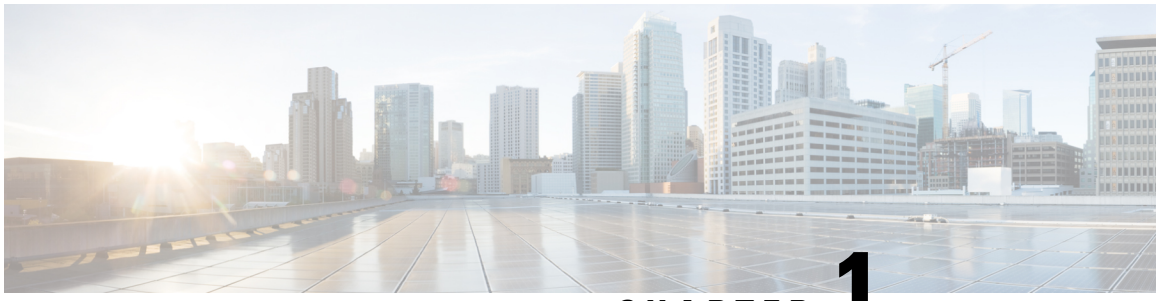
# Cisco Secure Equipment Access Quick Start Guide for Industrial Routers

**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

# CONTENTS



CHAPTER 1

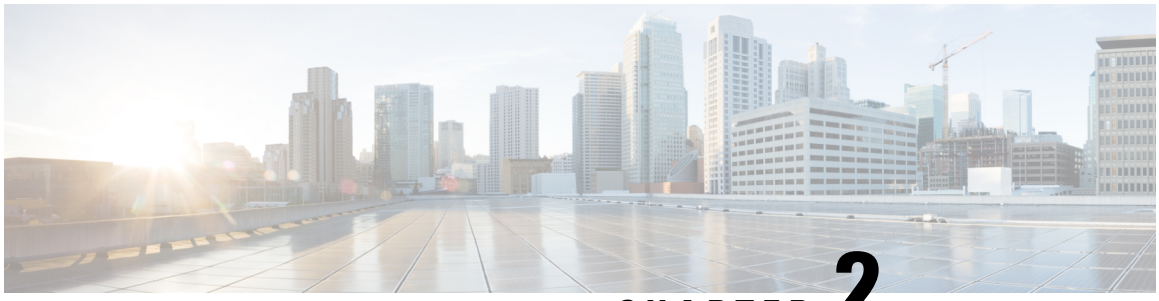
# Purpose of the Guide



## Purpose of this guide

This guide assists SEA administrators in enabling Secure Equipment Access (SEA) service on industrial routers (IR). The guide also helps administrators set up the first remote session via the SEA service.

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



CHAPTER 2

# Secure Equipment Access Service Enablement



## Cisco Secure Equipment Access service

The Cisco Secure Equipment Access (SEA) service is a hybrid-cloud solution with control and management handled by the Cisco IoT Operations Dashboard. The on-premises component runs on a supported industrial network device deployed at a remote site with the target operational technology (OT) asset. The SEA service aims to provide customers and partners with remote access to specific industrial IoT resources for maintenance operations.

## Prerequisites

- 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 both Application Manager and SEA System Admin roles in the organization. For details, see SEA roles and permissions.
- Verify that the IR 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.

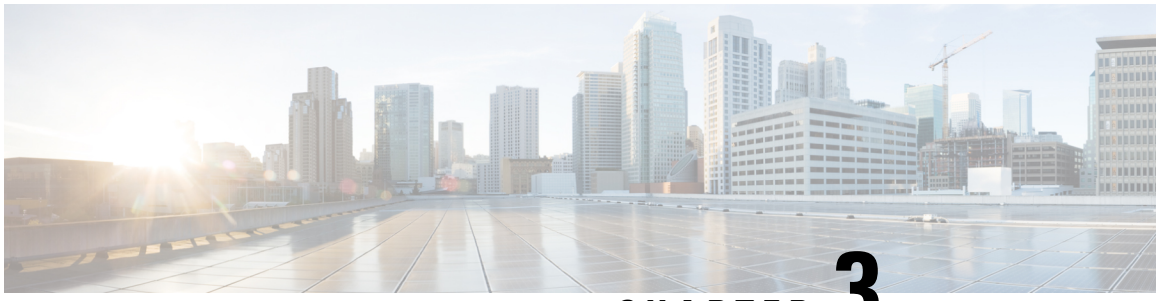
## Enabling the SEA service

### Workflow

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

1. Application Manager Service Configurations: Onboard the required IR device through the Application Manager service on IoT OD.

