

Cisco Secure Equipment Access Quick Start Guide for Industrial Routers

First Published: 2024-09-12

Last Modified: 2025-06-13

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 **Secure Equipment Access Overview** 1

Cisco Secure Equipment Access service 1

Prerequisites for enabling SEA 1

Enabling the SEA service 1

CHAPTER 2 **Add Network Devices and Assets** 3

Network devices onboarding and SEA Agent deployment 3

Deploy SEA Agent on network devices using CLI commands 3

Edit configuration details for onboarded devices 4

SEA Agent connectivity modes 5

Operational technology (OT) assets 5

Add OT assets to a network device 6

CHAPTER 3 **Manage Access Control Groups** 7

Access control groups 7

How remote session access requests work 7

Create access control groups for scheduled or request access 8

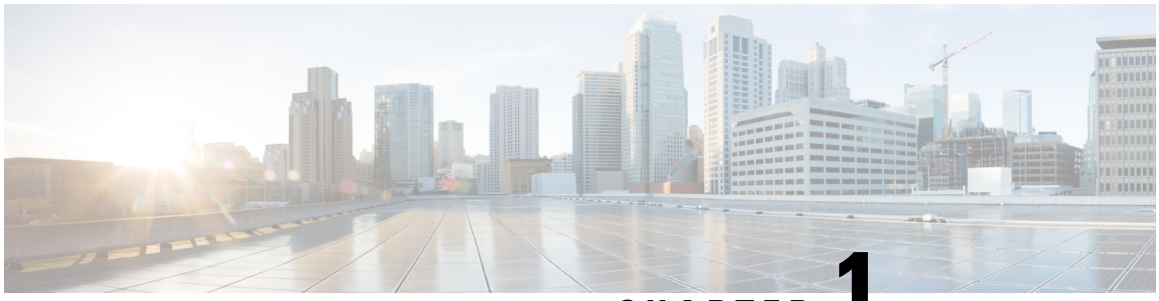
Assign approvers to an access control group 9

Schedule statuses 9

Send invitations to group members for a scheduled meeting 10

CHAPTER 4 **Remote Sessions Configurations** 11

Configure remote sessions 11



CHAPTER 1

Secure Equipment Access Overview

- Cisco Secure Equipment Access service, on page 1
- Prerequisites for enabling SEA, on page 1
- Enabling the SEA service, on page 1

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 industrial routers:

- 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.
- Verify that the routers are running Cisco IOS XE version 17.15.1 or later.
- Ensure the IR routers 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 industrial routers.
- Industrial routers: The device that is prepared and configured for enabling SEA service.
- SEA agent: An IOx application that runs on the device.

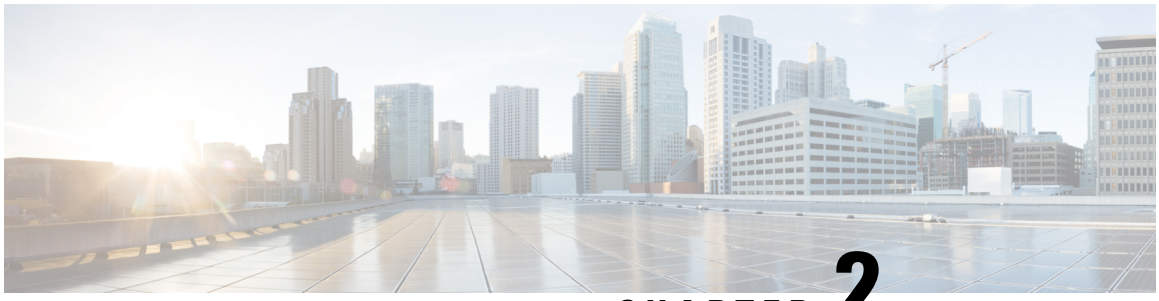
Workflow

These are the stages for enabling SEA service on your industrial routers:

1. Onboard the required Industrial routers 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 industrial router is enabled with SEA, allowing secure remote access for operational tasks.



CHAPTER 2

Add Network Devices and Assets

- Network devices onboarding and SEA Agent deployment, on page 3
- Operational technology (OT) assets, on page 5

Network devices onboarding and SEA Agent deployment

The process of network device onboarding and SEA Agent deployment enables efficient configuration and activation of the SEA Agent on supported devices.

