



Configure remote sessions

- [Overview, on page 1](#)
- [Add OT assets to network devices, on page 1](#)
- [Configure access methods for OT assets, on page 2](#)
- [Create an access group and assign users to the group, on page 3](#)
- [Assign assets to users in the group, on page 5](#)
- [Connect to remote sessions, on page 6](#)

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 1](#)
2. [Configure access methods for OT assets, on page 2](#)
3. [Create an access group and assign users to the group, on page 3](#)
4. [Assign assets to users in the group, on page 5](#)
5. [Connect to remote sessions, on page 6](#)

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.

The screenshot shows the 'System Management' page for asset 'IE-3400'. The left sidebar includes 'Service Secure Equipment Access', 'Dashboard', 'Remote Sessions', 'Access Management', 'System Management', and 'Quick Wizard'. The main content area is divided into sections: 'Network Device Details' (Network Device Name: IE-3400, IP Address: N/A, Model: IE-3400, Description: -), 'Additional Configuration' (Proxy: Not Configured, VLAN: VLAN Configured), and 'SEA Agent Details' (Status: Failed, Version: 0.81-stable-test-8fe706 (Stable), Connection: Up, 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. Up Time: 9 hours, Asset Health: Supported). Below these sections is an 'Assets' table with a search bar and a '+ Add Asset' button highlighted with a red arrow. The table has columns for Asset Name, IP Address/Host Name, Device Type, Description, Health Status, and Actions. One asset is listed: '3400-PI' with IP Address/Host Name, Device Type, Description, Health Status (Unknown), and Actions.

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

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

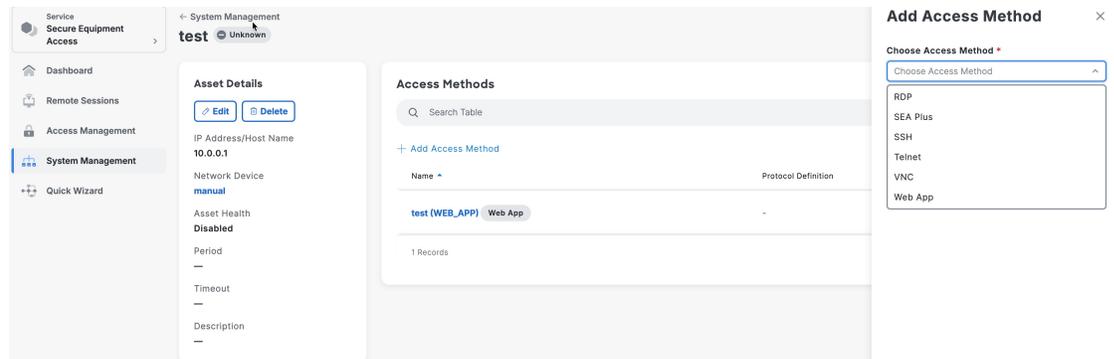
Configure access methods for OT assets

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](#).

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

The screenshot shows the 'System Management' page with the 'Assets' tab selected. The page has a search bar and a table with columns: Asset Name, IP Address/Host Name, Network Device, and Actions. Two assets are listed: 'docs-01' and 'test-01'. At the bottom, it shows '2 Records' and a 'Show Records' dropdown set to 10.

- Click the name of the asset for which you want to configure the access method. The asset details appear.
- Under **Access Methods**, click **Add Access Method** and select an access method from the list.



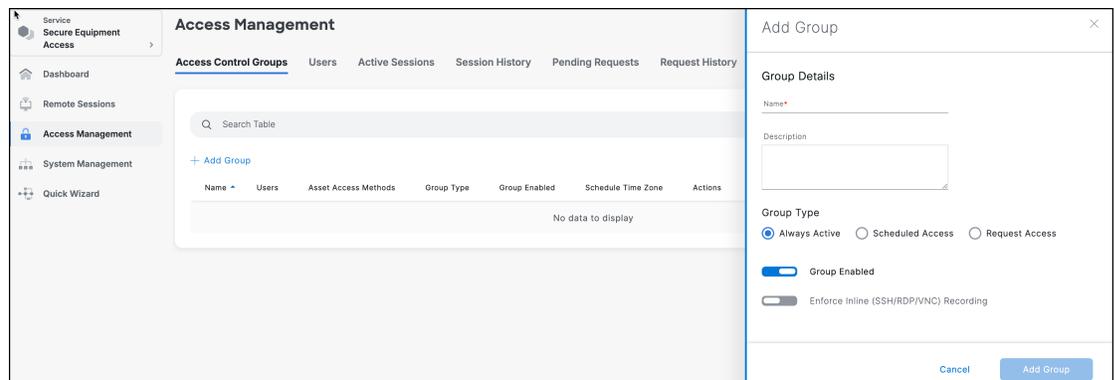
4. Provide the specific details relating to the access method that you selected, and then click **Add**.
The access method is listed under **Access Methods**.

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.