2. IR router configuration: Configure the IR device to establish a secure tunnel to the IoT OD for application management.
3. Remote access configuration: Install the SEA agent on the IR device and configure a remote session through SEA for the target OT asset.



CHAPTER 3

# Application Manager Service Configurations



## Create device profiles

A device profile is a configuration file that contains user credentials to access devices. Use the device profile to onboard multiple devices to the Cisco IoT OD. Cisco IoT OD uses the user credentials configured in the device profile to establish a connection with multiple devices.

### Procedure

**Step 1** Go to **Device Profiles** and click **Create Device Profile**.

The **Create Device Profile** page appears.

**Step 2** On the **Create Device Profile** page, enter a profile name in the **Device Profile Name** field and optionally enter a description in the **Device Profile Description** field.

**Step 3** In the **Configure credentials** area, enter the username and password in their respective fields for the device profile configuration.

**Note**
Use privilege level 15 user credentials.

**Step 4** Click **Next**.

The device profile is ready for your review.

**Step 5** After confirming the device profile details, click **Create Device Profile**.

The created device profile is listed on the **Device Profiles** page.

# Add IR devices to the Application Manager service

The purpose of this procedure is to enable you to add IR routers to the Application Manager service.

### Before you begin

Ensure the following:

- You have created a device profile on the IoT Operations Dashboard.
- You have noted down the serial number and product ID of your IR routers.

  To display the product ID and serial number, use this command on your device's console.

  Router# **show license udi**

## Procedure

**Step 1** In the Cisco IoT Operations Dashboard, navigate to the **Application Manager** service.

**Step 2** Choose **Devices** > **Staged** tab.

**Step 3** Click **Add Devices**.

**Step 4** On the **Select Add Device Method** window, select **Single Device**.

**Step 5** On the **Add Device** page, enter the product ID, serial number, and name in the respective fields.

**Step 6** Click **Next**.

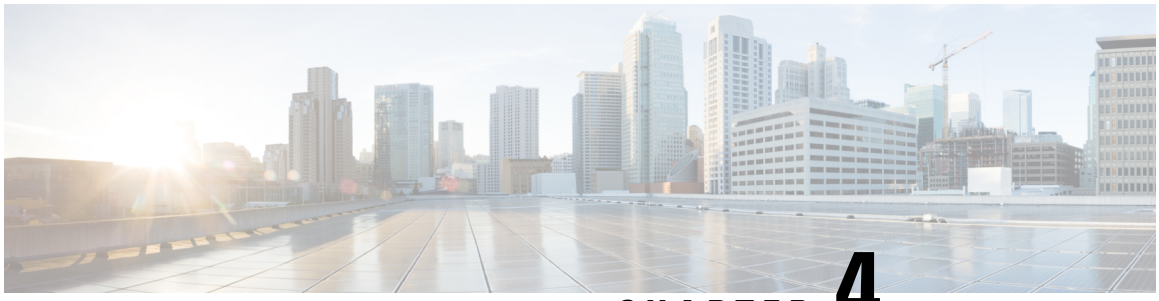
**Step 7** On the **Select Device Profile for Assignment** page, choose a device profile from the list and click **Next**.

**Step 8** Review the configuration information on the **Review** page, and click **Add Device**.

The new device is listed under **Staged Devices**, indicating that the device has not been registered with the Cisco IoT Operations Dashboard yet.

### What to do next

Perform the IR routers configurations.



CHAPTER 4

# Industrial Router Configurations



# Prerequisites for configuring industrial routers

### IR1101 devices

Ensure that your IR1101 device has IOx container keys programmed.

