SIEMENS

Insights Hub Private Operations

Documentation

A. General

1. **Updates.** We may make updates to this Documentation to improve the operations activities. The then-current Documentation will apply to the provisions of the operations activities to you.

2. **Remote Services.** All services shall be provided remotely in English language.

3. **Your Responsibilities.** This section outlines your responsibilities which are in addition to those responsibilities outlined in the Agreement which governs this Documentation.

   a. General

      i. You will provide us with all the information regarding your business, equipment, work procedures and plans which are required by us to render the deliverables and will ensure that any information provided is accurate and complete.

      ii. You coordinate monthly meetings with us and other relevant stakeholders for deployment alignment and planning.

      iii. Your operating environment meets all the prerequisites as described in Section D of this Documentation so that we may carry out the activities described in this Documentation. The availability of a qualified infrastructure is a critical success factor for the timely execution of the activities with the expected level of quality.

      iv. You shall provide Insights Hub Private Cloud Software subscription as needed for your purposes.

      v. You shall be solely responsible to contract for telecommunications facilities (data communications circuit, wiring, etc.), and for the costs associated with such facilities.

      vi. You shall be responsible for implementing and maintaining your information security controls for internet service provisioning according to ISO27001 or equivalent.

      vii. You shall adequately plan your infrastructure to accommodate number of Users to access your Insights Hub Private instance.

   b. Insights Hub Cloud Dedicated (VPC)

      i. You shall provide the Infrastructure as a Service ("IaaS") subscriptions as described in Section D of this Documentation.

      ii. We receive all administrative permissions (here: administrator privileges) to the IaaS subscriptions provided by you.

      iii. You coordinate between us, the IaaS supplier and other relevant third parties to provide all required information to us in a consolidated form.

   c. Insights Hub for Private Cloud (LPC)

      i. You shall provide third party and open source software and respective licenses, and operate your operating environment as laid out in Section D of this Documentation.

      ii. You coordinate between us and relevant third parties to provide all required information to us in a consolidated form.

      iii. You will be responsible for the infrastructure and network maintenance.

4. **Out-of-Scope Responsibilities for Us.** The following, non-exhaustive list shows examples of activities that are not in scope of the Insights Hub Private Operations.

SIEMENS

    a.   Any data upload services or tools to migrate or clean legacy or supplier/partner data into or out of your Insights Hub instance. You are responsible for data migration.

    b.   All activities, which are not explicitly mentioned in this Documentation, e.g. training, data backup and recovery procedures, certificates, Review of your information security controls.

    c.   Third party applications on your Insights Hub instance.

    d.   Reviewing your information security controls.

5. **Your Project Manager.** You will provide a project manager to act as your representative to us. This project manager will be responsible to:

    a.   Provide required information relevant to accomplishing the work activities quickly and accurately.

    b.   Provide your organizational linkages with your appropriate people & teams.

    c.   Ensure availability of key business subject matter experts on a best-effort basis during designated meetings, with the proper level of decision-making.

    d.   Provide your input, assistance, participation, and cooperation with our activities and requests required by the in-scope activities tasks of this Documentation.

    e.   Provide to us all your management decisions and responses, information, data, equipment, approvals if any in a timely manner.

    f.   Provide your business processes to us.

B. Initial Deployment

1. **Kick-off.** For the detailed planning of the deployment preparation, we shall prepare, perform, and document a remote kick-off meeting with you.

2. **Readiness of Operating Environment.** We shall verify if you are meeting all Insights Hub private install and system management prerequisites as described in Section D of this Documentation for your operating environment, such as e.g., proper sizing of the systems, system access, or installed software versions. We shall prescribe required system updates to be implemented by you as necessary. We shall confirm when your operating environment meets all Insights Hub install and system management prerequisites and declare its readiness for the initial deployment of the Insights Hub Private Software. Implementation of system updates necessary to fulfill the prerequisites for the readiness of the operating environment are not executed by us.

3. **Initial Deployment.** We shall align with you on a timeline for performance of the initial deployment. Provided that the operating environment is ready, we shall deploy the Insights Hub Private Software on your operating environment per remote installation according to the agreed timeline.

