

Cisco Secure Equipment Access Quick Start Guide for IE switches

First Published: 2024-06-12

Last Modified: 2025-09-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Purpose of the Guide** 1

Purpose of the Guide 1

CHAPTER 2 **Secure Equipment Access Overview** 3

Cisco Secure Equipment Access service 3

Prerequisites for enabling SEA 3

Enabling the SEA service 4

CHAPTER 3 **Manage access control groups for remote access** 5

Access control groups 5

How remote session access requests work 5

Create an access control group for remote access 6

Add users to an access control group 7

Add asset access to an access group 7

Assign approvers to an access control group 8

Create access control groups for scheduled access 8

Schedule statuses 10

Invite group members to a scheduled meeting 10

Modify a remote session 11

CHAPTER 4 **Deploy SEA Agents Using CLI commands** 13

Deploy SEA agent on IE switches using CLI commands 13

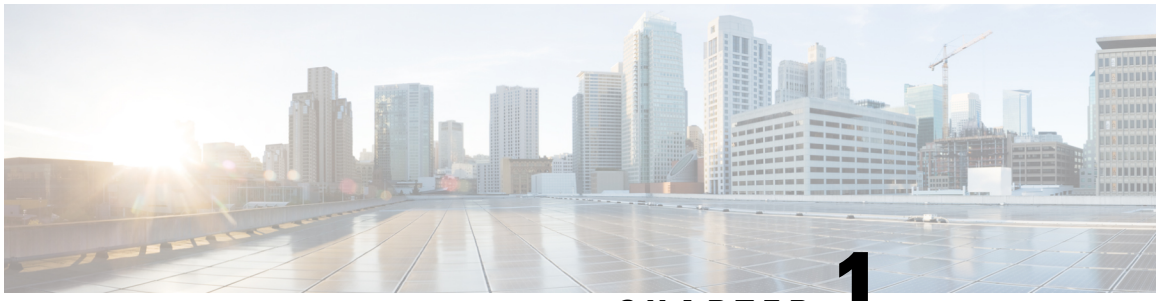
Deploy the SEA agent using CLI commands 13

Edit configuration details for onboarded IE switches 15

SEA Agent connectivity modes 15

CHAPTER 5 **Remote Sessions Configurations** 17

Configure remote sessions 17



CHAPTER 1

Purpose of the Guide

- Purpose of the Guide, on page 1

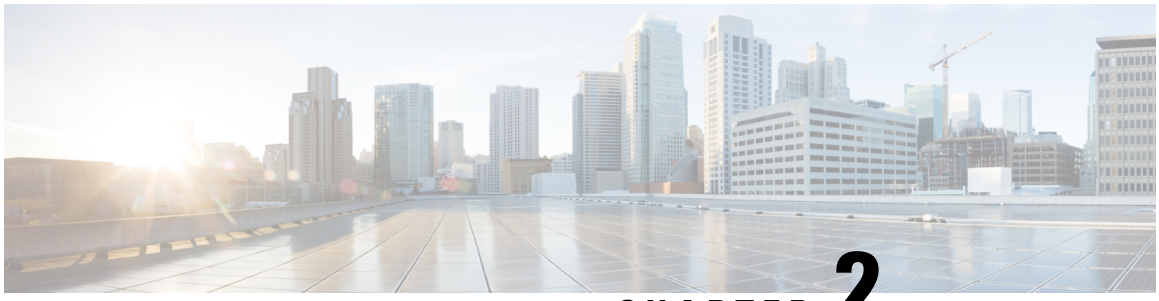
Purpose of the Guide

The Quick Start Guide is designed to assist SEA administrators in enabling Secure Equipment Access (SEA) service on IE switches and to provide step-by-step instructions for setting up the first remote session using the SEA service.

- Assist SEA administrators with enabling Secure Equipment Access (SEA) service on IE switches .
- Provide step-by-step instructions to help administrators set up the first remote session using the SEA service.

