Quick Start Guide for Onboarding IE Switches to Cisco Secure Equipment Access

First Published: 2024-06-12

Last Modified: 2024-06-28

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

New and changed features

- Changes to this document, on page 1

Changes to this document

This table lists the technical changes made to this document since it was first published.

Table 1: Changes to this Document

Date	Change Summary
July 2024	Initial release of this document

CHAPTER 2

Overview

Objective

The purpose of this document is to assist new SEA administrators in onboarding their first Cisco IE network device to Cisco IoT Operations Dashboard and configuring the first remote session through Secure Equipment Acccess (SEA) service. Upon completion, the SEA administrator will be able to perform remote access to the required OT asset from an Internet-enabled device.

It's a self-contained quick start guide designed to provide the shortest and most efficient path to achieving the objective.

For more details and advanced concepts, refer to the main documentation.

Introduction

Cisco Secure Equipment Access (SEA) service aims to provide customers and partners with remote access to specific industrial IoT resources for performing maintenance operations.

Enabling SEA on the IE switch

To enable SEA on an IE switch and perform a remote session with the connected assets, do the following steps:

1. Create a device profile and add an IE switch to the Application Manager service, on page 5
2. Configure the IE switch and initiate a connection with the IoT Operations Dashboard, on page 9
3. Add an IE switch to the Secure Equipment Access service, on page 15
4. Configure remote sessions, on page 19

Prerequisites

- You must have a valid IoT OD organization (cloud tenant). If you don’t have one, send a request to mailto:iotod-account-request@cisco.com.
- You must have an Application Manager admin and SEA System admin roles in the organization.
- The IE switch has an SD card.
- The IE switch requires a minimum IOS-XE version of 17.14.1.
- The IE switch has connectivity to the Internet site us.ciscoiot.com or eu.ciscoiot.com, depending on the IoT OD cluster used.

CHAPTER 3

Create a device profile and add an IE switch to the Application Manager service

Create a device profile

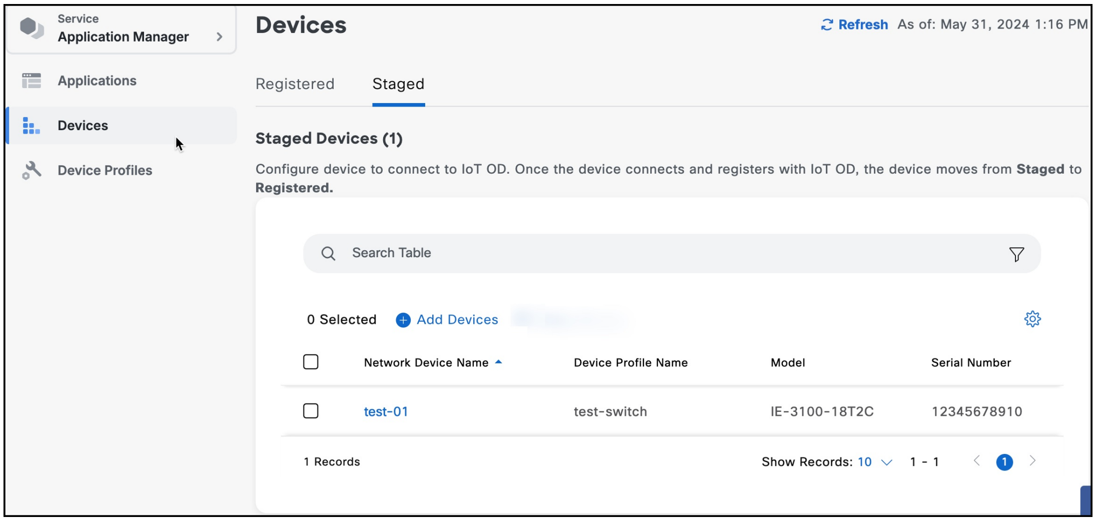
The device profile contains common settings such as user credentials. You can create a profile with the username and password credentials and link the profile to all devices that share these credentials. For more information, see device profile.

1. In the Cisco IoT Operations Dashboard, navigate to **Application Manager** service.
2. Go to **Device Profiles** and click the **Create Device Profile** link. The Create Device Profile page appears.
3. On the page, provide a name and description, and click **Next**.
4. Under **Configure credentials**, provide a user name and password for the device profile configuration.
5. Click **Next**. The created profile appears for your review.
6. On confirmation, click **Create Device Profile**. The created device profile is listed under **Device Profiles**.

Add and IE switch to App Manager service

After you create a device profile, you’re good to add an IE switch to the Application Manager service.

1. In the Cisco IoT Operations Dashboard, navigate to **Application Manager** service.
2. Click **Devices** > **Staged** tab.
3. Click **Add Devices**.
4. Select **Single Device** to open the **Add Device** page.
5. Click **Devices** > **Staged** > **Add Devices**.



Devices

As of: May 31, 2024 1:16 PM

Staged Devices (1)

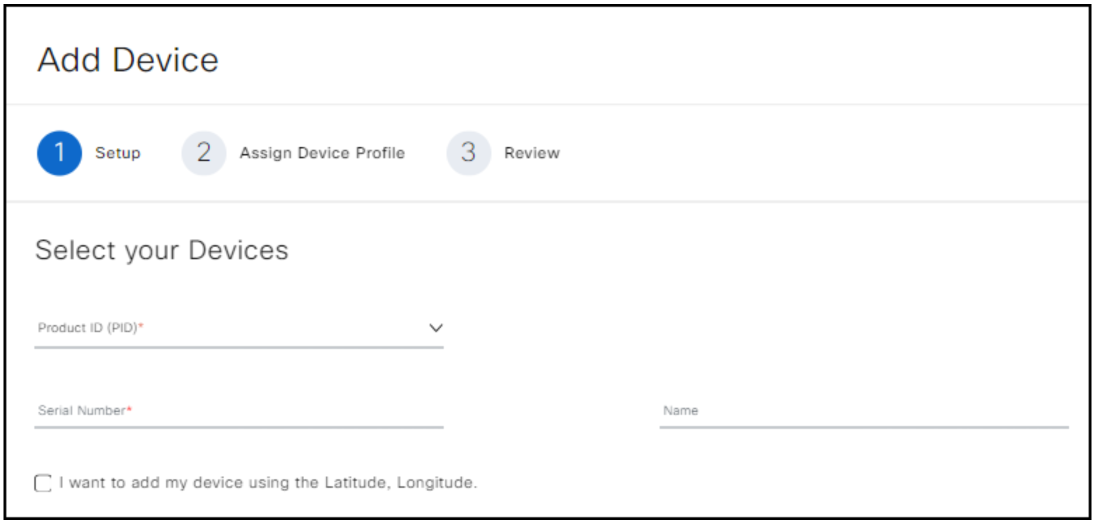
Configure device to connect to IoT OD. Once the device connects and registers with IoT OD, the device moves from **Staged** to **Registered**.