- A guided configuration flow in the SEA UI.
- A way to generate device-specific CLI configuration commands and to copy and run them on the device console.
- Reliable onboarding of the network device and activation of the SEA Agent.

Deploy SEA Agent on network devices using CLI commands

This task enables SEA on routers 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 the CLI deployment method.

Before you begin

- Depending on the cluster in use, the device 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.
- Ensure you get the client ID of the device by running this command:

```
Device# show license udi
```

Procedure

Step 1 On the **Service** panel, click **Secure Equipment Access** > **System Management** > **Add Network Device**.

Step 2 On the **Add Network Device** page, select **CLI Deployment** in the **Selection Method** drop-down list.

Step 3 Enter a unique device name in the **Network Device Name** field and the device serial number in the **Client ID** field.

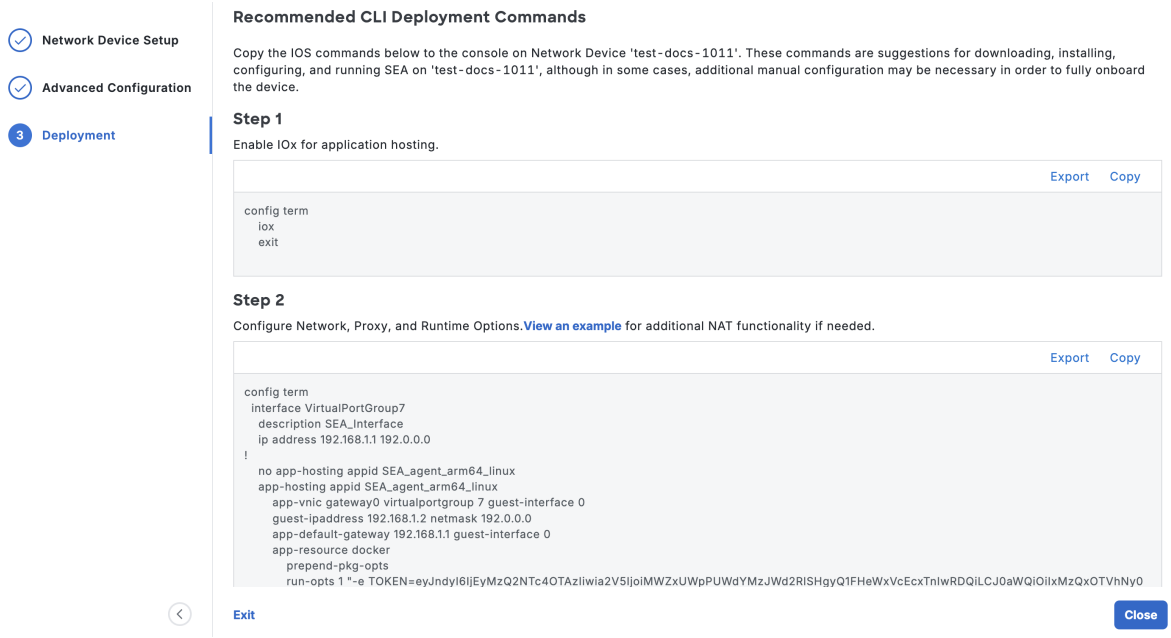
Step 4 To select a specific device series:

a) Select a device type (router or switch) from the **Network Device Model** drop-down list.
b) Select a specific model from the **Network Device Model** drop-down list.
c) Click **Next**.

Step 5 In the **Advanced Configuration** tab, enter the network configurations, and click **Add**.

The UI displays the CLI commands required to configure your network device and install the SEA Agent. These commands are specifically generated for the device currently being onboarded and are organized into three sequential steps: **Step 1**, **Step 2**, and **Step 3**.

Figure 1: CLI deployment commands



Step 6 Copy the generated commands from **Step 1** and **Step 2** and sequentially run them on your device console.
You have successfully enabled IOx application hosting and configured the required network and proxy settings.

Step 7 To install the SEA Agent:

a) Download the SEA Agent package to your local device by clicking **Download SEA Agent** in **Step 3**.
b) Copy the package to the flash drive of your device and run the command in **Step 3** to install the package.

Step 8 Click **Close** after the commands have finished 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 devices

Use this task to edit device or advanced settings for onboarded devices and apply the changes using the updated CLI commands.