4. **Completion of Deployment and Access Credentials.** Upon completion of the initial deployment of the Insights Hub Private Cloud Software on your operating environment, we shall announce the completion to you and provide you with the access credentials to your Account.

C. Insights Hub Private Operations

1. **Content of Insights Hub Private Operations.** We shall operate the Insights Hub Private Cloud Software as described in this section, hosted on an operating environment provided by you and dependent on the fulfillment of further obligations by you, and thus make the Insights Hub instance available to you. Management of your operating environment is not included in the Insights Hub Private Operations.

2. **Insights Hub Cloud Dedicated.** With regards to Insights Hub, the operations consist of the following actions:

    a.   Environment Access

Action	Customer	Siemens

Lifecycle management of user access to IaaS accounts	Yes	
Lifecycle management of technical access to IaaS accounts	Yes	Yes

To perform operational duties, access to the IaaS accounts shall be managed by you and continuously ensured for us.

Technical access to the **IaaS** API is granted by you by ensuring a trust relationship with a Siemens managed vault instance.

Network access to your Insights Hub instance is coordinated between you and us.

All of the accesses above must be available for our operational support.

b.   Deployments

Action	Customer	Siemens
Coordination of deployment windows	Yes	Yes
Deployment of Insights Hub Private Cloud Software component updates/patches and configuration of required IaaS services		Yes

You shall define a responsible contact person to coordinate deployments of Insights Hub Private Cloud Software components. Time slots for deployments should be set in regularly scheduled meetings.

c.   Monitoring

Action	Customer	Siemens
Health of Insights Hub Private Cloud Software components installed in your infrastructure (e.g. IaaS accounts) by us		Yes

We continuously monitor the health of installed Insights Hub Private Cloud Software components. To this purpose health metrics will be exported into our central monitoring service.

d.   Configuration

Action	Customer	Siemens
Environment for your Insights Hub instance configuration coordination	Yes	Yes
Changes to configuration of environment for your Insights Hub instance		Yes

Both parties shall coordinate a suitable environment configuration. This should be reviewed by both parties on a regular basis and adjusted to demands (e.g., for scaling).

Any changes to the environment configuration of your Insights Hub instance shall be implemented by us.

e.   Incident Management

Action	Customer	Siemens
Automatic detection of predefined Insights Hub Private Cloud Software system alerts		Yes
Manual reporting of incidents via Support Center	Yes	
Response to automatically/manually reported outages (24/7)		Yes
Incident documentation		Yes
Emergency deployment decisions		Yes
Root cause analysis on outages	Yes	Yes
Receival and forwarding of incidents reported by your IaaS supplier	Yes	

We will leverage continuous health monitoring to automatically detect Insights Hub Private Cloud Software system alerts indicating non availabilities. Incidents reported in this manner or manually by you via the Support Center will be responded to by us and we will directly access your Insights Hub instance to stabilize the system.

To be able to respond in time, we shall be able to unilaterally decide to deploy changes for the purpose of incident remedy.

For the purpose of minimizing outage occurrences, each instance shall result in us performing and documenting the root cause. You shall support this effort.

Incidents reported by your IaaS supplier shall be forwarded to us by you for further processing.

3. Insights Hub for Private Cloud. With regards to your instance, the operations consist of the following actions:

a. Environment Access

Action	CUSTOMER	Siemens
Admin access to infrastructure accounts	Yes	Yes
Admin access to your environment	Yes	Yes

Network access to your environment is coordinated between you and us.

All of the accesses above must be available for our operational support.

b. Deployments

Action	Customer	Siemens
Coordination of deployment windows	Yes	Yes
Deployment of Insights Hub Private Cloud Software component updates/patches and configuration of required operating environment		Yes

You shall define a responsible contact person to coordinate deployments of Insights Hub Private Cloud Software components. Time slots for deployments should be set in regularly scheduled meetings.

c. Monitoring

Action	Customer	Siemens
Health of Insights Hub Private Cloud Software components installed in your operating environment by us		Yes

We continuously monitor the health of installed Insights Hub Private Cloud Software components. To this purpose health metrics will be exported into our central monitoring service.

d. Configuration

Action	Customer	Siemens
Environment for your Insights Hub instance configuration coordination	Yes	Yes
Changes to configuration of environment for your Insights Hub instance		Yes

Both Parties shall coordinate a suitable environment configuration. This should be reviewed by both parties on a regular basis and adjusted to demands (e.g., for scaling).