☐	Network Device Name	Device Profile Name	Model	Serial Number
☐	test-01	test-switch	IE-3100-18T2C	12345678910

1 Records

6. From the Select Add Device Method window, click **Single Device**.

7. On the Add Device page, enter the details such as product ID, serial number, and a name.



☐ I want to add my device using the Latitude, Longitude.

Use the following command to show the product ID and serial# for your device:

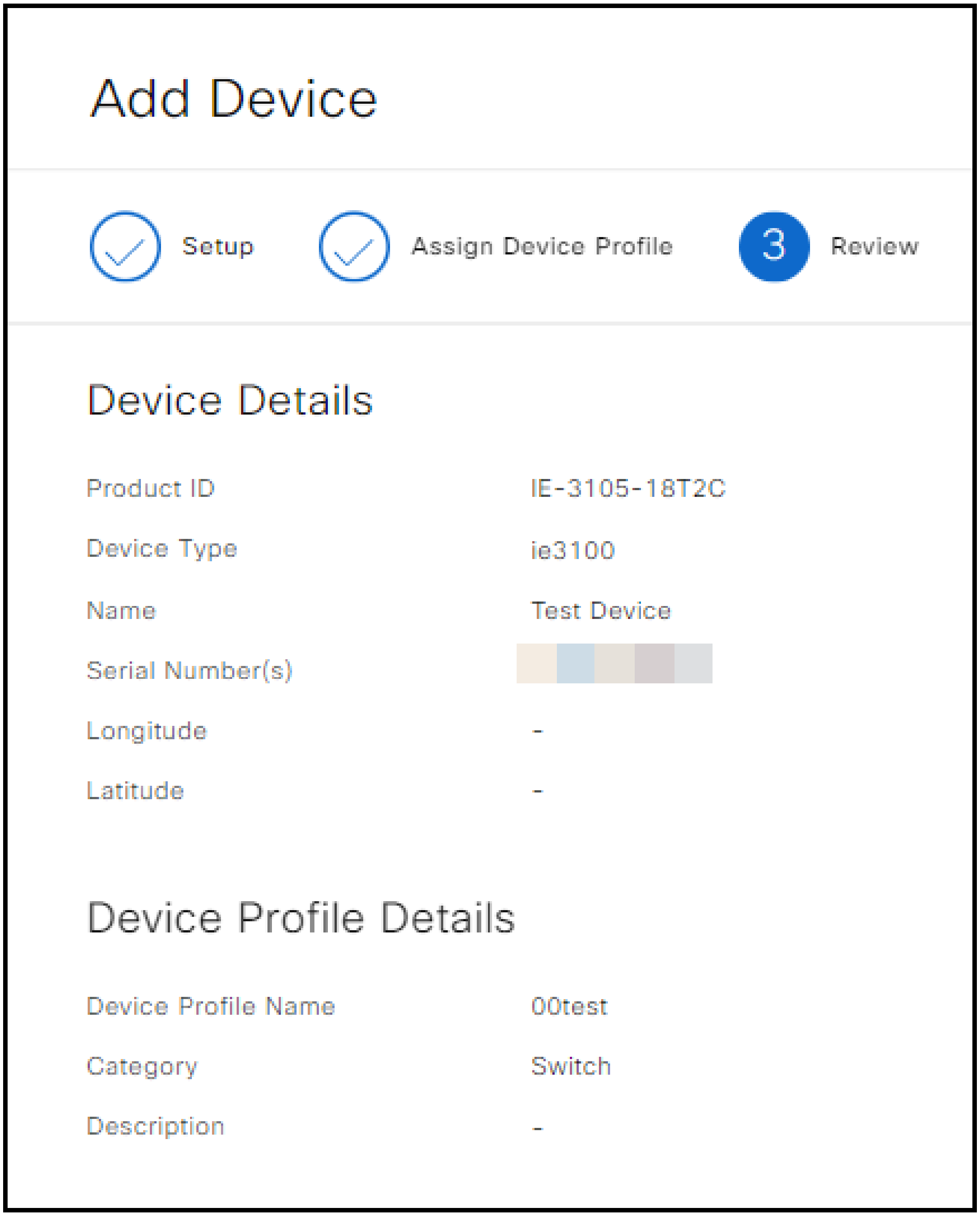
Switch# **show license udi**

The serial number and product ID can also be found on the identification sticker on the device and on the shipping box the device comes in.

8. Click **Next**.

9. In the **Select Device Profile for Assignment** screen, choose a device profile from the list and click **Next**.

10. Review the Configuration information on the Review screen.



Add Device

Device Details

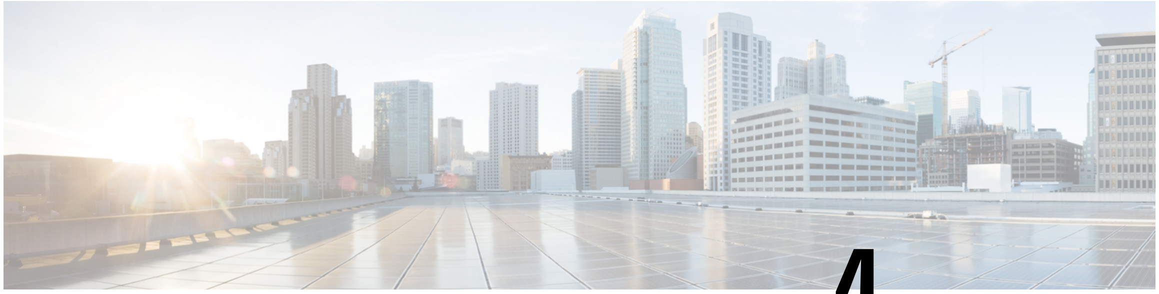
Product ID	IE-3105-18T2C
Device Type	ie3100
Name	Test Device
Serial Number(s)	[redacted]
Longitude	-
Latitude	-

Device Profile Details

Device Profile Name	00test
Category	Switch
Description	-

11. Click **Add Device**.

    You can see that the new device is listed under **Staged Devices**. This means that this device is added through the application manager but not registered with the IoT OD. The device is also not connected to the Cisco IoT Operations Dashboard yet.