- Run this command:

  ```
  Router# show software authenticity keys | i Name
  ```

- In the output, look for lines containing "Product Name: Cisco Services Containers". If the lines are present, the device has IOx container keys programmed.
- If the lines are missing:
  - Devices shipped before January 2020: Either disable signature verification or upgrade the device.
  - Devices shipped after January 1, 2020: No action is required, the device should have the container keys programmed by default.

**Note** SEA installation will fail with a signature verification error if the device has neither container keys programmed nor signature verification enabled.

### Application Manager service

Ensure that the IR router is added to Cisco IoT OD Application Manager.

# Configuring industrial routers

### Workflow

There are the stages of configuring industrial routers to establish connection with Cisco IoT OD.

1. Prepare the device
2. Configure and enable IOx, on page 8
3. Configure the IR device to connect to IoT OD, on page 10
4. Verify configuration on the device, on page 11
5. Verify the device status on the Operations Dashboard, on page 12

### Result

You have successfully configured the device to be able to communicate with the IoT OD.

### What's next

Configure remote sessions

# Prepare industrial routers

Use this procedure to prepare industrial routers for SEA configuration.

### Procedure

**Step 1** Attach the necessary networking cables.

**Step 2** Power up the device.

Your industrial routers are ready for SEA configuration.

# Configure and enable IOx

Perform this task to ensure that IOx applications have the necessary IP connectivity and network settings to operate effectively.

IOx is a container hosting platform that runs on Cisco IOS XE. It's used to install and execute several services that Cisco IoT Operations Dashboard can deliver such as Secure Equipment Access (SEA), Cisco Cyber Vision (CCV), and Edge Intelligence (EI).

## Procedure

**Step 1** Configure the VirtualPortGroup0 (VPG) Interface , DHCP Pool, and NAT rules on the device for IOx network.

**a.** Configure the VPG Interface. The virtual interface that connects IOx applications to IOS XE is called VirtualPortGroup0. The IOx applications need IP connectivity through the virtual interface, which includes receiving an IP address. An example configuration is given in the next line. You can change the IP address to suit your requirements. Enter these configuration commands on the router console, in the config mode.

```
! Example
  conf t
  interface VirtualPortGroup0
  description IOx Interface
  ip address 192.168.16.1 255.255.255.0
  ip nat inside
  ipv6 enable
  end
```

**b.** Configure the DHCP pool. When the IOx applications start, they will request an IP address via DHCP. Therefore, you need to configure a DHCP pool for IOx applications. An example configuration of IP pool and DNS server is given in the next line. You can customize this configuration to suit your requirements. Ensure that the default router IP address is the same as the IP address previously configured for the `VirtualPortGroup0` interface.

```
! Example
  conf t
  ip dhcp pool ioxpool
  network 192.168.16.0 255.255.255.0
  default-router 192.168.16.1
  dns-server 192.168.16.1 8.8.8.8
  end
```

**c.** Configure NAT. IOx Apps use private IP addresses obtained from DHCP. They need Network Address Translation (NAT) to access the internet. Add NAT Rules for the DHCP pool to enable IOx App traffic to access the internet.

In the example below, assume that the connection to the internet will be through Cellular 0/1/0. Make sure to change or adjust the interface if it is not Cellular 0/1/0. For example, it could be GigabitEthernet 0/0/0 or Cellular 0/3/0.

```
! Example of a NAT rule for using Cellular0/1/0 as an uplink:
  conf t
  interface Cellular0/1/0
  ip nat outside
  ip access-list extended NAT_ACL
  10 permit ip 192.168.16.0 0.0.0.255 any
  route-map RM_WAN_ACL2 permit 10
  match ip address NAT_ACL
  match interface Cellular0/1/0
  ip nat inside source route-map RM_WAN_ACL2 interface Cellular0/1/0 overload
  end
```

**Step 2** Enable IOx.

```
conf t
iox
end
```

**Step 3** Verify that IOx is running correctly by running this command in exec mode:

```
show iox-service
! Example 1: When IOx is up and running, both the "IOx service (CAF)" and "dockerd" will be running.
Router#sh iox-service
```

```
IOx Infrastructure Summary:
---------------------------
IOx service (CAF)          : Running
IOx service (HA)           : Not Supported
IOx service (IOxman)       : Running
IOx service (Sec storage)  : Running
Libvirtd 5.5.0             : Running
Dockerd v19.03.13-ce       : Running
```

IOx services are running on the device.

