



Remote Sessions Configurations

- [Install SEA agent on industrial routers, on page 1](#)
- [Configure remote sessions, on page 2](#)
- [Connect to remote assets, on page 3](#)

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.

