migration, the new RSA Archer Security Operations Management 1.3 templates do not work. The following error message is displayed in the collector.log while pushing the message: <*Date*> <*Time*>,350 | ERROR - ArcherDataStore.createArcherRecordField(974) | Error creating cross referenced record application Splunk_Security Alerts java.lang.NullPointerException	This issue occurs because new templates do not work with the migrated mapping file. You would need to either use the existing templates from RCF (SecOps 1.1) OR perform the following workaround: • Post migration, in Secops_import_archer.xml - look for the application "Splunk_Security Alerts" • Find the "Alert Timestamp" field, which looks like this: <field name="Alert Timestamp"><UUID>71F462F2-CAB7-43BE-B83B-B71BCE9B972F</UUID> <fieldType>TEXT</fieldType> <keyName>rt</keyName> </field> • Modify the Alert Timestamp field as below: <field name="Alert Timestamp"><UUID>71F462F2-CAB7-43BE-B83B-B71BCE9B972F</UUID> <fieldType>DATE</fieldType> <keyName>rt</keyName> <dateFormat>epochInSecs</dateFormat> </field> • Save the file and restart the service.

Syslog

Problem	Resolution
When Syslog is configured in SSL mode and a SIEM tool is configured to forward messages, but the SSL certificates were not added to the SIEM host, an error occurs that begins similarly to the following: <*Date*> <*Time*>| ERROR - TcpNioConnection.readPacket(489) | Exception on Read <*IP Address*> Unrecognized SSL message, plaintext connection?.	To add the certificates to the UCF trust store, do the following: 1. Download the certificate from the SIEM tool and copy it to a location on the UCF. 2. Open a command prompt. 3. Type: runConnectionManager.bat 4. Enter the number for Install Certs from Directory. 5. Enter the directory location of where the certificates are stored. 6. Restart UCF server. 7. Attempt to send the alerts from the SIEM tool.
When SA RE is configured in secure TCP mode, the following exception occurs in the logs: <*Date*> <*Time*>| ERROR - TcpNioConnection.readPacket(489) | Exception on Read <*IP Address*> An established connection was aborted by the software in your host machine java.io.IOException: An established connection was aborted by the software in your host machine	Alerts are not lost.

Security Analytics Incident Management Integration Troubleshooting

Problem	Resolution
After adding the endpoint for SA IM, the CA truststore fails to set.	1. Ensure that the SSH credentials for the SA host are valid. 2. Ensure that port 22 is open. 3. If the credentials are correct, but the error still occurs, **Manually Copy Certificates**.

Problem	Resolution

Findings and Security Incidents do not appear in RSA Archer Security Operations Management solution.	1. Confirm that the time on your middleware system and the RSA Archer Platform are synchronized or with a difference of no more than one second.
	2. Verify that the endpoint is configured correctly.
	3. Confirm that the UCF is set to the appropriate mode.
	• For Findings, you should select to manage the incident workflow in RSA Security Analytics.
	• For Security Incidents, you should select to manage the incident workflow in RSA Archer Security Operations Management.
	4. SSH to the SA web server host and enter the following commend to verify that the RSA Archer incident queue (im.archer_incident_queue) is created:
	`curl -k -u guest:guest https://127.0.0.1:15671/api/queues/%2Frsa%2Fim%2Fintegration/im.archer_incident_queue --silent --stderr - | grep -o '"name"\:.*`
	Note: If the queue is created, the output reads as follows:
	`"name":"im.archer_incident_queue","vhost":"/rsa/im/integration","durable":true,"auto_delete":false,"arguments":{},"node":"sa@localhost"}`
	5. SSH to the SA web server host and enter the following command to verify that the RSA Archer tickets queue (im.archer_tickets_queue) is created:
	`curl -k -u guest:guest https://127.0.0.1:15671/api/queues/%2Frsa%2Fim%2Fintegration/im.archer_tickets_queue --silent --stderr - | grep -o '"name"\:.*'`
	Note: If the queue is created, the output reads as follows:
	`"name":"im.archer_tickets_queue","vhost":"/rsa/im/integration","durable":true,"auto_delete":false,"arguments":{},"node":"sa@localhost"}`
	6. SSH to the SA web server host and enter the following command to check the number of messages in the incident queue:
	`curl -k -u guest:guest https://127.0.0.1:15671/api/queues/%2Frsa%2Fim%2Fintegration/im.archer_incident_queue --silent --stderr - | grep -o '"messages"\:[0-9]*'`
	Note: If the queue is created, the output reads as follows: `"messages":5`
	7. Confirm the above queues are populated with messages from the UCF.

