Delegated Administration

If you have opted to use delegated administration, you will be provided with access to a parent organization and two or more subsidiary organizations in Cisco ScanCenter. No traffic is passed via the parent organization, but any policies set there will be applied to all subsidiary organizations. Policies set at the subsidiary level will be applied only to that specified subsidiary organization.

- Logging In to the Parent Organization, on page 1
- Enabling Subsidiary Organizations to Create Certificates, on page 1
- Enabling Subsidiary Organizations to Set Policies, on page 2
- Managing Exported and Imported Policy, on page 4
- Managing Filters, Schedules, and Dictionaries, on page 5
- Setting Global and Local User Messages, on page 5
- Configuring Email Domains, on page 5
- Running Audits, on page 5
- Delegated Reporting, on page 5
- Threat Analysis Role, on page 6

Logging In to the Parent Organization

When you log in to the parent organization with the administrator password, the Delegated Administration page is displayed. The parent and child companies are displayed with their associated Seats and Last Use date.

Note

This view of child accounts while logged in to their parent account is only available to Company Super User and Full Access administrators.

Enabling Subsidiary Organizations to Create Certificates

To enable subsidiary organizations to set their own HTTPS Inspection policy, it is necessary to enable them to create their own certificates.
### Enabling Subsidiary Organizations to Set Policies

Policies set at the parent organization are applied automatically to subsidiary organizations but can only be viewed at the parent. Creating and activating an **Execute Subsidiary Policy** rule, enables subsidiary organizations to apply their own policies. The subsidiary rules will be applied after parent rules with a higher priority but before parent rules with a lower priority.

Only the parent organization can edit the approved list of potentially unwanted programs.

#### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to the parent organization as administrator.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>On the Delegated Administration page, click the parent organization.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Rule Action pull-down list, select Execute Subsidiary Policy.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Create Rule. You can create only one rule of this kind.</td>
</tr>
</tbody>
</table>
Step 6  Select the Active check box to enable the **Execute Subsidiary Policy** rule action. This rule represents the policies set at each subsidiary organization.

Step 7  In the Move column, click the up and down arrows to set the order in which the parent and subsidiary policies will be applied.

Step 8  Click **Apply Changes**. The order will be updated.

Clearing the Active check box or removing the **Execute Subsidiary Policy** rule will prevent the subsidiary policies from being used.

---

### Enabling HTTPS Inspection

#### Before you begin

Create and activate an **Execute Subsidiary Policy** rule to enable subsidiary organizations to apply their own policies. See **Enabling Subsidiary Organizations to Set Policies**, on page 2.

#### Procedure

**Step 1** Log in to the parent organization as administrator.

**Step 2** On the **Admin > HTTPS Inspection > Policy** page, click **Create HTTPS Rule**.

**Step 3** In the **Certificate** pull-down list, select **Execute Subsidiary Policy**.

**Step 4** Select the Active check box to enable the rule action. Alternatively, clear the check box to activate the rule at another time.

**Step 5** Click **Submit** to apply your changes. Alternatively, click **Cancel** or navigate away from the page to abandon your changes.

---

### Subsidiary Privacy Policy

When delegated administration is enabled, it is possible for subsidiary organizations to set their own privacy policy.

As with all subsidiary policies, the privacy policy will be active only when the Active check box is selected.
Regardless of the priority assigned to the Execute Subsidiary Policy rule action, any subsidiary privacy policy will be applied immediately after the parent organization’s privacy rule actions.

**Note**

To enable a subsidiary organization to set its own HTTPS policy, the Execute Subsidiary Policy rule must be applied to the HTTPS inspection rule at the parent organization.

---

**Managing Exported and Imported Policy**

An exported policy can be shared for import between parent and child companies, both within and outside of the same delegated administration family.

When importing an exported child policy into:

- The same child company:
  - Any links to parent filters or schedules will remain intact.
  - All exported data will be imported.

- A different child company within the same delegated administration family:
  - Any links to parent filters or schedules will remain intact.
  - All exported data, except for license keys and HTTPS certificates, will be imported.

- A different child company in a different delegated administration family is supported only if the child company does not have any links to its parent company.

When importing an exported parent policy within the same company:

- All exported data will be imported.
- Any child policy links to the parent filters, schedules, or certificates will remain intact.
- Any new filter, schedule, or certificate that has been added since the export and is currently in use by any child company, will not be removed. Effectively results in a merge with the contents of the export being imported.
- Any new filter, schedule or certificate that has been added since the export and is not currently in use by any child company, will be removed and replaced by the contents of the export being imported.

Importing to a different parent company in a different delegated administration family is supported, but:

- Any company, group, or user license keys will be removed.
- Any HTTPS certificates will be removed.

See **Backing Up a Policy** and **Restoring a Policy** for details on how to export and import a policy.
Managing Filters, Schedules, and Dictionaries

The filters, schedules, and dictionaries of the parent organization are available at the subsidiary organizations. There they can be viewed and used, but not edited. Filters, schedules, and dictionaries created at the subsidiary organization will not be available at the parent or other subsidiary organizations.

Setting Global and Local User Messages

By default any user messages set at the parent organization will be inherited by the subsidiary organizations.

Procedure

Step 1 Log in to the subsidiary organization as an administrator.
Step 2 Navigate to the required User Messages page.
Step 3 Clear the Inherit Master alert page settings check box.
Step 4 Enter the required message in the box.
Step 5 Click Save to apply your changes.

Configuring Email Domains

Email domains configured at the parent organization are available at every subsidiary organization. This enables you to create an organization-wide email domain. Email domains configured at the subsidiary organization are only available at that organization.

Running Audits

Audits run at a subsidiary organization will only include information for that organization.

Delegated Reporting

Reports run at the parent organization will include results for all of the subsidiary organizations. In addition to the standard reporting attributes, the following attributes are available to refine your searches:

- **Company Name**—Name of the subsidiary organization
- **Company User**—Fully qualified user name including the subsidiary organization name
- **Company Group**—Fully qualified group name including the subsidiary organization name

Reports run at the subsidiary organization will include only results for that organization.
Note

Saved searches will only be available to the organization where they were created. For example, a parent organization would not see the saved searches of a subsidiary organization.

Threat Analysis Role

Users with the Threat Analysis role in the parent organization also have access to the Threats tab of their subsidiary organizations. Users with the Threat Analysis role in the subsidiary organization have access to only their own.