For more details and advanced concepts, refer to the Cisco IoT Operations Dashboard documentation on Cisco DevNet.

Purpose of the Guide



CHAPTER 2

Secure Equipment Access Overview

- Cisco Secure Equipment Access service, on page 3
- Prerequisites for enabling SEA, on page 3
- Enabling the SEA service, on page 4

Cisco Secure Equipment Access service

Cisco Secure Equipment Access is a remote access solution that

- provides secure, managed connectivity to industrial IoT devices,
- integrates hybrid-cloud control through Cisco IoT Operations Dashboard, and
- enables customers and partners to perform maintenance on OT assets at remote sites.

The on-premises component runs on supported industrial network devices.

Prerequisites for enabling SEA

You must meet the following prerequisites before enabling SEA on IE switches:

- Ensure you have a valid IoT Operations Dashboard (IoT OD) organization (cloud tenant). If you don't have one, send a request to mailto:iotod-account-request@cisco.com.
- Confirm you have SEA System Admin roles in the organization.
- The switch must have an SD card.
- The switch must run Cisco IOS XE version 17.14.1 or later.
- Ensure the switches have an active Internet connection to us.ciscoiot.com or eu.ciscoiot.com, depending on the IoT OD cluster used.

Enabling the SEA service

Summary

The key components or participants involved in the process are:

- Network administrator: Configures and manages the IE switches.
- IE switches: The device that is prepared and configured for enabling SEA service.
- SEA agent: An IOx application that runs on the device.

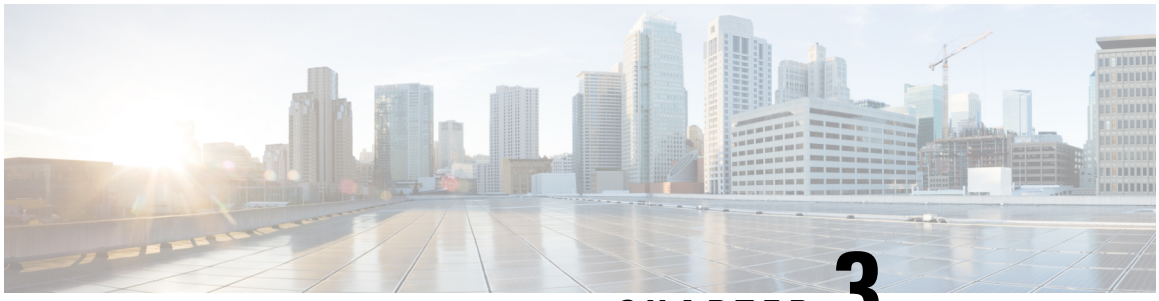
Workflow

These are the stages for enabling SEA service on your switches:

1. Onboard the required switches to the Cisco IoT Operations Dashboard.
2. Create access control groups and add users and assets to the groups.
3. Configure remote sessions.

Result

The switch is enabled with SEA, allowing secure remote access for operational tasks.



CHAPTER 3

Manage access control groups for remote access

- Access control groups, on page 5

Access control groups

An access control group is a security feature that provides administrators with the ability to define and manage secure remote access for groups of SEA users to specific remote assets.

- Provides granular control over who can access what and when.
- Enables creation of groups and assignment of permissions for remote access.
- Supports multiple access control group types for flexible access management.

Types of access control groups

There are three types of access control groups you can configure:

- **Always Active** – users in this group can always access the access methods defined in this group.
- **Scheduled Access** – users in the group can access remote assets for the configured duration.
- **Request Access** – Users must explicitly request access to the remote assets. They can access the assets only after the Access manager (approver) approves the requests.

How remote session access requests work

Remote session access requests allow organizations to control access to OT assets securely and according to policies, using the IoT Operations Dashboard.