Any changes to device or advanced settings require regeneration and manual application of new CLI commands.

Before you begin

- Confirm you have administrative access to the device.

Procedure

Step 1 On the **System Management** page, click **Network Device Details** > **Edit**.

Step 2 In the **Edit Network Device Details** window, edit the required details, and click **Save**.

Step 3 To edit network details such as proxy URL and VLAN configurations:

a) In the **Additional Configuration** section, click **View Details**.

b) Click **Edit**, modify the desired settings, and click **Save**.

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

SEA Agent connectivity modes

SEA Agent connectivity mode is the operational state that

- Determines how the SEA Agent establishes a secure connection with the IoT Operations Dashboard.
- Starts in recovery mode during initial device onboarding.
- Switches to rotation mode after successful connection.

Recovery and rotation modes

SEA Agent supports two connectivity modes:

- **Recovery Mode**: When a device is onboarded for the first time, it enters recovery mode for 48 hours. During this period, the SEA Agent uses the recovery key to establish its initial secure connection to Cisco IoT Operations Dashboard. Recovery mode also lets the device restore connectivity if reconnection is needed.
- **Rotation Mode**: After the SEA Agent successfully connects to the IoT Operations Dashboard using the recovery key, it transitions to rotation mode. In this mode, the SEA Agent periodically rotates or renews its security credentials (keys) to maintain secure communication. If the connection using the rotated key fails, you can switch the Agent back to recovery mode so it can reconnect by using the recovery key.

You can manually switch the SEA Agent back to recovery mode by clicking the three dots (…) next to the **View Deployment Commands** area in the **Deployment Details** section in the management interface.

Operational technology (OT) assets

An OT asset is a physical device such as a PLC, sensor, or industrial controller that directly monitors or manipulates physical industrial processes.

- Represents critical physical endpoints within an IIoT network.
- Requires robust, authenticated access controls to ensure operational integrity and security.

Add OT assets to a network device

Use this procedure to manually add an asset for a device.

This task allows you to add an OT asset to a network device.

Procedure

Step 1 From the **System Management** page, choose a **Network Device**.

Step 2 From the **Network Device Details** page, click **Add Asset**.

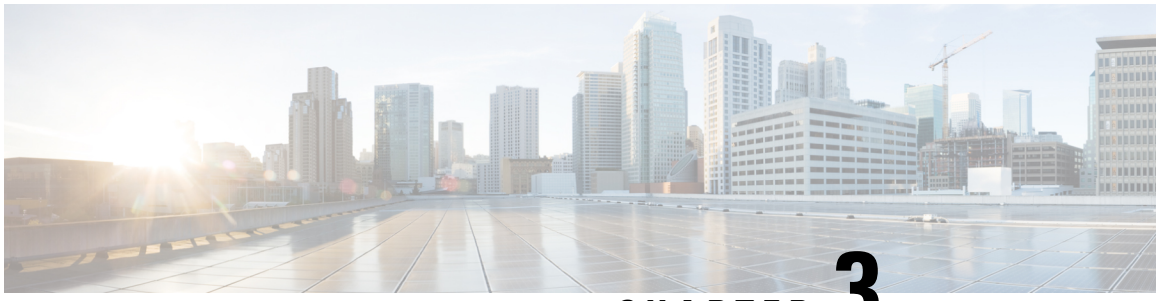
Step 3 On the **Add Asset** page, choose one of the following options:

- **Select from list (Recommended)**
- **Manual entry**

Step 4 After you choose the option, enter the asset name, IP address or host name, and description in the respective fields and click **Add**.

Note
To access this asset using the SEA Plus protocol, you must enter the IP address only. Entering the hostname will cause the SEA Plus connection to fail.

The asset is associated with the network device.



CHAPTER 3

Manage Access Control Groups

- Access control groups, on page 7

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 remote sessions defined in this group.
- **Scheduled Access** – users in the group can log in to the IoT Operations Dashboard and access the remote sessions during the configured time window. No approvals required.
- **Request Access** – users must explicitly request access to the remote assets, and they can access the assets only after the Access manager (approver) approves the requests.

How remote session access requests work

Remote session access requests provide a secure, policy-driven method for controlling access to OT assets through the IoT Operations Dashboard.

Summary

The following 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 user interfaces for all actions.

