



Deploy SEA Agents Using CLI commands

- [Deploy SEA agent on IE switches using CLI commands, on page 1](#)

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 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.