Problem	Resolution
Remediation Tasks being pushed to the Operations queue through the UCF are not appearing in RSA Archer Security Operations Management as Findings.	1. Open the Connection Manager: a. Open a command prompt b. Change directories to <*install_dir*>\SA IM integration service\data-collector. c. Type: runConnectionManager.bat 2. Enter 2 for Edit Endpoint. 3. Enter 3 for Security Analytics IM. 4. Ensure the Target Queue is set to All or Operations.
In the <*install_dir*>\SA IM integration service\logs\collector.log, there are SSL errors between RSA Security Analytics and RSA Unified Collector Framework.	1. Verify that the SSL certificates are valid. **Note:** Certificates expire after two years. 2. If your certificates are expired, regenerate and copy the expired certificates. See **Regenerate Expired SA IM Certificates**.
In the <*install_dir*>\SA IM integration servicelogs\collector.log, there are a series of connection timeout/reset issues.	This is a known issue when using an operating system less than Window Service 2008 R2 DataCenter. Please wait 4 to 5 minutes after the service starts for the SA IM Integration Service to establish a connection. This error can occur if the computer is not connected to the Internet. If you still encounter errors, turn off the local security policy that attempts to validate certificates from the Microsoft online certificate store.
In RSA Archer Security Operations Management, there are more events per alert or alerts per incident displayed than desired.	By default, RSA Archer GRC will send and receive all events and alerts. To adjust your settings, **Set the Maximum Number of Alerts or Events Sent Through the SA IM Integration Service**.

Problem	Resolution
RSA Archer GRC is pulling data from SA IM at an undesirable rate. The default interval between incident updates is 1 minute. The default interval between findings updates is 5 minutes.	1. **Stop the RSA Unified Collector Framework**. 2. Open the <*install_dir*>\SA IM integration service\config\collector-config.properties file, and edit the applicable property. • To update the interval for incident updates, change the cron expression of archer.*pull*.getIncidents.schedule. • To update the interval for findings updates, change the cron expression of archer.*pull*.getFindings.schedule. Where: *pull* is the endpoint name for the account used to pull data from RSA Archer GRC. 3. **Start the RSA Unified Collector Framework**. For more information on spring cron expressions, see the Spring Quartz Job Scheduler tutorial on the CronTrigger website.
Adding an SA IM Endpoint in the Connection Manager fails.	Retry adding the endpoint.

Problem	Resolution
In SA IM 10.5, output suppression only prevents ESA alert notifications from appearing while the alerts themselves are still created. This can cause performance issues for the UCF and RSA Archer GRC.	Convert each ESA alert that had suppression applied to an Advanced Alert. 1. Modify the EPL statement in the new alert, as follows: a. Add window(*) to the beginning of the SELECT statement. SELECT **window(*)** FROM b. Add OUTPUT every 60 minutes to the end of the SELECT statement. GROUP BY ip_src HAVING COUNT(*) = 10 **OUTPUT every 60 minutes;** 2. Remove the old alert from ESA sync. 3. Add the new alert to ESA sync. Example: Original syntax: /* Description: Multiple failed login attempts from the same source have been detected within the specified time window. The count of failed login attempts and the time window is configurable. Version: 2 */ module Module_e2e7bb7f_9445_4d71_8d34_67c89a52e8fc; @Name('Module_e2e7bb7f_9445_4d71_8d34_67c89a52e8fc_Alert') @RSAAlert(oneInSeconds=0, identifiers={"ip_src"}) SELECT * FROM Event(medium = 32 AND ec_activity = 'Logon' AND ec_theme = 'Authentication' AND ec_outcome = 'Failure' AND ip_src IS NOT NULL).std:groupwin(ip_src).win:time_length_batch(60 seconds, 10) GROUP BY ip_src HAVING COUNT(*) = 10; Syntax after adding the change (bolded) to suppress the alert for 1 hour: /* Description: Multiple failed login attempts from the same source have been detected