Summary

Actors and components participate in the remote session access request process:

- **SEA System Admin** or **SEA Access Admin** : Creates and configures access groups with request controls.
- **Remote access user** : Requests access to the asset via the dashboard.
- **SEA Access Manager** (or other approvers): Reviews and approves or rejects access requests.

- **IoT Operations Dashboard** : Hosts the interfaces for all actions.

This process ensures that only authorized users can access assets. All actions are subject to approval and audit.

Workflow

These stages describe how remote session access requests are processed:

1. The SEA System Admin or SEA Access Admin logs in to the IoT Operations Dashboard and creates an access control group with the "Request Access" feature enabled. At least one SEA user and one asset must be assigned to the group.
2. The remote access user logs in and requests access to an asset within an enabled group.
3. The SEA Access Manager, or other permitted roles such as the SEA System Admin, SEA Access Admin, or any role with 'Access Approver' permission, reviews and either approves or rejects the access request.
4. Upon approval, the remote access user gains access to the asset for the specified time period.

Result

The system enforces policy-driven, auditable, and time-bound access for OT assets, minimizing the risk of unauthorized usage.

Create an access control group for remote access

Set up control over remote access by grouping users and assets under defined access conditions.

Create access control groups in the Secure Equipment Access (SEA) system to define which users can access specific remote assets and under what conditions.

Before you begin

- Ensure you have either an **SEA System Admin** or **SEA Access Admin** role.

Procedure

Step 1 From the left **Service** panel, choose **Secure Equipment Access** > **Access Management**.

Step 2 On the **Access Management** page, view the **Access Control Groups** table.

The **Access Control Groups** table lists the available access control groups, including the group name and the number of users assigned to each group. You can search for a specific group in the **Search** field at the top of the table.

Step 3 Click **Add Group**.

Step 4 On the **Add New Access Control Group** page, configure the group details:

a) Enter the name of the access group in the **Name** field.

b) (Optional) Enter a brief description about the access group in the **Description** field.

c) Choose a group type in the **Group Type** section depending on the remote session you want to configure.

For more information, refer to Cisco DevNet documentation on Request access to a remote session and Manage access control groups for remote access.

d) (Optional) Click the **Group Enabled** toggle switch if you want to disable the group. By default, the group is enabled. If you disable it, the SEA users can't access remote sessions in the group.

Note
Disable a group during situations such as device upgrades or repairs, when the Access Admin does not want access to certain remote sessions. When you disable a group, the group won't be listed in the Access Sessions screen.

e) (Optional) Click the **Enforce Inline (SSH/RDP/VNC) Recording** toggle switch to enforce inline recording. By default, it's disabled.

Step 5 Click **Next**.

Step 6 (Optional) In the **Assign Users** section, choose the users from the list who you want to add to the group, and click **Next**.

Step 7 (Optional) In the **Assign Remote Sessions** section, choose the assets you want the SEA users to access.

Step 8 Click **Save**.

The system creates a new access control group with defined settings. Assigned users and assets can be managed from the group's details page.

Add users to an access control group

Add users to an existing access control group to grant them remote access permissions.

Group membership can be updated after creation to provide selected users with the necessary access permissions.

Before you begin

- Confirm that you have either the SEA System Admin or SEA Access Admin role.

Procedure

Step 1 From the **Service** panel, select **Secure Equipment Access** > **Access Management** .

Step 2 Select the desired access control group.

Step 3 Click **Add Users** in the **Users** tab.

Step 4 Select the users to add to the group, then click **Save**.

Note
If the required user is not listed, add them through SEA System Management. Contact your SEA System Admin for help.

The selected users become members of the access control group.

Add asset access to an access group

Use this task to define asset access for group members. After assets are assigned, users can view remote sessions in the IoT Operations Dashboard. Connection rights may depend on further approval.

Procedure

Step 1 From the left **Service** panel, choose **Secure Equipment Access** > **Access Management**.

Step 2 Choose a **group** from the Access Management page.

Step 3 Click **Asset Access** tab. Click **Add Asset Access**.