# Configure the IR device to connect to IoT OD

To establish a connection with the Cisco IoT Operations Dashboard, you must run a set of IOS commands on the device's CLI. To manage the IOx Apps, the Cisco IoT Operations Dashboard requires a valid user configured with level 15 credentials on the switch in IOS XE.

1. Create a privilege 15 user by applying the following configuration. The credentials should match the values configured in the Device Profile on the Cisco IoT Operations Dashboard:

   ```
   conf t
   username <DEVICE PROFILE USERNAME> privilege 15 algorithm-type scrypt secret <DEVICE
   PROFILE PASSWORD>
   end
   ```

2. Configure the authentication-related settings and WSMA settings.

   ```
   conf t
   aaa new-model
   aaa authentication login default local
   aaa authorization exec default local
   ip http server
   ip http authentication local
   ip http secure-server
   wsma agent exec
   profile exec
   wsma profile listener exec
   transport http path /wsma/exec
   cgna gzip
   end
   ```

3. Configure the IDA transport profile: Enable a secure TLS connection using WebSocket to Cisco IoT Operations Dashboard using TLS with port TCP 443.

   **For the US Cluster**:

   ```
   conf t
   ida transport-profile wst
    callhome-url wss://device-us.ciscoiot.com/wst/cgna
    active
   end
   ```

   **For the EU Cluster**:

   ```
   conf t
   ida transport-profile wst
    callhome-url wss://device-eu.ciscoiot.com/wst/cgna
   ```

```
 active
end
```

4. Configure the CGNA registration profile.

```
conf t
  cgna profile cg-nms-register
   transport-profile wst
   add-command show version | format flash:/managed/odm/cg-nms.odm
   add-command show inventory | format flash:/managed/odm/cg-nms.odm
   interval 3
   active
   url https://localhost/cgna/ios/registration
   gzip
  end
```

**Note** Once the configuration is done, the device connects to IoT OD and triggers the registration process.

5. (Optional) Enable DNS on the router if it's not already acquired through the DHCP server.

   This is important if the router is configured with a static IP and a static default gateway, and no DNS server is explicitly specified. In this example, we use a Cisco DNS. You can use any DNS server.

```
conf t
ip name-server 208.67.222.222
end
```

# Verify configuration on the device

Use the following commands to verify that the device is configured correctly to connect to IoT OD.

Router# **show ida transport-profile-state all**

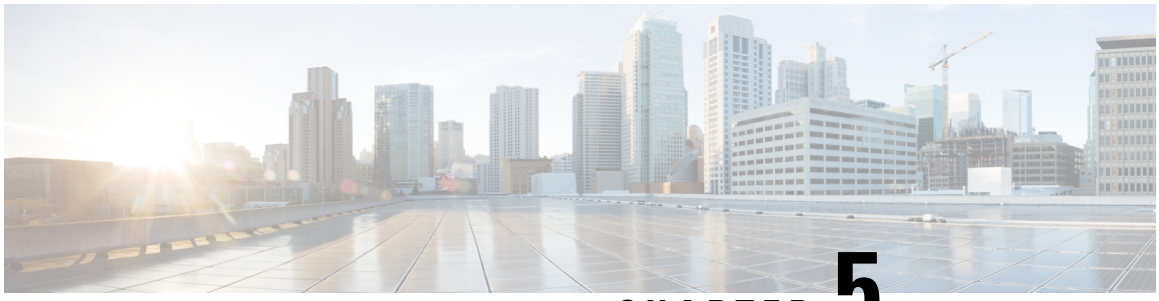
```
! Verify that IDA status is connected for the "wst" transport profile
 ! Notice the line "IDA Status: Connected" in the show command output below for the "wst"
transport profile.
 Router#sh ida transport-profile-state all
 Transport Profile 1:
 Profile Name: wst
 Activated at: Fri Jun  7 07:26:42 2024
 Reconnect Interval: 30 seconds
 keepalive timer Interval: 50 seconds
 Source interface: [not configured]
 callhome-url: wss://device-us.ciscoiot.com/wst/cgna
 Local TrustPoint: CISCO_IDEVID_SUDI
 Remote TrustPoint: [not configured]
 Execution-url: http://192.168.16.1
 Proxy-Addr: [not configured]
 IDA Status: Connected
 State: Wait for activation
 Last successful response at Fri Jun  7 08:25:29 2024
 Last failed response:
 Last failed reason:
```

