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

CONTENTS

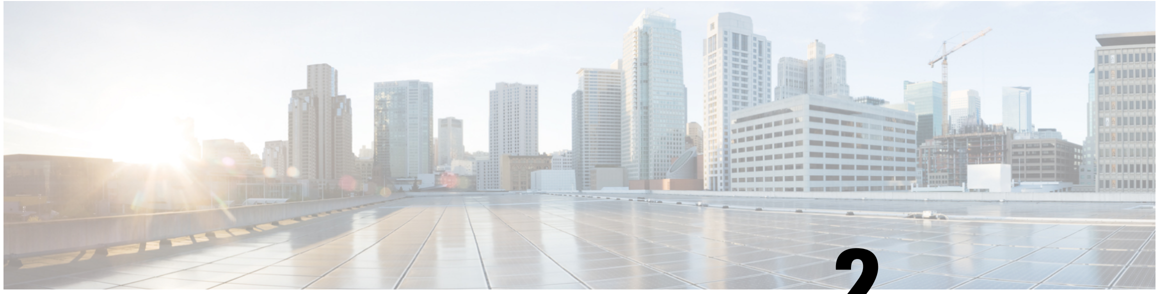
CHAPTER 1

Purpose of the Guide

Purpose of this guide

This guide assists SEA administrators in enabling Secure Equipment Access (SEA) service on IE switches. 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 on Ciso DevNet.



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 for enabling SEA service

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 both Application Manager and SEA System Admin roles in the organization. For details, see SEA roles and permissions.
- The IE switch must have an SD card.
- The IE switch must run Cisco IOS XE version 17.14.1 or later.
- Ensure the IE 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

Enabling SEA services involves multiple stages. 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.
- Application Manager service: Handles onboarding and device management.
- SEA agent: An IOx application that runs on the device.

Workflow

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

1. Onboard the required IE switches through the Application Manager service on IoT OD. For more information, see Application Manager service configurations.
2. Configure the IE switches to establish a secure tunnel to the IoT OD for application management. For more information, see IR router configuration.
3. Install the SEA agent on the IE switches and configure a remote session through SEA for the target OT asset. For more information, see Remote access configuration.

Result

The IE switches is enabled with SEA service, allowing secure remote access for operational tasks.

CHAPTER 3

Application Manager service configurations

Application Manager service

The Application Manager is a service that enables you to manage the IOx application lifecycle. The lifecycle involves tasks such as uploading, installing and managing application on a specific network device.

Within the IoT OD, you can also perform tasks such as upgrading the applications, viewing event logs, uninstalling applications, and much more using the Application Manager service.

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.

Add a new device profile to store credentials for onboarding multiple devices to Cisco IoT Operations Dashboard (IoT OD).

Before you begin

Ensure you have privilege level 15 user credentials to assign to the device profile.

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.

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 new device profile appears in the Device Profiles list, ready for use in device onboarding.

What to do next

Add devices to the Application Manager service.

Add IE devices to the Application Manager service

Adding devices to the Application Manager service enables easy deployment and management of applications on the IE switches.

Add network devices to the Application Manager service of the Cisco IoT Operations Dashboard.

Before you begin

- Create a device profile in the IoT Operations Dashboard.
- Note the serial number and product ID of IE switches.

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

  Switch# **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**.

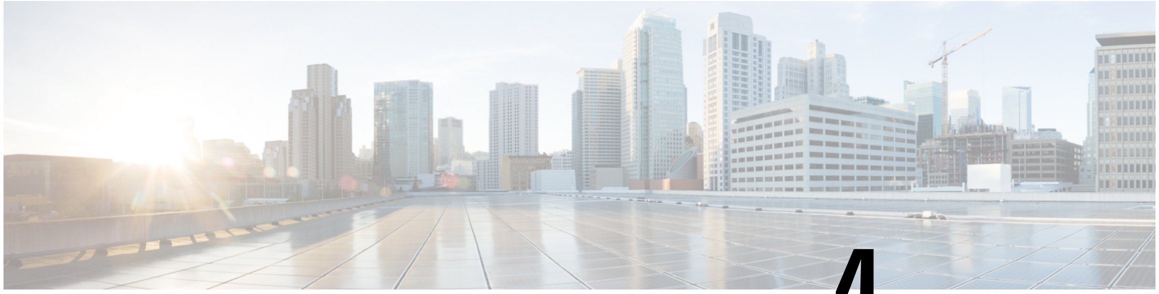
Step 7 On the **Select Device Profile for Assignment** page, choose a device profile from the list and click **Next**.

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 IE switches configurations.