Step 4 Select **Assets** from the list. Click the **checkbox** next to each asset.

Group members can now view the designated remote sessions for the assigned assets in the IoT Operations Dashboard. They cannot connect to the remote sessions until further approval is granted, according to group policy.

What to do next

You can optionally assign a specific approver for the access request. If approvers are assigned, they will be responsible for reviewing and approving the request.

If no approver is assigned, all admins in your organization will receive email notifications. Any SEA Access Admin or SEA System Admin can review and approve the request.

Assign approvers to an access control group

Ensure each request for access in “Request Access” groups is explicitly reviewed and approved, as required.

Before you begin

The approver must have the **Access Admin** or **Access Manager** role.

Procedure

Step 1 From the **Service** panel, choose **Secure Equipment Access** > **Access Management**.

Step 2 On the **Access Management** page, click the name of the access group created for the **Request Access** feature.

A page appears displaying the **Assigned Users**, **Assigned Remote Sessions** , and **Access Approvers** sections.

Step 3 In the **Access Approvers** section, click **Add access Approver**.

Step 4 In the **Add access Approver** window, select an approver from the available list, and click **Save**.

When an SEA user in the group requests access to a session, the selected approvers receive an email notification. Tenant admins do not receive the email notification unless they are explicitly selected as approvers. Approvers can log in to the IoT Operations Dashboard to manage access requests.

Create access control groups for scheduled access

Use this task to set up control over remote access by grouping users and assets under defined access conditions.

Creating access control groups in Secure Equipment Access enables you to manage and restrict which users can access specific remote assets and set conditions for their access. You may choose to disable a group temporarily during device upgrades, repairs, or other situations where access should be restricted.

Before you begin

- Ensure you have either an **SEA System Admin** or **SEA Access Admin** role.

Procedure

Step 1 From the **Service** panel, choose **Secure Equipment Access** > **Access Management**.

Step 2 On the **Access Management** page, review the **Access Control Groups** table.

The **Access Control Groups** table lists the available access control groups and their details such as the name of the group and the number of users assigned to the group.

Step 3 Click **Add Group**.

Step 4 On the **Add New Access Control Group** page, configure the group details:

a) Enter a name for the access group.
b) (Optional) Enter a brief description about the access group.
c) Choose **Scheduled Access** in the **Group Type** section.
d) (Optional) Click the **Group Enabled** toggle switch if you want to disable this group. If you disable it, the SEA users can't access remote sessions in the group.
e) (Optional) Click the **Enforce Inline (SSH/RDP/VNC) Recording** toggle switch to enforce recording of the remote session that is configured in the access control group. The recording happens when a remote user accesses the remote session. By default, it's disabled.
f) Select a time zone for the group. The time zone selected ensures that access times are accurately set according to the group's regional time.
g) Specify the date and time when the group's scheduled access window begins.
h) Specify the end of the access window for the group on the specified date.

Step 5 (Optional) In the **Assign Users** section, choose the users from the list who you want to add to the group, and click **Next**. Users selected here are authorized to access the remote sessions assigned to the group.

Step 6 (Optional) In the **Assign Remote Sessions** section, choose the assets you want the users to access., and click **Next**.

- A new access control group is created with the defined settings.
- You can view the configured access window in the **Schedule** column on the **Access Control Groups** tab.
- Group members can view the designated remote sessions for the assigned assets in the IoT Operations Dashboard.

What to do next

- Members in this group can access the configured remote sessions during the configured time window.

Schedule statuses

The schedule status is a session attribute. It indicates the current access state for a remote session, determines when remote access is available, and distinguishes between ongoing, scheduled, active, and expired session availability.

- Indicates the current access state for a remote session.
- Determines when remote access is available.
- Distinguishes between ongoing, scheduled, active, and expired session availability.

Schedule Statuses in SEA Access Management

When you open the **SEA Access Management** screen and choose **Access Control Groups**, the Schedule Status column displays four possible statuses for a remote session.