CHAPTER 4

Configure the IE switch and initiate a connection with the IoT Operations Dashboard

Prerequisites for configuring the IE switch

- Ensure that the IE switch is added to the Cisco IoT OD Application Manager. For more information, see Create a device profile and add an IE switch to the Application Manager service.

Configuration steps

1. Prepare the device
2. Configure SD card and Enable IOx
3. Configure the IE3x00 Device to Connect to IoT OD
4. Verify the configuration on the device
5. Verify the device status in the IoT OD

Prepare the IE device

1. Attach the required networking cables.
2. Power up the device.

Configure SD card and enable IOx

IOx is a container hosting platform that runs on Cisco IOS XE, and 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). As a first step, we’ll now configure and enable IOx.

To work with IOx applications, the IE3x00 must have an SD card in the **ext4** format. However, the SD card that is ordered as part of the shipment will be in FAT32 format. Therefore, you must reformat the SD card to **ext4**.

Use the following command:

```
format sdflash: ext4
```

Do the following:

1. Configure AppGigabitEthernet1/1 in trunk mode. Cisco recommends that you configure this trunk with a native VLAN that isn’t likely to be used anywhere in the switch. It’s also possible, but not required, to allow on this trunk only the VLANs needed for communication from the applications and the internet or other VLANs. If using a native VLAN number greater than 1004 like the example below, make sure that the switch is configured for "vtp mode transparent" to allow for the creation of this VLAN. With this configuration, applications will be deployed in any desired VLAN you wish the application traffic to follow.

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

2. Enable IOx.

```
conf t
iox
end
```

3. Verify that IOx is running correctly.

   For example:

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

   The device displays an output similar to the following:

```
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
```

Configure the IE3x00 switch to connect to IoT OD

We’re now going to execute a set of IOS commands on the device's CLI to establish a connection with the Cisco IoT Operations Dashboard. The Device Profile in the IoT Operations Dashboard is associated with devices such as IE switches, with a set of username / passwords for managing them. 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. Apply the following configuration to create a privilege 15 user.

   The credentials should match the values configured in the Device Profile in 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.

Note Usage of the WSMA service relies on http, therefore "ip http server" is required to be enabled in the configuration. To deploy applications securely, add “ip http secure-server” as well. review running-config on the device first. Some related configurations might be available out of the box.

```
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, which can be accessed using port 443. If the device is exposed to the internet without enterprise firewall protection, it’s important to control access to this web service to prevent potential security risks. For more details on this issue and resolution, see Technote: Troubleshooting tips. For any assistance, please contact: Cisco TAC

3. Configure the IDA transport profile to 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 switch if it’s not already acquired through the DHCP server.

Note This is important if the switch is configured with a static IP and the static default gateway and not explicitly given a DNS server to use. In this example, we use a Cisco DNS. You can use any DNS server. To verify, execute the following commands:

Switch# **ping us.ciscoiot.com**

```
  Type escape sequence to abort.
  Sending 5, 100-byte ICMP Echos to 35.84.105.79, timeout is 2 seconds:
  .....
  Success rate is 0 percent (0/5)
```

Ping will fail and that is expected, however it’s important to validate that the hostname has been resolved to an IP address. The configured DNS server can be checked with "show ip dns view". If the DHCP server doesn’t provide DNS, a DNS must be explicitly configured in the device. An example is provided below:

```
conf t
  ip name-server 208.67.222.222 208.67.220.220
  end
```

Verify the configuration on the device

Ensure that the configuration steps are complete and the template from CLI is pushed to the switch. Use the following commands to verify that the device is configured correctly to connect to IoT OD.

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

The device displays an output similar to this. Notice the line *IDA Status: Connected*.

```
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
```

Verify the device status on the IoT Operations Dashboard

Once a device connects with a registration request, the device configuration is recognized and validated by IoT OD, and the device automatically moves from **Devices > Staged** status to Registered status in your IoT OD Organization.

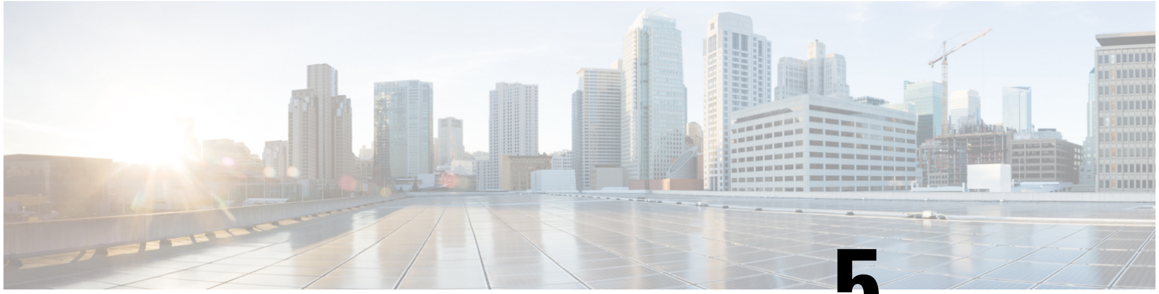
If IoT OD didn't receive any registration attempt, the IE3x00 device stays in the **Devices > Staged** list. Check the following on the device:

- Verify that the device has connectivity to the appropriate IoT OD cluster (US/EU) by using the telnet command.

