



Manage access control groups for remote access

- [Access control groups, on page 1](#)

Access control groups

An access control group is a security feature that provides administrators with the ability to define and manage secure remote access for groups of SEA users to specific remote assets.

- Provides granular control over who can access what and when.
- Enables creation of groups and assignment of permissions for remote access.
- Supports multiple access control group types for flexible access management.

Types of access control groups

There are three types of access control groups you can configure:

- **Always Active** – users in this group can always access the access methods defined in this group.
- **Scheduled Access** – users in the group can access remote assets for the configured duration.
- **Request Access** – Users must explicitly request access to the remote assets. They can access the assets only after the Access manager (approver) approves the requests.

How remote session access requests work

Remote session access requests allow organizations to control access to OT assets securely and according to policies, using the IoT Operations Dashboard.

Summary

Actors and components participate in the remote session access request process:

- **SEA System Admin** or **SEA Access Admin** : Creates and configures access groups with request controls.
- **Remote access user** : Requests access to the asset via the dashboard.
- **SEA Access Manager** (or other approvers): Reviews and approves or rejects access requests.

- **IoT Operations Dashboard** : Hosts the interfaces for all actions.

This process ensures that only authorized users can access assets. All actions are subject to approval and audit.

Workflow

These stages describe how remote session access requests are processed:

1. The SEA System Admin or SEA Access Admin logs in to the IoT Operations Dashboard and creates an access control group with the "Request Access" feature enabled. At least one SEA user and one asset must be assigned to the group.
2. The remote access user logs in and requests access to an asset within an enabled group.
3. The SEA Access Manager, or other permitted roles such as the SEA System Admin, SEA Access Admin, or any role with 'Access Approver' permission, reviews and either approves or rejects the access request.
4. Upon approval, the remote access user gains access to the asset for the specified time period.

Result

The system enforces policy-driven, auditable, and time-bound access for OT assets, minimizing the risk of unauthorized usage.

Create an access control group for remote access

Set up control over remote access by grouping users and assets under defined access conditions.

Create access control groups in the Secure Equipment Access (SEA) system to define which users can access specific remote assets and under what conditions.

Before you begin

- Ensure you have either an **SEA System Admin** or **SEA Access Admin** role.

Procedure

Step 1 From the left **Service** panel, choose **Secure Equipment Access > Access Management**.

Step 2 On the **Access Management** page, view the **Access Control Groups** table.

The **Access Control Groups** table lists the available access control groups, including the group name and the number of users assigned to each group. You can search for a specific group in the **Search** field at the top of the table.

Step 3 Click **Add Group**.

Step 4 On the **Add New Access Control Group** page, configure the group details:

- a) Enter the name of the access group in the **Name** field.
- b) (Optional) Enter a brief description about the access group in the **Description** field.
- c) Choose a group type in the **Group Type** section depending on the remote session you want to configure.

For more information, refer to Cisco DevNet documentation on [Request access to a remote session](#) and [Manage access control groups for remote access](#).

- d) (Optional) Click the **Group Enabled** toggle switch if you want to disable the group. By default, the group is enabled. If you disable it, the SEA users can't access remote sessions in the group.

Note

Disable a group during situations such as device upgrades or repairs, when the Access Admin does not want access to certain remote sessions. When you disable a group, the group won't be listed in the Access Sessions screen.

- e) (Optional) Click the **Enforce Inline (SSH/RDP/VNC) Recording** toggle switch to enforce inline recording. By default, it's disabled.

Step 5 Click **Next**.

Step 6 (Optional) In the **Assign Users** section, choose the users from the list who you want to add to the group, and click **Next**.

Step 7 (Optional) In the **Assign Remote Sessions** section, choose the assets you want the SEA users to access.

Step 8 Click **Save**.

The system creates a new access control group with defined settings. Assigned users and assets can be managed from the group's details page.

Add users to an access control group

Add users to an existing access control group to grant them remote access permissions.

Group membership can be updated after creation to provide selected users with the necessary access permissions.

Before you begin

- Confirm that you have either the SEA System Admin or SEA Access Admin role.

Procedure

Step 1 From the **Service** panel, select **Secure Equipment Access > Access Management**.

Step 2 Select the desired access control group.

Step 3 Click **Add Users** in the **Users** tab.

Step 4 Select the users to add to the group, then click **Save**.

Note

If the required user is not listed, add them through SEA System Management. Contact your SEA System Admin for help.

The selected users become members of the access control group.

Add asset access to an access group

Use this task to define asset access for group members. After assets are assigned, users can view remote sessions in the IoT Operations Dashboard. Connection rights may depend on further approval.

Procedure

-
- Step 1** From the left **Service** panel, choose **Secure Equipment Access > Access Management**.
 - Step 2** Choose a **group** from the Access Management page.
 - Step 3** Click **Asset Access** tab. Click **Add Asset Access**.
 - Step 4** Select **Assets** from the list. Click the **checkbox** next to each asset.
-

Group members can now view the designated remote sessions for the assigned assets in the IoT Operations Dashboard. They cannot connect to the remote sessions until further approval is granted, according to group policy.