CHAPTER 4

IE Switch Configurations

Configuring IE switches

Summary

Configuring industrial switches to communicate with Cisco IoT Operations Dashboard involves several stages. The key components or participants involved in the process are:

- Administrator: Configures and manages the IE switches throughout the process.
- IE switches: The device that is being prepared and connected to the Cisco IoT Operations Dashboard
- Cisco IoT Operations Dashboard: The cloud-based platform used to manage registered devices and confirm successful connectivity.

Workflow

These are the stages of configuring IE switches to establish connection with Cisco IoT OD.

1. Prepare the device: The administrator ensures the device is powered on, connected to the network, and accessible for configuration. For more information, see Prepare the device.
2. Configure the SD card and enable IOx: The administrator configures a compatible SD card and enables IOx on the device, preparing it to support IoT application deployment. For more information, see Configure the SD card and enable IOx on IE switches, on page 10.
3. Configure the device to connect to Cisco IoT Operations Dashboard: Using the IOS commands, the administrator configures the device to communicate with the IoT Operations Dashboard. For more information, see Configure IE switches for IoT Operations Dashboard connectivity, on page 11.
4. Verify the configuration on the device: The administrator checks the connection status on the device using IOS commands. For more information, see Verify configuration on the device terminal, on page 13.

5. Verify the device status in Cisco IoT Operations Dashboard: The administrator confirms that the device appears as “registered” in the Operations Dashboard. For more information, see Verify the device status on the Operations Dashboard, on page 14.

Result

The IE switch is securely connected to Cisco IoT Operations Dashboard, ready for remote management.

What’s next

Configure remote sessions to manage OT assets.

Prepare IE devices

Use this task to prepare your IE devices before configuring them for SEA.

Get your devices ready for SEA configuration.

Procedure

Step 1 Attach the necessary networking cables.

Step 2 Power up the device.

Your IE devices are ready for SEA configuration.

Configure the SD card and enable IOx on IE switches

Prepare the SD card and enable IOx to allow deployment of containerized applications on Cisco IE switches.

IOx applications require the SD card in ext4 format. Shipped SD cards are formatted as FAT32 and must be reformatted.

Before you begin

- Ensure the SD card is inserted in the switch.
- Have console or SSH access to the switch CLI.

Follow these steps to configure the SD card and enable IOx:

Procedure

Step 1 Format the SD card to ext4 format:

```
format sdflash: ext4
```

Step 2 Configure the AppGigabitEthernet1/1 interface in trunk mode.

To configure AppGigabitEthernet1/1 in trunk mode, set the switchport mode to trunk and define a native VLAN. For the native VLAN, it's best to use a number that isn't likely to be used elsewhere, such as 4094. If the native VLAN is greater than 1004, the switch's VTP mode must be set to transparent to allow the VLAN to be created.

Example:

~~~
conf t
vtp mode transparent
vlan 4094
name app-man-native-vlan
interface AppGigabitEthernet1/1
switchport trunk native vlan 4094
switchport mode trunk
end
```
~~~

Step 3 Enable IOx.

```
conf t
iox
end
```

Step 4 Verify that IOx is running correctly.

IE-3400# **show iox-service**

Confirm all relevant services display as "Running".

```
IOx Infrastructure Summary:
---------------------------
IOx service (CAF)              : Running
IOx service (HA)               : Not Supported
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Running
Libvirtd                       : Running
Dockerd                        : Running
```

The switch is ready to deploy IOx applications; the SD card is correctly formatted, interface is configured, and IOx is enabled.

What to do next

Deploy desired IOx applications as needed.

Configure IE switches for IoT Operations Dashboard connectivity

Enable IE devices to connect securely to the Cisco IoT Operations Dashboard (IoT OD).

To establish a secure connection between IE switches and the IoT Operations Dashboard, you must configure user credentials, enable necessary services, and set up secure transport profiles using device CLI commands.

Before you begin

- Ensure you have access to the switch's CLI with privilege level 15.
- Have an appropriate device profile with validated credentials ready on IoT OD.

Follow these steps to configure IE switches for IoT Operations Dashboard connectivity:

Procedure

Step 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:

Example:

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

Step 2 Configure authentication settings and enable WSMA and HTTP services.

Note
The WSMA service requires "ip http server" to be enabled. For secure application deployment, also enable "ip http secure-server." Review the running-config on the device to avoid duplicate configuration.

