

Manage onboarded device settings

This chapter provides guidance on managing the device settings of the onboarded device.

- Changing a device's IP address in Security Cloud Control Firewall Management, on page 1
- Changing a device's name in Security Cloud Control Firewall Management, on page 2
- Export a list of devices and services, on page 3
- Export device configuration, on page 3
- External links for devices, on page 4
- Bulk reconnect devices to Security Cloud Control Firewall Management, on page 7
- Moving devices between organizations, on page 8
- Device certificate expiry detection, on page 8
- Write a device note, on page 8
- Delete a device from Security Cloud Control Firewall Management, on page 9
- Back up Firewall Threat Defense devices, on page 9
- Manage Firewall Threat Defense devices through Security Cloud Control Firewall Management, on page 10
- Security devices overview, on page 11
- Security Cloud Control Firewall Management labels and filtering, on page 12
- Use Security Cloud Control Firewall Management search functionality, on page 13
- Security devices overview, on page 17
- Security Cloud Control Firewall Management labels and filtering, on page 18
- Use Security Cloud Control Firewall Management search functionality, on page 19

Changing a device's IP address in Security Cloud Control Firewall Management

When you onboard an device to Security Cloud Control Firewall Management using an IP address, Security Cloud Control Firewall Management stores that IP address in its database and communicates with the device using that IP address. If the IP address of the device changes, you can update the IP address stored in Security Cloud Control Firewall Management to match the new address. Changing the device's IP address on Security Cloud Control Firewall Management does not change device's configuration.

To change the IP address, Security Cloud Control uses to communicate with a device, follow this procedure:

Procedure

Step 1 Choose **Inventory**.

Step 2 Choose **Security Devices**

Step 3 Click the **Devices** tab to locate the device.

Step 4 Click the appropriate device type tab.

You can use the filter and search functionalities to find the required device.

Step 5 Select the device whose IP address it is you want to change.

Step 6 Above the **Device Details** pane, click the edit button next to the device's IP address.



Step 7 Enter the new IP address in the field and click the blue check button.

No change is made to the device itself, so the device's Configuration Status will continue to show that it is Synced.

Changing a device's name in Security Cloud Control Firewall Management

All devices, models, templates, and services are given a name when they are onboarded or created in Security Cloud Control Firewall Management. You can change that name without changing the configuration of the device itself.

Procedure

Step 1 Choose **Inventory**.

Step 2 Choose **Security Devices**.

Step 3 Click the **Device** tab to locate the device.

Step 4 Select the device whose name it is you want to change.

Step 5 Above the **Device Details** pane, click the edit button next to the device's name.



Step 6 Enter the new name in the field and click the blue check button.

No change is made to the device itself, so the device's Configuration Status will continue to show that it is Synced.

Export a list of devices and services

This article explains how to export your list of devices and services to a comma-separated value (.csv) file. Once in that format, you can open the file in a spreadsheet application such as Microsoft Excel to sort and filter the items in your list.

The export button is available in both the Devices and Templates tab. You can also export details from devices under the selected device type tab.

Before you export your list of devices and services, look at the filter pane and determine if the **Security Devices** page is displaying the information you want to export. Clear all filters to view all managed devices and services, or apply filters to display a subset of your devices and services. The export function includes only the information currently displayed in the **Security Devices** page.

Procedure

Step 1 Choose **Inventory**.

Step 2 Choose **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab to export details from devices under that tab or click **All** to export details from all devices.

You can use the filter and search functionalities to find the required device.

Step 5 Click **Export list to CSV**.



Step 6 If prompted, save the .csv file.

Step 7 Open the .csv file in a spreadsheet application to sort and filter the results.

Export device configuration

You can only export one device configuration at a time. Use the following procedure to export a device's configuration to a JSON file:

Procedure

Step 1 Choose **Inventory**.

Step 2 Choose **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

You can use the filter and search functionalities to find the required device.