  ```
  // Verify that opening a telnet session to the cluster is successful. The output should
   have "Open"

    Example:
    #telnet us.ciscoiot.com 443
    Trying us.ciscoiot.com (10.105.58.227, 443)... Open
  ```

- If you encounter problems, use the Event Log page on the device level to see the connectivity and Application Manager-related events. Use the troubleshooting tools on the device's Troubleshooting page for debugging.



CHAPTER 5

Add an IE switch to the Secure Equipment Access service

Overview

After you are done with configuring the IE switch to communicate with the Cisco IoT Operations Dashboard, you can add the device to SEA service.

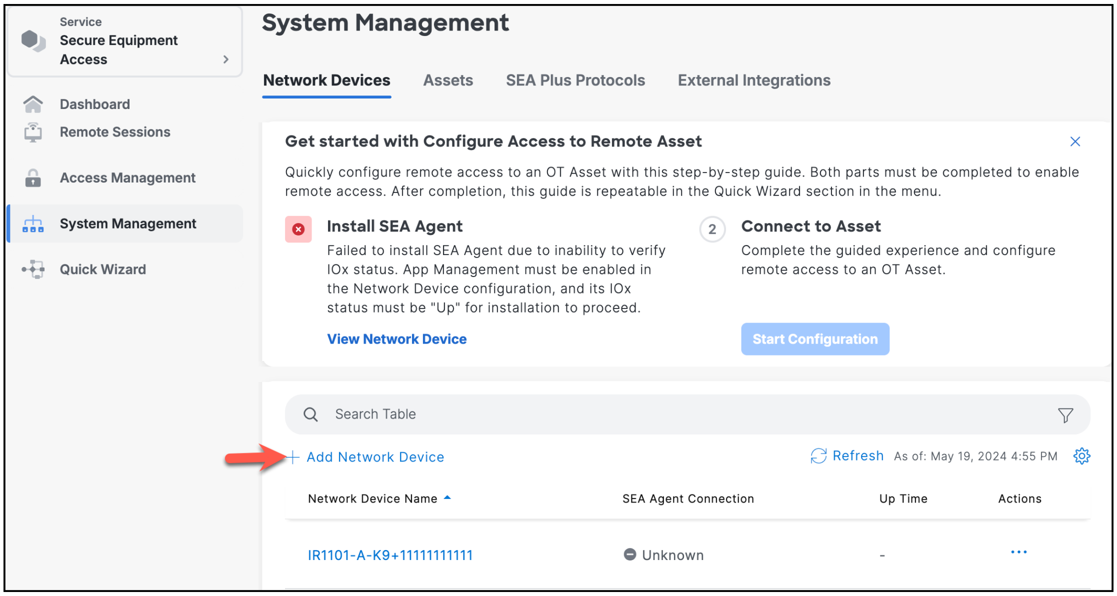
Note

- Only the SEA System Admin role can open the SEA Management menu option that provides secure remote communication to Network Devices or Assets.
- Cisco also provides a guided New User Workflow designed to help a first-time SEA System Admin to access a remote OT Asset in a few steps. For more information, see SEA: New User Workflow.
- For a more efficient means of installing and updating Network Devices or Assets, see SEA Quick Wizard.

Configuration steps

1. From the **Services** panel, choose **Secure Equipment Access** > **System Management** .

2. Under the **Network Devices** panel, click **Add Network Device**.



System Management

Get started with Configure Access to Remote Asset

Quickly configure remote access to an OT Asset with this step-by-step guide. Both parts must be completed to enable remote access. After completion, this guide is repeatable in the Quick Wizard section in the menu.

Install SEA Agent

Failed to install SEA Agent due to inability to verify IOx status. App Management must be enabled in the Network Device configuration, and its IOx status must be "Up" for installation to proceed.

2 Connect to Asset

Complete the guided experience and configure remote access to an OT Asset.

As of: May 19, 2024 4:55 PM

Network Device Name	SEA Agent Connection	Up Time	Actions