Problem	Resolution
	within the specified time window. The count of failed login attempts and the time window is configurable. Version: 2 */ module Module_e2e7bb7f_9445_4d71_8d34_67c89a52e8fc; @Name('Module_e2e7bb7f_9445_4d71_8d34_67c89a52e8fc_Alert') @RSAAlert(oneInSeconds=0, identifiers={"ip_src"}) SELECT **window(*)** FROM Event(medium = 32 AND ec_activity = 'Logon' AND ec_theme = 'Authentication' AND ec_outcome = 'Failure' AND ip_src IS NOT NULL).std:groupwin(ip_src).win:time_length_batch(60 seconds, 10) GROUP BY ip_src HAVING COUNT(*) = 10 **OUTPUT first every 60 minutes;** This example suppresses notifications for the same repeated ip_src field for 60 minutes after the first one fires. If a new or different ip_src fires the alert again within the same 60 minute window, it will not be suppressed. This avoids suppressing a different potential threat source during that window. For more information on EPL Language, see **http://espertech.com/esper/release-5.3.0/esper-reference/html_single/index.html#enumeration-method-anyof**.

Enterprise Management Plug-In Setup Troubleshooting

If you finish configuring the Enterprise Management plug-in, but RSA Archer asset criticality information is not showing up in RSA Security Analytics, use the following table to help identify the source of the issue and resolve the problem. The left-hand column lists specific items to check, the middle column tells you how to determine if this item is your issue, and the right-hand column gives potential resolutions for each issue. If any of the resolutions do not solve the problem, contact RSA Customer Support.

Checklist Item	How to Determine	Resolution
Is your RSA Archer Devices application populated with device and criticality information?	1. On the RSA Archer GRC Platform, expand the Enterprise Management solution in the Navigation Menu. 2. Expand the Devices application, and click Display All. 3. Open a device record and note whether the Criticality Rating field is populated.	Contact RSA Professional Services for assistance.
Is the asset criticality .csv feed file located in the file you specified?	On your UCF system, open the folder that you specified for the feed file location and note whether the feed file is present.	Review the following items.
• Is your RSA Archer GRC system reachable from your UCF?	Log on to your UCF system, and do the following: 1. Open a command prompt and ping your RSA Archer system. 2. Open a web browser and log on to your RSA Archer system using your WebServices user account.	If you are not successful at step 1, contact your network administrator. If the RSA Archer GRC Platform logon page does not render in step 2, reset Internet Information Services (IIS) on the RSA Archer web server, as follows: 1. Log on to the Windows system hosting the RSA Archer GRC Platform. 2. Open a command prompt. Type: iisreset
• Does the WebServices user account created for the UCF have the correct credentials and access rights?	Log on to the system on which you installed the UCF, open a web browser and log on to your RSA Archer GRC system using your WebServices user account.	Do the following: • Review the logon credentials and access rights for your WebServices user account. • Verify that the user credentials selected in the RSA Archer GRC system match what you entered in the UCF.
Is the UCF configured properly?		
• Is the UCF running?	Click Start > Administrative Tools > Services, and see if the UCF is running.	Start the UCF. See **Start the RSA Unified Collector Framework**.