This process ensures that only authorized users can access assets, with all actions 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 SEA System Admin, SEA Access Admin, or any role with Access Approver permission) reviews and 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 access control groups for scheduled or request access

Creating access control groups in Secure Equipment Access enables you to control remote access by grouping users and assets under defined access conditions.

Access control groups allow administrators to manage remote access for users and assets, supporting both scheduled and request-based workflows. Groups can be temporarily disabled during device upgrades, repairs, or other periods when access should be restricted.

Before you begin

- You must be an SEA System Admin or SEA Access Admin.

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 to see the available groups and their details, including group names and the number of users assigned.

Step 3 Click **Add Group** and enter a name and a description.

Step 4 Select the group type:

- **Request Access**: Use request-based workflow for access.
- **Scheduled Access**: Set the time zone, start date/time, and end date/time for scheduled access.

Step 5 (Optional) Click the **Group Enabled** toggle switch to disable the group as needed. When disabled, users cannot access remote sessions in the group.

Step 6 (Optional) Click the **Enforce Inline (SSH/RDP/VNC) Recording** toggle switch if you want to record remote sessions accessed by group members, and click **Next**.

Step 7 (Optional) In the **Assign Users** section, select the users you want to add to the group and click **Next**. These users will be authorized to access the remote sessions assigned to the group.

Step 8 (Optional) In the **Assign Remote Sessions** section, choose the assets you want the group's users to access and click **Next**.

Step 9 Review all settings and confirm to create the access control group.

A new access control group is created with your chosen settings. Group members can access assigned remote sessions according to scheduled or request access conditions. If inline recording is enabled, remote sessions are automatically recorded.

What to do next

For request access groups, assign approvers who will handle access requests from group members.

Assign approvers to an access control group

This process is essential for groups configured with the Request Access type, ensuring requests are explicitly approved.

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.

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**.

The selected approvers receive an email notification when a member of the group requests access to a session. Even if you are a tenant admin, you won't receive the email notification unless you are explicitly selected as an approver. The approvers can log in to the IoT Operations Dashboard and manage the access requests.

Schedule statuses

The **Schedule** column in the **Access Control Groups** page indicates the current access state for a remote session.

- Determines when remote access is available.
- Distinguishes between ongoing, scheduled, active, and expired sessions.

When you go to **Secure Equipment Access** > **Access Management** > **Access Control Groups**, the **Schedule** column lists the 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.

Send invitations to group members for a scheduled meeting

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

Before you begin

- You must be an SEA System Admin or SEA Access Admin.

Procedure

Step 1 Go to **Secure Equipment Access** > **Access Management**.

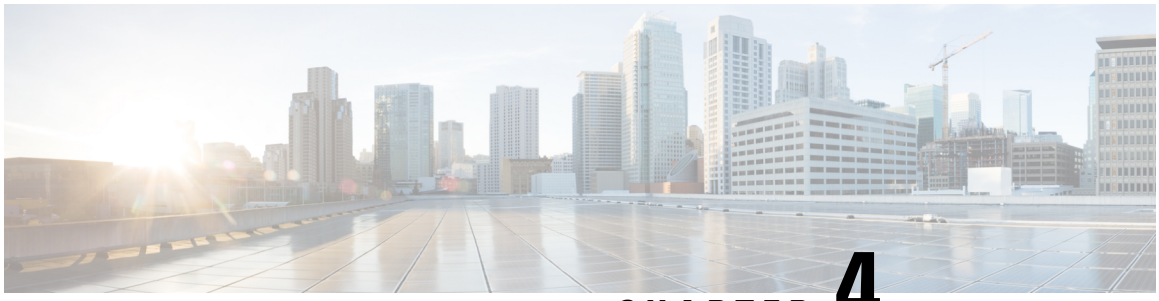
Step 2 Select a group that has the meeting scheduled.

Step 3 In the **Actions** column, choose **Send Invitation** from the drop-down list.

Step 4 In the **Select members for invitation notification** window, select the group members to whom you want to send the invitation.

Step 5 After choosing members, click **Send**.

Each member receives an email with meeting information.



CHAPTER 4

Remote Sessions Configurations

• Configure remote sessions, on page 11

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 industrial router 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 industrial router 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 1

I

IR on SEA service 1

O

Onboarding industrial routers to SEA service 1