IR1101-A-K9+11111111111	Unknown	-	···

3. On the Add Network Device page:

   a. Choose a network device from the list or search for it in the **Search** field. Click **Next**.

   b. Enter a network device description, VLAN ID, and IP Assignment. For more information on the management VLAN and IP assignment configurations, see Multi-VLAN and Static IP support.

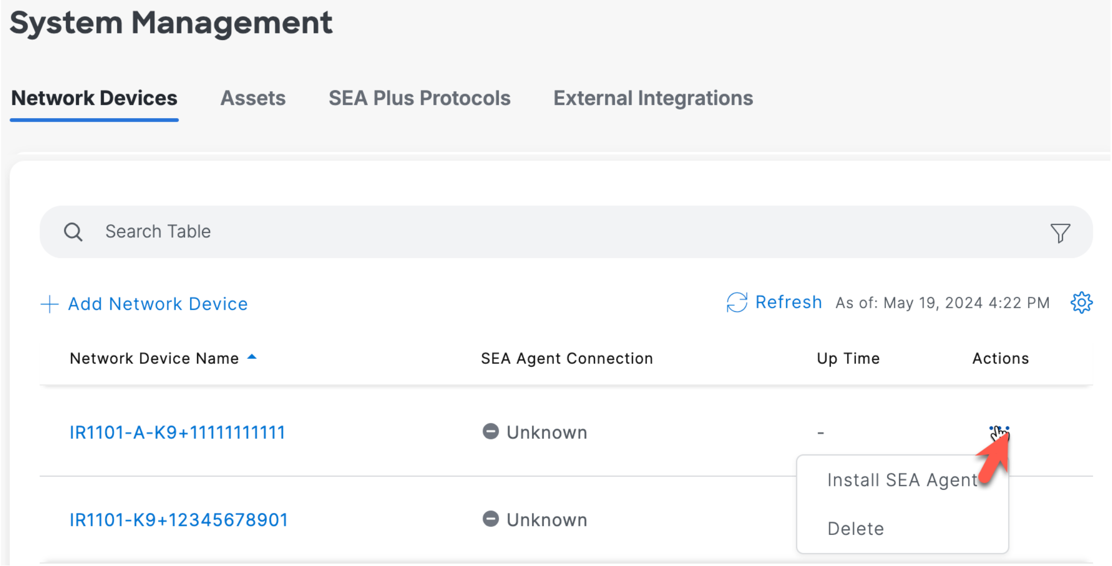
   c. Click **Add Network Device**.

   The installation of the SEA application starts.

4. Click **Next.** A confirmation box opens.

5. Check the SEA Agent **state of deployment** associated with the network device.

The **SEA Agent** deployment state changes to **Installed**. If the status doesn't change to installed, go to the network device listing and hover over the **3 dots** in the **Actions** column and choose **Install SEA Agent**.



System Management

Network Devices | Assets | SEA Plus Protocols | External Integrations

Search Table

+ Add Network Device

Refresh As of: May 19, 2024 4:22 PM

Network Device Name	SEA Agent Connection	Up Time	Actions
IR1101-A-K9+11111111111	Unknown	-	
IR1101-K9+12345678901	Unknown		

CHAPTER 6

Configure remote sessions

Overview

SEA Admins can use Secure Equipment Access (SEA) to remotely manage and interact with OT assets and network devices.

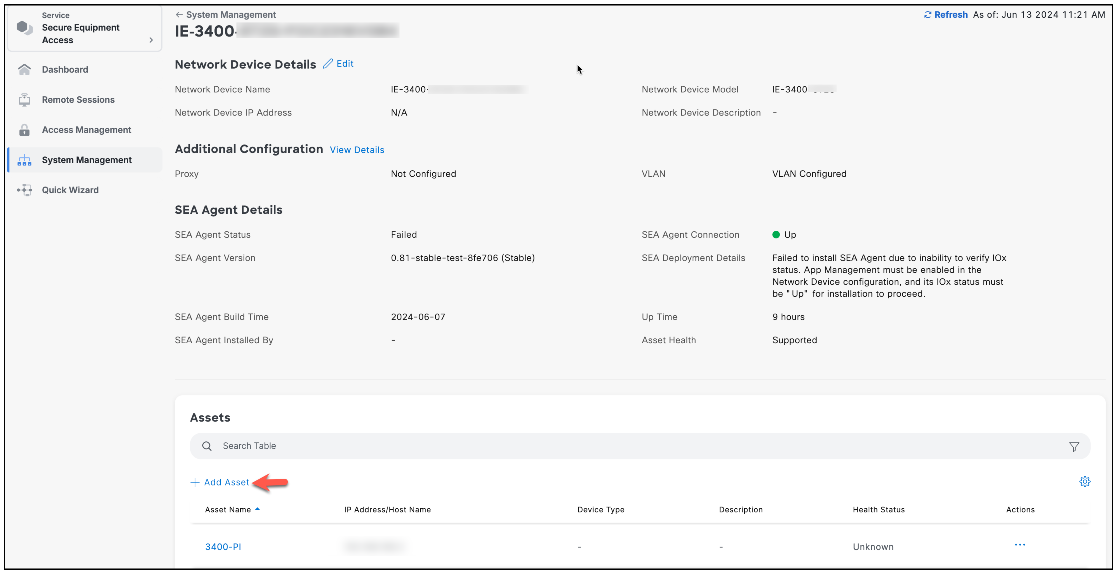
While SEA Admins create groups and manage access, SEA Users are granted access through specific access groups. The purpose of a group is to define which SEA Users can access which access methods. The SEA users will only be able to see the devices they have access to.

Configuring remote sessions includes the following steps:

1. Add OT assets to network devices, on page 19
2. Configure access methods for OT assets, on page 20
3. Create an access group and assign users to the group, on page 21
4. Assign assets to users in the group, on page 23
5. Connect to remote sessions, on page 24

Add OT assets to network devices