Checklist Item	How to Determine	Resolution
• Are the endpoint.properties details entered properly?	Open the collector-config.properties file in the C:\Program Files\RSA\SA IM integration service\config folder.	If you need to make any changes, follow the instructions for changing the configuration of an application in the Running state in **Component Troubleshooting**.
• Are the plugin.properties details entered properly?	Open the collector-config.properties file in the C:\Program Files\RSA\SA IM integration service\config folder.	If you need to make any changes, follow the instructions for changing the configuration of an application in the Running state in **Component Troubleshooting**.
• Do the log files indicate errors or exceptions?	Open C:\Program Files\RSA\SA IM integration service\logs\collector.logs to view the logs.	Contact Customer Support.
Did the recurring task run correctly?	1. In the Security Analytics menu, click Live > Feeds. 2. Note the task you created, when it last ran, and what the last run result was.	Review the following items.
• Is your RSA Security Analytics system reachable from your UCF system?	Log on to your UCF system, open a command prompt, and ping your RSA Security Analytics system.	Try to log on to your RSA Security Analytics system. If you are not successful, contact your administrator.
• Does the UCF user account created for Security Analytics to use have the right credentials?	Review the logon credentials and access rights that you entered for Security Analytics to access the UCF in **Create a Recurring Feed Task**.	• Enter the correct credentials in the recurring feed task, save the task, and restart any Decoders to which the feed is pushed.
Does the new meta data category appear in the Investigation Module?	In the Security Analytics menu, click Investigation > Navigate, and select a device to investigate, and see whether the Criticality report is visible. **Note:** If you do not see the report, check to see if the report contains any results for the active query. The list of reports that contain no results is at the bottom of the collection screen.	Do the following: • Review **Create Criticality Category**. **Note:** Double check that you have restarted the Concentrator after editing the index file.

Checklist Item	How to Determine	Resolution
Does the Criticality report contain results?	In the Investigation Module, locate the Criticality report and see if it lists report values and associated session counts.	Do the following: • Verify that the name attribute of the key that you entered in the index-concentrator-custom.xml file matches the name of the key value you entered in **Create a Recurring Feed Task**.

Package Installation Log Message Examples

For more information on the Package Installation Log messages, see "Package Installation Log Messages" in the RSA Archer Online Documentation.

For information on the dependencies for each solution, see the *Data Dictionary*.

Warning Message	Explanation	Remediation
<Object Name> Alias was changed from <Original Alias> to <New Alias>	This message is an informational warning indicating that the Alias was updated on the object. There are two reasons for an alias in the Target Instance to have been updated: • Update was in the Source Package. • Alias has to be unique in the Target Instance. If the alias already exists in Target, packaging adds a unique identifier to the end.	This message is only potentially an issue if the change occurs on a field that is utilized in a Mail Merge Template or Data Publication Service. In that scenario, update the DPS or the mail merge template with the new alias.
<Field Name> in the application <Application Name> cannot be changed from a private field to a public field.	This message is an informational warning notifying you that packaging does not change a private field in the target instance to a public field.	Change the field to public manually (optional).
Field <Field Name> could not be saved due to inability to identify the related module.	This message is seen when a cross-reference or related record field could not be created because the related application does not exist in the target instance. This message usually occurs because the field is part of a related core solution that has not been updated in the target instance.	1. Install the package for the solution containing the related application. You must have a license for the related application. 2. Reapply the original package to resolve the warning. See the *Data Dictionary*.

Warning Message	Explanation	Remediation
The calculated field <Field Name> in the application <Application Name> cannot be verified.	The formula in the calculated field is incorrect. Most often, this message occurs when the formula references a field in a related application and either the field or the application does not exist in the target instance. This may be because the application is in a related core solution that has not been updated.	1. Install the package for the solution containing the related application. You must have a license for the related application. 2. Reapply the original package to resolve the warning. See the *Data Dictionary*.
Field <Field Name> was not found and removed from a collection.	This warning may be seen on Inherited Record Permission fields, cross-reference/related record fields (record lookup and grid display), or as a display field in a report. The warning means that the field could not be found in the target instance and was not included in the package. This is usually because the field is part of an application in a related core solution that has not been updated in the target instance.	1. Install the package for the solution containing the related application (to obtain the missing field). You must have a license for the related application. 2. Reapply the original package to resolve the warning. See the *Data Dictionary*. **Note:** If you do not have a license for the related application, you may ignore this message, and the field remains omitted from the object.