What to do next

You can optionally assign a specific approver for the access request. If approvers are assigned, they will be responsible for reviewing and approving the request.

If no approver is assigned, all admins in your organization will receive email notifications. Any SEA Access Admin or SEA System Admin can review and approve the request.

Assign approvers to an access control group

Ensure each request for access in “Request Access” groups is explicitly reviewed and approved, as required.

Before you begin

The approver must have the **Access Admin** or **Access Manager** role.

Procedure

-
- Step 1** From the **Service** panel, choose **Secure Equipment Access > Access Management**.
 - Step 2** On the **Access Management** page, click the name of the access group created for the **Request Access** feature.
A page appears displaying the **Assigned Users**, **Assigned Remote Sessions**, and **Access Approvers** sections.
 - Step 3** In the **Access Approvers** section, click **Add access Approver**.
 - Step 4** In the **Add access Approver** window, select an approver from the available list, and click **Save**.
-

When an SEA user in the group requests access to a session, the selected approvers receive an email notification. Tenant admins do not receive the email notification unless they are explicitly selected as approvers. Approvers can log in to the IoT Operations Dashboard to manage access requests.

Create access control groups for scheduled access

Use this task to set up control over remote access by grouping users and assets under defined access conditions.

Creating access control groups in Secure Equipment Access enables you to manage and restrict which users can access specific remote assets and set conditions for their access. You may choose to disable a group temporarily during device upgrades, repairs, or other situations where access should be restricted.

Before you begin

- Ensure you have either an **SEA System Admin** or **SEA Access Admin** role.

Procedure

-
- Step 1** From the **Service** panel, choose **Secure Equipment Access > Access Management**.
- Step 2** On the **Access Management** page, review the **Access Control Groups** table.
- The **Access Control Groups** table lists the available access control groups and their details such as the name of the group and the number of users assigned to the group.
- Step 3** Click **Add Group**.
- Step 4** On the **Add New Access Control Group** page, configure the group details:
- a) Enter a name for the access group.
 - b) (Optional) Enter a brief description about the access group.
 - c) Choose **Scheduled Access** in the **Group Type** section.
 - d) (Optional) Click the **Group Enabled** toggle switch if you want to disable this group. If you disable it, the SEA users can't access remote sessions in the group.
 - e) (Optional) Click the **Enforce Inline (SSH/RDP/VNC) Recording** toggle switch to enforce recording of the remote session that is configured in the access control group. The recording happens when a remote user accesses the remote session. By default, it's disabled.
 - f) Select a time zone for the group. The time zone selected ensures that access times are accurately set according to the group's regional time.
 - g) Specify the date and time when the group's scheduled access window begins.
 - h) Specify the end of the access window for the group on the specified date.
- Step 5** (Optional) In the **Assign Users** section, choose the users from the list who you want to add to the group, and click **Next**. Users selected here are authorized to access the remote sessions assigned to the group.
- Step 6** (Optional) In the **Assign Remote Sessions** section, choose the assets you want the users to access., and click **Next**.
-

- A new access control group is created with the defined settings.
- You can view the configured access window in the **Schedule** column on the **Access Control Groups** tab.
- Group members can view the designated remote sessions for the assigned assets in the IoT Operations Dashboard.

What to do next

- Members in this group can access the configured remote sessions during the configured time window.

Schedule statuses

The schedule status is a session attribute. It indicates the current access state for a remote session, determines when remote access is available, and distinguishes between ongoing, scheduled, active, and expired session availability.

- Indicates the current access state for a remote session.
- Determines when remote access is available.
- Distinguishes between ongoing, scheduled, active, and expired session availability.

Schedule Statuses in SEA Access Management

When you open the **SEA Access Management** screen and choose **Access Control Groups**, the Schedule Status column displays four possible statuses for a remote session.

- **Always Active** : No specific time for access; access is always available.
- **Scheduled** : A specific time span for access to a session has been scheduled for a future date.
- **Active** : The scheduled time for access to a session is currently in progress.
- **Schedule Expired** : The scheduled time for access to a session has expired.



Note If a scheduled session is listed as **Schedule Expired**, you can update that expired session for a future date without creating a new scheduled session.

Invite group members to a scheduled meeting

Invite some or all group members to participate in scheduled remote access sessions.

Before you begin

- You must have either an SEA System Admin or SEA Access Admin role.

Procedure

- Step 1** Choose the group with the scheduled meeting.
- Step 2** In the **Actions** column, choose **Send Invitation** from the drop-down list.
- Step 3** To select specific members, tick the checkbox next to each user's name.
- Step 4** Click **Send Invitation**.

Each chosen member receives an email notification with the meeting details.

Modify a remote session

Only sessions viewed in List View can be modified.

Procedure

- Step 1** Hover over the **3 dots** in the **Actions** column.
 - Step 2** Click **Edit**. The **Session Details** panel opens.
 - Step 3** Click the **Edit** icon and edit the session details.
 - Step 4** Click **Close** to save your changes.
-

Session details are updated according to your changes.