1. From the **System Management** screen, select the network device to which you want to add the OT asset.
2. From the **Network Device details** screen, click **Add Asset**. A page appears, displaying the **Network Device Details**, **SEA Agent Details**, and **Assets**.
3. On the page, under **Assets**, click **Add Asset**. The Add Asset page appears.



← System Management

IE-3400[redacted]

Refresh As of: Jun 13 2024 11:21 AM

Network Device Details Edit

Network Device Name	IE-3400[redacted]	Network Device Model	IE-3400[redacted]
Network Device IP Address	N/A	Network Device Description	-

Additional Configuration View Details

Proxy	Not Configured	VLAN	VLAN Configured

SEA Agent Details

SEA Agent Status	Failed	SEA Agent Connection	● Up
SEA Agent Version	0.81-stable-test-8fe706 (Stable)	SEA Deployment Details	Failed to install SEA Agent due to inability to verify IOx status. App Management must be enabled in the Network Device configuration, and its IOx status must be "Up" for installation to proceed.
SEA Agent Build Time	2024-06-07	Up Time	9 hours
SEA Agent Installed By	-	Asset Health	Supported

Assets

Search Table

+ Add Asset

Asset Name	IP Address/Host Name	Device Type	Description	Health Status	Actions
3400-PI	[redacted]	-	-	Unknown	···

4. On the page, select **Manual entry** from the **Selection Method**, and provide the name and IP address/host name of the asset.

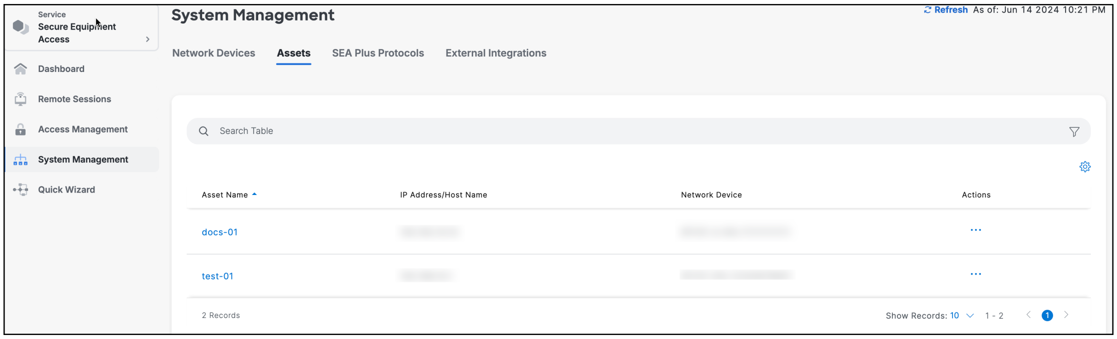
5. Click **Add**.

   The newly added asset is listed under the **Assets** section.

Configure access methods for OT assets

After you add an OT asset, you can configure an access method to connect with the asset. SEA provides various access methods such as SSH, RDP, VNC, Web App, and Telnet to configure SEA-connected clients. For more information on the access methods, see Access Methods.

1. Go to **Secure Equipment Access** > **System Management** > **Assets**.



System Management

Refresh As of: Jun 14 2024 10:21 PM

Network Devices | Assets | SEA Plus Protocols | External Integrations