Any changes to the environment configuration of your Insights Hub instance shall be implemented by us.

e. Incident Management

Action	Customer	Siemens
Automatic detection of predefined Insights Hub Private Cloud Software system alerts		Yes
Manual reporting of incidents via Support Center	Yes	
Response to automatically/manually reported outages (24/7)		Yes
Incident documentation		Yes
Emergency deployment decisions		Yes
Root cause analysis on outages	Yes	Yes

We will leverage continuous health monitoring to automatically detect Insights Hub Private Cloud Software system alerts indicating non availabilities. Incidents reported in this manner or manually by you via the Support Center will be responded to by us and we will directly access your instance to stabilize the system.

To be able to respond in time, we shall be able to unilaterally decide to deploy changes for the purpose of incident remedy.

For the purpose of minimizing outage occurrences, each instance shall result in us performing and documenting the root cause. You shall support this effort.

D. Operating Environment Prerequisites

1. **Insights Hub Cloud Dedicated.** The following prerequisites apply to you when using IaaS from AWS or Microsoft Azure as your operating environment.

Requirements	Details
Subscriptions	12 IaaS subscriptions: 9 product lines, 1 global infrastructure, 1 Logging & Monitoring, 1 for Malware Protection.
Backing Services	Part of your IaaS subscription.
DNS	mindsphere.<customerdomain> with zone delegation. This domain should be added / configured to your DNS Server.
SSL	Based on SAN. You will provide ssl certificates to us for the installation.
ADFS	Your IDP information should be provided to us for the integration so that we will be able to access your environment.
SMTP Server	You should provide the SMTP server details to integrate with Insights Hub notification services for email notifications.

2. **Insights Hub for Private Cloud.** The following prerequisites apply to you when using an operating environment other than IaaS.

    a. General Prerequisites on your operating environment

Requirements	Details
ADFS	Your IDP information should be provided to us for the integration so that we will be able to access your environment.
Backing Services	All backing services should be deployed by you with Insights Hub specified configurations and namespace and ready for the Insights Hub Private Cloud Software installation. Please see the Backing Services section below for details.
Deployment Environment	Availability of operating environment according to Insights Hub specific configuration, with following specifications: • Admin access will be provided to us. • Ingress setup is complete with wildcard and ingress logs are enabled.

Requirements	Details
DNS	*.mindsphere.<customerdomain>, *.piam.mindsphere.<customerdomain>, *.uiam.mindsphere.<customerdomain>, *.apps.<cluster-name>.<customerdomain>, api.<cluster name>.<customerdomain>: These domains need to be added to your DNS server.
Monitoring Agents	• Monitoring agent provided by you is available in Insights Hub specified monitoring namespace. • Alerting channel (PagerDuty, Slack, Teams, Webhook, Mail, etc.) needs to be provided by you for the incident alert.
SMTP Server	You should provide the SMTP server details to integrate with Insights Hub Notification services for email notifications.
SSL (for external communication)	• *.mindsphere.<customerdomain>, *.piam.mindsphere.<customerdomain>, *.uiam.mindsphere.<customerdomain>: the certificate is needed for your Insights Hub Private instance. • *.apps.<cluster name>.<customerdomain>, api.<cluster name>.<customerdomain>: the certificate is needed for your operating environment.
Static virtual IP	Two static IP associated with below DNS entries need to be configured to your DNS server. • IP1 - *.apps.<cluster name>.<customerdomain> • IP2 - api.<cluster name>.<customerdomain>

b. Deployment Environment

  i. OpenShift/Rancher: The compatible versions for the deployment environment are listed at https://documentation.mindsphere.io/resources/private-cloud/Backing-Services.pdf.

  ii. Hardware Requirements: to be aligned project specifically between you and us.

c. Backing Services
The compatible versions for the operating environment are listed at
https://documentation.mindsphere.io/resources/private-cloud/Backing-Services.pdf.