```
conf t
  aaa new-model
  aaa authentication login default local
  aaa authorization exec default local

  ip http secure-server
  ip http server
  ip http authentication local

  wsma agent exec
    profile exec
  wsma profile listener exec
    transport http path /wsma/exec

  cgna gzip
  ntp server pool.ntp.org
  end
```

Note
The "ip http server" command initiates a web server on the device, accessible via port 443. If the device is exposed to the internet without firewall protection, restrict access to this web service to reduce security risks.

Step 3 Enable a secure TLS connection with the IoT Operations Dashboard using an IDA transport profile.

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


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

Step 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

After configuration, the device connects to IoT Operations Dashboard and triggers registration.

Step 5 (Optional) Enable DNS services if not already configured via DHCP. This is required for static IP setups without DNS server assignment.

Verify the configuration by using the ping command:

```
Switch# ping us.ciscoiot.com
```

The IE switch establishes a secure connection to the IoT Operations Dashboard and completes device registration.

What to do next

Verify device registration on the IoT Operations Dashboard and optionally on the device's terminal.

Verify configuration on the device terminal

This task helps you confirm that the device’s transport profile is properly configured and able to establish a secure connection with the Cisco IoT Operations Dashboard.

After configuring the device, you must ensure that that device is able to communicate with the Operations Dashboard.

Before you begin

- Ensure you have access to the device terminal as an administrator or a user with sufficient privileges.
- Make sure the transport profile has already been configured on the device.

Procedure

Step 1 Run this command to verify the network connectivity:

Example:

```
Switch# 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.
   Switch#sh ida transport-profile-state all
```

```
Transport Profile 1:
Profile Name: wst
Activated at: Tue Mar 12 15:12:19 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://localhost:80
Proxy-Addr: [not configured]
IDA Status: Connected
State: Wait for activation
Last successful response at Tue Mar 12 15:13:19 2024
Last failed response at Tue Mar 12 15:12:15 2024
Last failed reason: Gracefully disconnected
```

Step 2 Notice the line "IDA Status: Connected" in the show command output.

What to do next

If the IDA status is connected, proceed with remote session configurations.

Verify the device status on the Operations Dashboard

Confirm that a device has successfully moved from the Staged status to the Registered status in your IoT OD Organization after a registration attempt.

When a device submits a registration request to IoT OD and its configuration is validated, the device automatically moves from **Devices** > **Staged** to **Devices** > **Registered**. If no registration attempt occurs, the device remains listed as Staged.

Before you begin

- Ensure you have configured the device to communicate with IoT OD.
- Verify that the device has attempted registration, if applicable.

Procedure

Step 1 Log in to the IoT Operations Dashboard.

Step 2 From the **Sevices** pane, select **Application Manager**.

Step 3 Click **Devices** > **Registered** tab.

The device you added appears in the **Registered** tab, indicating successful registration.

What to do next

Configure your IE switches to enable IOx application deployment.

CHAPTER 5

Remote Sessions Configurations

Install the SEA agent on IE switches

Use this procedure when you need to deploy or update the SEA agent on iIE switches managed through the IoT OD Application Manager service. Installing the agent enables SEA service on industrial routers..

Before you begin

Ensure the IE switch is added to the IoT OD Application Manager service.

Procedure

Step 1 Navigate to **Secure Equipment Access** > **Quick Wizard** on the **Cisco IoT Operations Dashboard.**

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

All network devices added to the **App Manager Service** appear 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 displays the default installation settings. By default, the SEA agent installs on the native VLAN using DHCP without a proxy.

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

The SEA agent is successfully deployed on the selected IE switch, enabling Secure Equipment Access (SEA) services for that device..

What to do next

Verify the agent's status in the **SEA Agent Connection** column on the **System Management** page. Allow 5–10 minutes for the deployment to complete before verifying the status.

Configure remote sessions

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

Before you begin

Ensure the following:

- SEA agent is installed on the IE switch associated with the OT assets you want to manage.
- An access group is created, and both users and the configured remote session are added to the group.

Note Only users in the group can remotely access OT assets.

Procedure

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

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

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

Step 3 Select a IE switchfrom the list and then click **Next**.

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

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

- **Asset Name**: Name of the assets to be added.
- **IP Address**: IP address of the asset.
- **Description**: A brief description of the asset.

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 by 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

Log in to the Cisco IoT Operations Dashboard to access the remote session.

Connect to remote assets

Enable secure access to remote assets for monitoring, management, or troubleshooting.

Use this task when you need to initiate a remote session with your OT assets to perform any maintenance operations.

Follow these steps to connect to remote assets:

Before you begin

- Obtain SEA user credentials with the necessary permissions.
- Verify that your network connection allows access to the IoT Operations Dashboard.
- Ensure a valid remote session is configured by the SEA administrators.

Procedure

Step 1 Log in to the Cisco IoT Operations Dashboard as an SEA user.

Step 2 Click **Secure Equipment Access > Remote Sessions**.

Step 3 Go to the desire session and click **Connect**.

You are securely connected to the selected remote asset using the preconfigured access method. You can now monitor, manage, or troubleshoot the asset as required.

What to do next

Log out of your session when finished to maintain system security.

INDEX