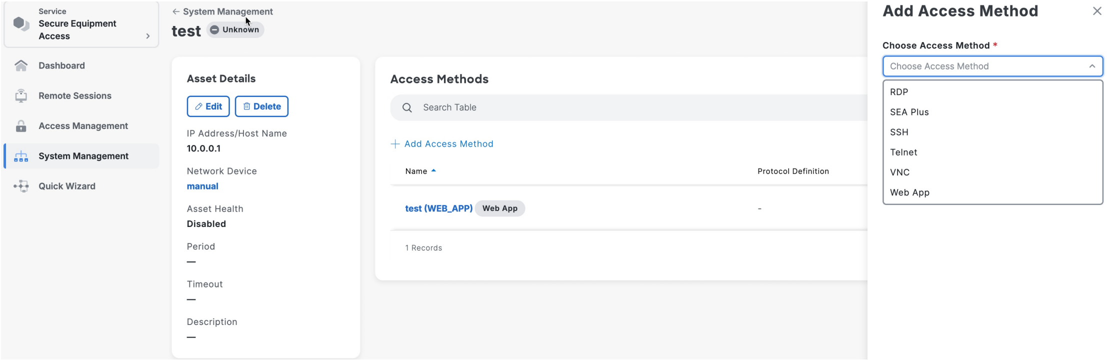
Search Table

Asset Name	IP Address/Host Name	Network Device	Actions
docs-01	[redacted]	[redacted]	···
test-01	[redacted]	[redacted]	···

2 Records Show Records: 10 1 - 2 1

2. Click the name of the asset for which you want to configure the access method. The asset details appear.

3. Under **Access Methods**, click **Add Access Method** and select an access method from the list.



4. Provide the specific details relating to the access method that you selected, and then click **Add**.

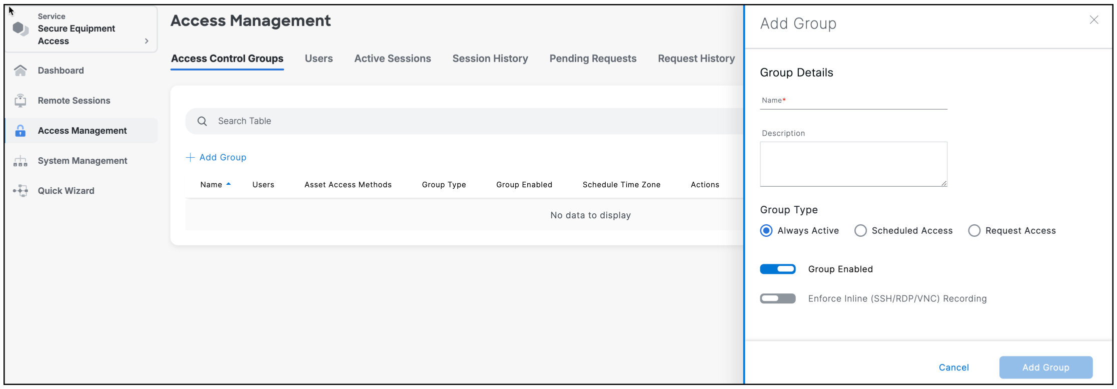
   The access method is listed under **Access Methods**.

Create an access group and assign users to the group

An access group is a collection of users who need access to specific OT assets within the group. You can add multiple users and OT assets to the access group.

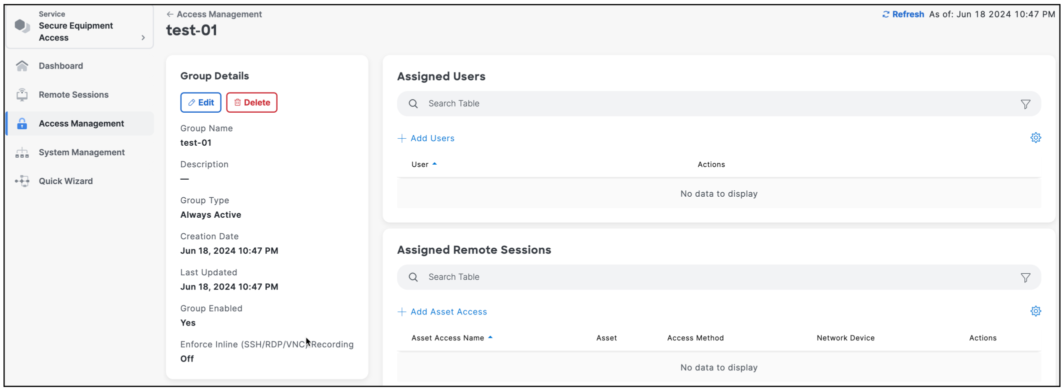
Do the following steps:

1. From the **Secure Equipment Access** > **Access Management** screen, click **Add Group**. The Add Group window appears.



2. On the window, provide the following details:

   - Name of the group you want to add.
   - A description to the group
   - Select **Always Active** from the **Group Type**.
   - Leave the **Group Enabled** option enabled.
   - Click **Add Group**. The details of the added group appear.



← Access Management

test-01

As of: Jun 18 2024 10:47 PM

Group Details

Group Name: test-01

Description: —

Group Type: Always Active

Creation Date: Jun 18, 2024 10:47 PM

Last Updated: Jun 18, 2024 10:47 PM

Group Enabled: Yes

Enforce Inline (SSH/RDP/VNC) Recording: Off

Assigned Users

Search Table

User	Actions
No data to display	

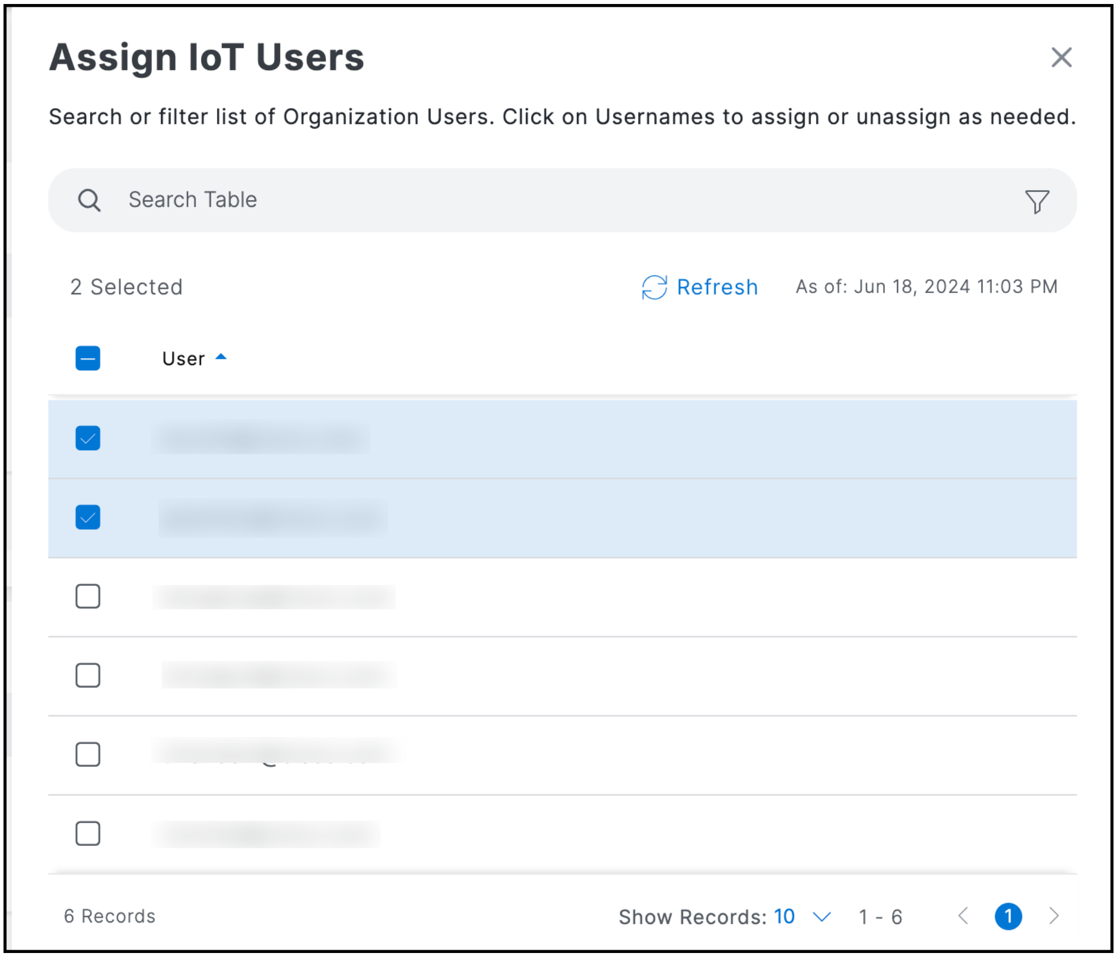
Assigned Remote Sessions

Search Table

Asset Access Name	Asset	Access Method	Network Device	Actions
No data to display				

3. Under **Assigned Users,** click **Add Users**. The Assign IoT Users window appears.

4. On the window, select one or more users from the list, and click **Save**.



Assign IoT Users