- **Always Active** : No specific time for access; access is always available.
- **Scheduled** : A specific time span for access to a session has been scheduled for a future date.
- **Active** : The scheduled time for access to a session is currently in progress.
- **Schedule Expired** : The scheduled time for access to a session has expired.



Note If a scheduled session is listed as **Schedule Expired** , you can update that expired session for a future date without creating a new scheduled session.

Invite group members to a scheduled meeting

Invite some or all group members to participate in scheduled remote access sessions.

Before you begin

- You must have either an SEA System Admin or SEA Access Admin role.

Procedure

Step 1 Choose the group with the scheduled meeting.

Step 2 In the **Actions** column, choose **Send Invitation** from the drop-down list.

Step 3 To select specific members, tick the checkbox next to each user's name.

Step 4 Click **Send Invitation**.

Each chosen member receives an email notification with the meeting details.

Modify a remote session

Only sessions viewed in List View can be modified.

Procedure

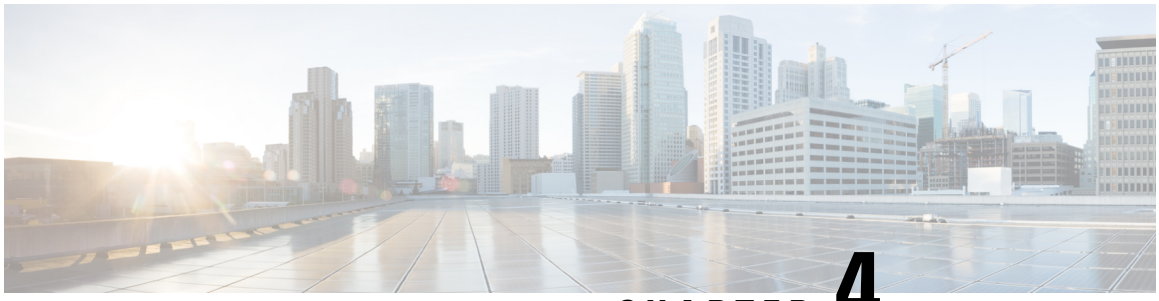
Step 1 Hover over the **3 dots** in the **Actions** column.

Step 2 Click **Edit**. The **Session Details** panel opens.

Step 3 Click the **Edit** icon and edit the session details.

Step 4 Click **Close** to save your changes.

Session details are updated according to your changes.



CHAPTER 4

Deploy SEA Agents Using CLI commands

- Deploy SEA agent on IE switches using CLI commands, on page 13

Deploy SEA agent on IE switches using CLI commands

By following a guided configuration flow in the SEA User Interface and copying suggested CLI commands to the device, you can efficiently enable SEA.

Recommended method for activating SEA on standalone devices

This section describes the recommended method for activating the SEA agent on standalone (CLI-managed) network devices.

- Follow the guided configuration flow in the SEA User Interface.
- Copy and execute the suggested CLI commands on the device.

Note Previously, onboarding and installing the SEA agent required several steps: creating a device profile, adding the network device to the Application Manager service, configuring the device with CLI commands for IoT Operations Dashboard connectivity, and then installing the SEA agent.

For a video tutorial, see Onboarding devices with CLI method.

Deploy the SEA agent using CLI commands

This task enables SEA on CLI-managed switches by generating device-specific CLI commands after guided configuration in the SEA user interface.

Use this procedure to add a network device to the SEA service using CLI deployment.

Before you begin

- Depending on the cluster in use, the IE device (SEA Gateway) must always have access to us.ciscoiot.com or eu.ciscoiot.com.

  If you use an external DNS server, configure your firewall rules to allow your SEA Gateway access to IoT OD and DNS.

For Cisco Catalyst 9300: To install apps, your device must have a valid Cisco DNA Network Advantage license enabled.