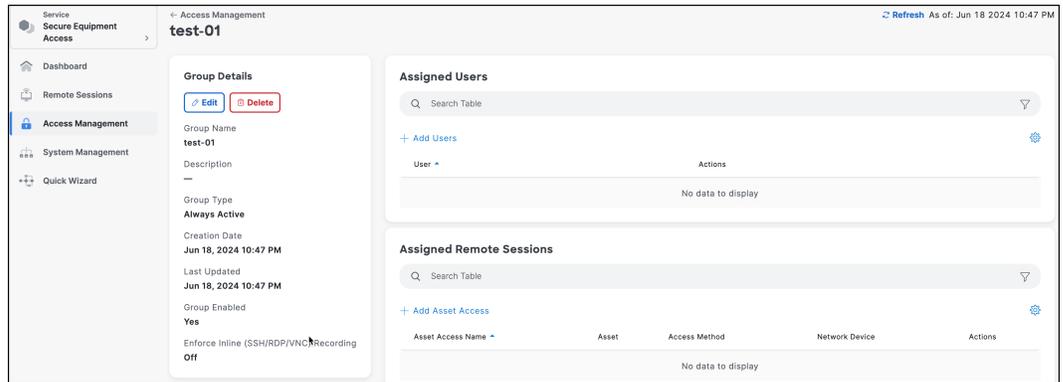
Do the following steps:

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

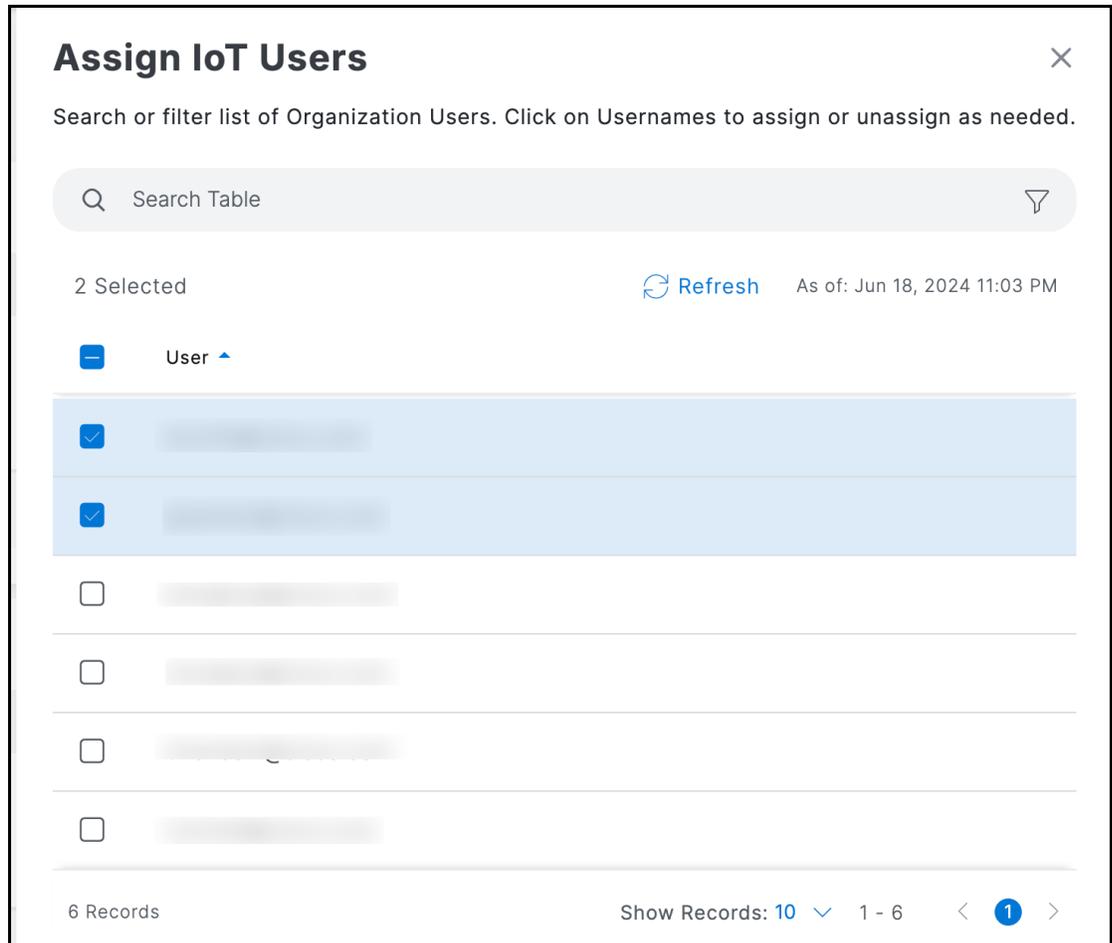


2. On the window, provide the following details:
 - Name of the group you want to add.
 - A description to the group
 - Select **Always Active** from the **Group Type**.
 - Leave the **Group Enabled** option enabled.
 - Click **Add Group**. The details of the added group appear.

Create an access group and assign users to the group



- Under **Assigned Users**, click **Add Users**. The Assign IoT Users window appears.
- On the window, select one or more users from the list, and click **Save**.



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.

The screenshot displays the 'Group Details' page for a group named 'Test-01'. The page is part of the 'Access Management' section under 'Secure Equipment Access'. The left sidebar contains navigation options: Dashboard, Remote Sessions, Access Management (selected), System Management, and Quick Wizard. The main content area shows the group name 'Test-01' and a 'Group Details' section with the following information:

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

Below the group details is the 'Assigned Users & Asset Access' section, which shows 'Users' with a count of 0 and 'Asset Access' with a count of 0. The 'Asset Access' link is highlighted in blue.

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.

2 Selected [Refresh](#) As of: May 12, 2024 3:51 PM

	Asset Access Name ▲	Asset	Access Method	Network Device
<input checked="" type="checkbox"/>	192.168.2.30 (SSH)	192.168.2.30	SSH	etychon-VIRTUAL-1
<input checked="" type="checkbox"/>	Asset-1 (SSH)	Asset-1	SSH	Test-Switch-Girish
<input type="checkbox"/>	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**.

SSH

Vaudree (SSH)

Asset IP

Network Device LaVaudree

Serial Number

Connect