Search or filter list of Organization Users. Click on Usernames to assign or unassign as needed.

Search Table

2 Selected

As of: Jun 18, 2024 11:03 PM

6 Records

1 - 6

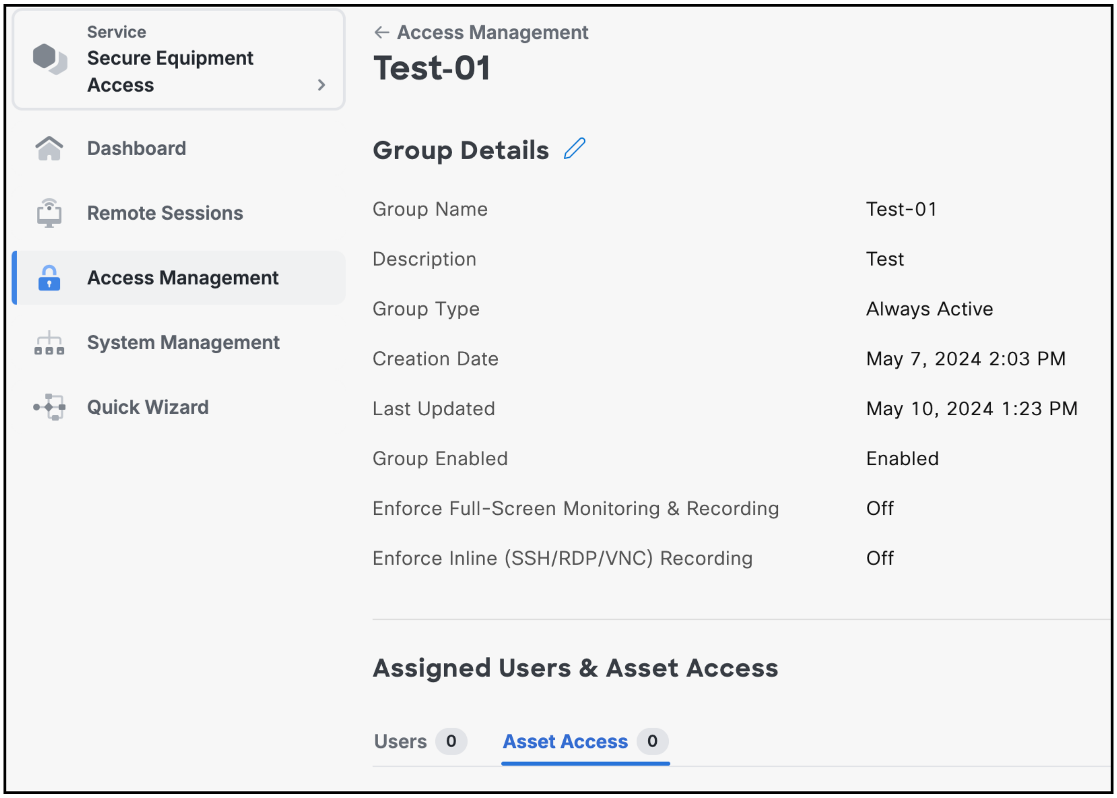
The added users are listed under **Assigned Users**

Assign assets to users in the group

SEA administrators can assign assets to group members.

1. Click **Secure Equipment Access** > **Access Management**.
2. On the Access Management page, click the name of the group.

   The Group Details page appears.
3. On the Group Details page, under **Assigned Users & Asset Access**, click **Asset Access**.
4. Click **Add Asset Access**. The Assign Asset Access page appears.



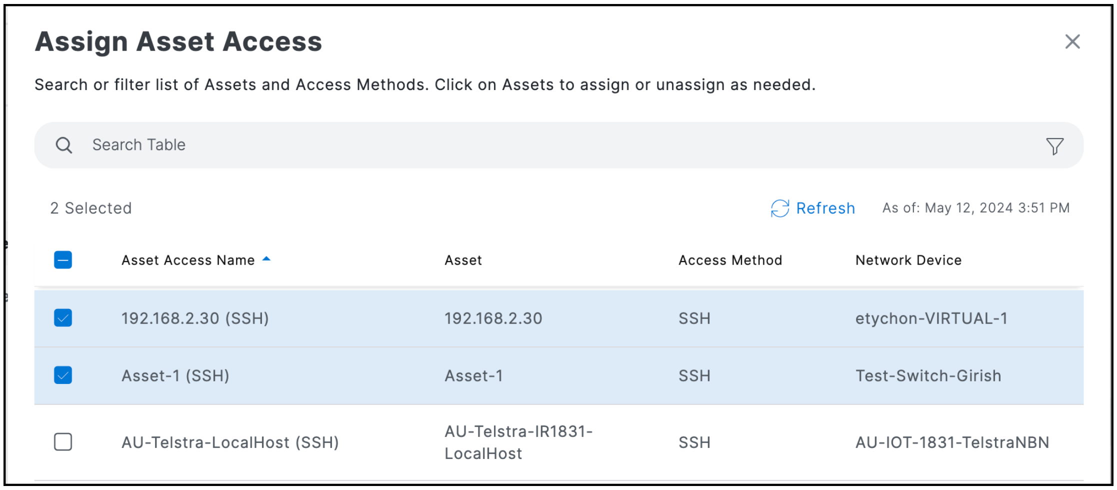
Test-01

Group Details

Group Name	Test-01
Description	Test
Group Type	Always Active
Creation Date	May 7, 2024 2:03 PM
Last Updated	May 10, 2024 1:23 PM
Group Enabled	Enabled
Enforce Full-Screen Monitoring & Recording	Off
Enforce Inline (SSH/RDP/VNC) Recording	Off

Assigned Users & Asset Access

5. On the Assign Asset Access page, select one or more assets from the list.



Assign Asset Access

Search or filter list of Assets and Access Methods. Click on Assets to assign or unassign as needed.

	Asset Access Name	Asset	Access Method	Network Device
☑	192.168.2.30 (SSH)	192.168.2.30	SSH	etychon-VIRTUAL-1
☑	Asset-1 (SSH)	Asset-1	SSH	Test-Switch-Girish
□	AU-Telstra-LocalHost (SSH)	AU-Telstra-IR1831-LocalHost	SSH	AU-IOT-1831-TelstraNBN

6. Click **Save**.

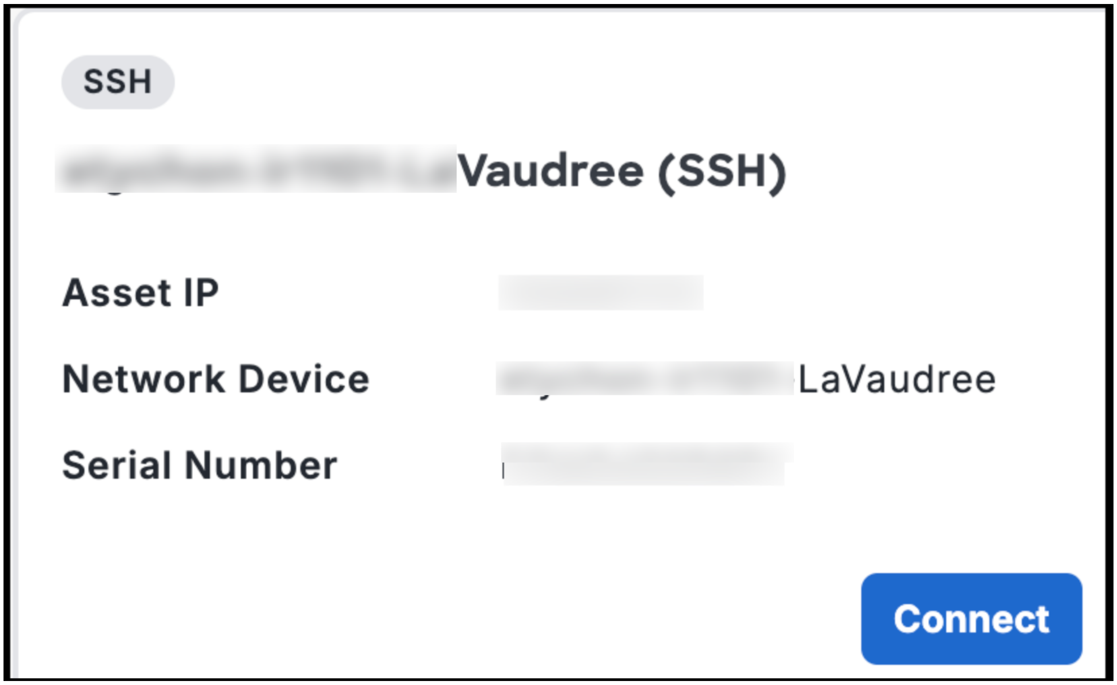
   The sessions appear under **Secure Equipment Access** > **Remote Sessions** when an SEA user logs in to IoT OD.

Connect to remote sessions

SEA users can connect to remote sessions after SEA Admins configure the sessions for them.

1. Log in as an SEA user.
2. Click **Secure Equipment Access** > **Remote Sessions**.

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



[redacted]Vaudree (SSH)

Asset IP [redacted]

Network Device [redacted]LaVaudree

Serial Number [redacted]

INDEX