SD Card requirement (IE3xx Platforms Only): Format or partition the SD card to create the required IOx partition if it does not already exist. This action erases all data and formats or partitions the card.

- If the complete SD card is reserved for IOx, use this command to format the SD card.

  ```
  Switch# format sdflash: ext4
  ```

- To partition the SD card for both an IOx partition and a FAT32 partition, use this command:

  ```
  Switch# partition sdflash: iox
  ```

- Ensure you note down the client ID of the device by running this command:

  ```
  Switch# show license udi
  ```

Procedure

Step 1 From the **Services** panel, navigate to **Secure Equipment Access** > **System Management**.

Step 2 In the **Network Devices** panel, click **Add Network Device**.

Step 3 On the **Add Network Device** page, locate the **Network Device** area and select **CLI Deployment** from the **Selection Method** drop-down list.

Note
Selecting this option will reveal the Name, Client ID, and Device Type fields.

Step 4 Enter a unique device name in the **Network Device Name** field and the device serial number in the **Client ID** field.

To find your serial number, run this command on your device console:

```
Router# show license udi
```

Step 5 In the **Network Device Model** drop-down list, select your specific model (e.g., Catalyst 9300 Series) and and click **Next**.

The **Advanced Configuration** tab appears. By default, the SEA agent is configured for the native VLAN using DHCP without a proxy.

Step 6 (Optional) Enter any specific configuration details if you need to customize the default settings and click **Add**.

The system generates tailored CLI commands, which are displayed in the **Recommended CLI Deployment Commands** section of the **Deployment** tab.

Step 7 Copy the generated commands and sequentially run them on your device console.
IOx is enabled and configured; VLAN and proxy are configured.

Step 8 Install the **SEA Agent**.

a) Download the SEA Agent package to your local device by clicking **Download SEA Agent**.
b) Copy the package to the flash drive of your network device and use the command in the **Recommended CLI Deployment Commands** section to install it.

Step 9 Click **Close** when the commands finish running.

After successfully running the commands, the status of the network device changes to **active** on the **System Management** page. The CLI commands are automatically saved. To view them at a later time, click **View Deployment Commands** under **Deployment Details** .

Edit configuration details for onboarded IE switches

Use this task to edit device or advanced settings for onboarded IE switches. If you change device or advanced settings, you must regenerate and manually apply new CLI commands.

If you enable SEA on a Cisco Catalyst 9300 device using the CLI with the HTTP Connect Proxy option, the option cannot be disabled by clicking **Edit** on the **Additional Configuration** page.

Before you begin

- Confirm you have access to the device and required privileges.

Procedure

Step 1 Follow these steps to edit **Network Device Details**.

a) On the **System Management** > **Network Device Details**, click **Edit**.

The **Edit Network Device Details** window opens.

b) In the window, edit the **Network Device Name** and **Network Device Description** in the respective fields.

c) Click **Save**.

Step 2 To edit **Additional Configuration**, use these steps.

a) On the **System Management** > **Additional Configuration** page, under, click **View Details**.

The **Additional Configuration** window opens, displaying the current settings.

b) In the window, click **Edit**. The **Edit Additional Configuration** page appears.

c) Modify the settings as required, and click **Save**.

Based on your input, the CLI commands are updated. You can find these commands under the **CLI Restart Commands** section to execute on the device's console.

SEA Agent connectivity modes

A SEA Agent connectivity mode is a connection state setting that determines how the SEA agent establishes a secure connection with the IoT Operations Dashboard, manages which cryptographic key is used during connection, and indicates the agent's current authorization and recovery status.