# Verify the device status on the Operations Dashboard

Once IoT OD receives a registration request from a device and validates its configuration, the device automatically moves from the **Devices > Staged** status to **Registered** status in your IoT OD Organization.

**Troubleshoot Issues**

- If IoT OD receives a registration attempt but encounters some issues, (e.g., incorrect credentials), the IR device remains in the **Devices > Staged** list with **Configure Failure** status until IoT OD receives a registration attempt with the correct credentials.
- If IoT OD does not receive any registration attempt, the IR device remains in the **Devices > Staged** list.



CHAPTER 5

# Remote Sessions Configurations



# Install SEA agent on industrial routers

### Before you begin

Ensure the IR router is added to the IoT OD Application Manager service.

### Procedure

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

The **Quick Wizard** page appears.

**Step 2** Under **Install SEA Agent**, click **Start Configuration**.

All network devices added to the **App Manager Service** are listed under the **Select Network Device** area.

**Step 3** Select the device on which you want to install the SEA agent, and click **Next**.

The **Advanced Configuration** page appears, displaying the default settings for the agent installation. By default, the SEA agent is installed on the native VLAN using DHCP without a proxy.

**Step 4** (Optional) To customize the settings for agent installation, enter the required configuration details on the **Advanced Configuration** page, and click **Deploy**.

The SEA agent will be installed on the network device. You can verify its status on the **SEA Agent Connection** column on the **System Management** page. Wait for 5 to 10 minutes before checking the status.

# Configure remote sessions

### Before you begin

Ensure that the SEA agent is installed on the IR router that can reach the OT assets you want to manage.

**SEA Users and Access Groups**

SEA users are granted access through specific access groups. It is recommended that you create an access group and add both users and the configured remote session to the group. Only users in the group can remotely access OT assets.

**High-Level Steps to Configure a Remote Session**

1. Select a network device to be connected to the asset
2. Configure the asset
3. Configure an access method for remotely accessing the asset
4. Choose an access control group to which both the asset and the user belong
5. Verify that the connection is working

### Procedure

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

The **Quick Wizard** page appears on the right.

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

All network devices added to the **App Manager Service** are listed under the **Select Network Device** area.

**Step 3** Select an IR router from the list and then click **Next**.

The OT asset that you configure in the next step will be associated with this device.

**Step 4** Configure connected asset. In the **Configure Connected Asset** area, enter the following details, and click **Next**:

a) **Asset Name**: Name of the assets to be added.
b) **IP Address**: IP address of the asset.
c) **Description**: A brief description about the asset.

**Step 5** Configure access method.

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

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

b) Choose 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** Test the remote connection by clicking **Test Access Method**.

A new page appears confirming the connection to the asset.

**Step 7** Click **Done**.

The remote session you configured will be displayed on the **Remote Sessions** page. An SEA user can log in to the Cisco IoT Operations Dashboard to access the session.

# Connect to remote assets

After you configure remote sessions, SEA users can connect to remote OT assets.

1. Log in to the Cisco IoT Operations Dashboard as an SEA user.
2. Click **Secure Equipment Access > Remote Sessions**.

   All available sessions are displayed on the screen.
3. Go to the session of your choice and click **Connect**.

   The SEA user connects to the asset using the previously configured access method.

# INDEX