SEA Agent connectivity modes: Recovery Mode and Rotation Mode

There are two main connectivity modes:

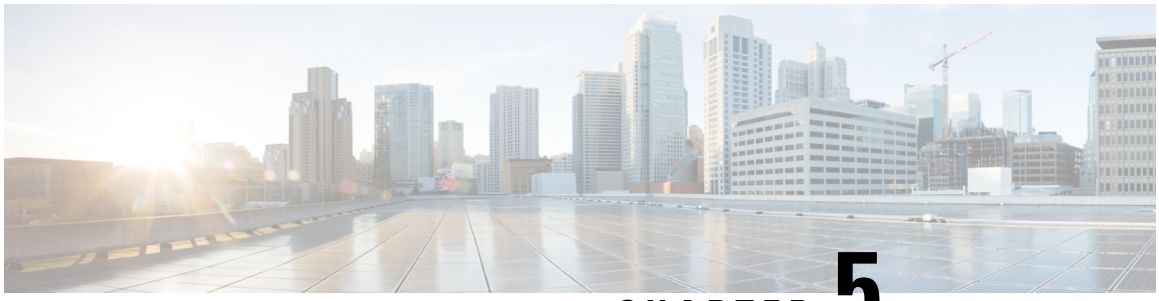
- **Recovery Mode** : When you add a device for the first time, it enters Recovery Mode. This status stays active for 48 hours. During this time, installing the SEA agent using CLI commands generates a new ("rotated") key, and the agent connects to the IoT Operations Dashboard using this rotated key.

- **Rotation Mode** : After a successful connection with the rotated key, the agent switches to Rotation Mode. If a connection fails using the rotated key, the agent prompts you to switch back to Recovery Mode, allowing connection with the recovery key.

You can switch to Recovery Mode by clicking the three dots (…) next to the **View Deployment Commands** area under the **Deployment Details** section in the dashboard.

Example: SEA Agent connectivity mode transitions

Suppose a new device is onboarded. It enters Recovery Mode by default. You install the SEA agent, a rotated key is created, and the agent transitions to Rotation Mode for ongoing secure connections. If future connectivity fails, you may need to revert to Recovery Mode.



CHAPTER 5

Remote Sessions Configurations

• Configure remote sessions, on page 17

Configure remote sessions

Set up OT sessions using Secure Equipment Access (SEA) so authorized users can manage operational technology (OT) assets remotely.

Authorized users can access and manage remote OT devices with improved operational efficiency.

Before you begin

- SEA Agent must be installed on the IE switch associated with the OT assets you want to manage.
- Requested access control groups must be created.

Procedure

Step 1 Navigate to **Secure Equipment Access** > **Quick Wizard**.

Step 2 Under **Connect to Asset**, click **Start Configuration**.

All network devices onboarded to the IoT Operations Dashboard appear in the **Select Network Device** area.

Step 3 In the **Select Network Device** area, select a IE switch from the list and then click **Next**.

Step 4 To configure an OT asset, in the **Configure Connected Asset** area, enter the required details, and click **Next**.

Step 5 To configure an access method, complete these steps:

a) Select an access method from the **Choose Access Method** drop-down list.

An SEA user can access the asset using the access method you select. The available options are RDP, SSH, Telnet, VNC, and Web App. Depending on the access method you select, additional fields are populated.

b) Select an access control group from the **Assign to an Access Control Group** drop-down list and click **Finish**.

Only users who are added to the access control group can remotely access the assets within the group.

Step 6 To test the remote connection, click **Test Access Method**, then click **Done**.

The configured remote sessions appear on the **Remote Sessions** page.

What to do next

If the test fails, perform the following troubleshooting steps before proceeding:

- Verify Agent Status: Ensure the SEA Agent on the industrial router or IE switch is Online and has a stable connection to the IoT Operations Dashboard.
- Check Asset Connectivity: Confirm the industrial router can "ping" or reach the OT asset's IP address within the local network.
- Validate Port Settings: Ensure the port associated with your chosen access method (e.g., Port 3389 for RDP, Port 22 for SSH) is open on the OT asset and not blocked by a local firewall.



INDEX

E

Enabling SEA on industrial routers 3

I

IR on SEA service 3

O

Onboarding industrial routers to SEA service 3