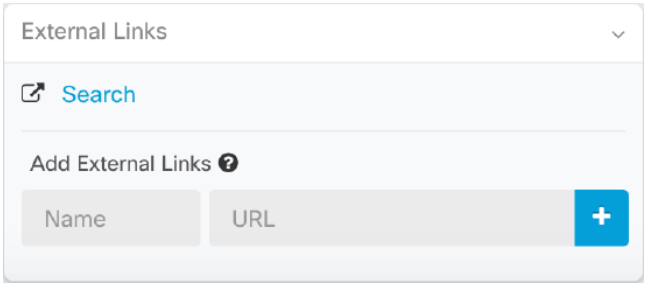
Step 5 Select the device you want so it is highlighted.

Step 6 In the **Actions** pane, select **Export Configuration**.

Step 7 Select **Confirm** to save the configuration as a JSON file.

External links for devices

You can create a hyperlink to an external resource and associate it with a device you manage with Security Cloud Control. You could use this feature to create a convenient link to the local manager of one of your devices (Adaptive Security Device Manager (ASDM) for ASA Firepower Device Manager (FDM) for an FTD). You could also use it to link to a search engine, documentation resource, a corporate wiki, or any other URL that you choose. You can associate as many external links with a device as you want. You can also associate the same link with multiple devices at the same time.



The links you create can reach anywhere, but your company's security requirements do not change. For example, if you ordinarily need to be connected to your corporate network, by being on-premises or through a VPN connection to reach a particular URL, those requirements remain. If your company blocks specific URLs, those URLs continue to be blocked. URLs that are not restricted continue to not be restricted.

Location Variable

We have created the {location} variable that you can incorporate in your URLs. This variable will be populated with the IP address of your device. For example,

```
https://{location}
```

should reach the ASDM for your ASA or the FDM of your FDM-managed device.

Create an External Link from your Device

Procedure

Step 1 Choose **Inventory**.

Step 2 Choose **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

Step 5 Select a device or model.

You can use the filter and search functionalities to find the required device.

Step 6 Enter a name for the link in the details pane under the **External Links** section.

Step 7 Enter the URL for the link in the URL field. You need to specify the full URL. For example, for Cisco, enter http://www.cisco.com.

Step 8 Click + to associate the link with the device.

Create an External Link to ASDM FDM

Here is a convenient way to open the Adaptive Security Device Manager (ASDM) of your ASA the Firepower Device Manager (FDM) of your FDM-managed device, directly from Security Cloud Control.

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

You can use the filter and search functionalities to find the required device.

Step 5 Select a device or model.

Step 6 In the details pane, on the right, go to the **External Links** section.

Step 7 Enter a name for the link such as ASDM FDM.

Step 8 Enter https://{location} in the URL field. The {location} variable will be populated with the IP address of your device.

Step 9 Click the + box.

Create an External Link for Multiple Devices

Procedure

Step 1 Choose **Inventory**.

Step 2 Choose **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

You can use the filter and search functionalities to find the required devices.

Step 5 Select multiple devices or models.

Step 6 In the details pane, on the right, go to the **External Links** section.

Step 7 Enter a name for the link.

Step 8 Enter the URL you want to reach using one of these methods:

- Enter

  ```
  https://{location}
  ```

  in the URL field. The {location} variable will be populated with the IP address of your device. This creates an automatic link to the ASDM for your device.

- Enter the URL for the link in the URL field. You need to specify the full URL, for example, for Cisco enter http://www.cisco.com.

Step 9 Click + to associate the link with the device.

Edit or Delete External Links

Procedure

Step 1 Choose **Inventory**.

Step 2 Choose **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

You can use the filter and search functionalities to find the required device.

Step 5 Select a device or model.

Step 6 In the details pane, go to the **External Links** section.

Step 7 Mouse-over the name of the link to reveal the edit and delete icons.

Step 8 Click the appropriate icon to edit or delete the external link and confirm your action.

Edit or Delete External Links for Multiple Devices

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

You can use the filter and search functionalities to find the required devices.

Step 5 Select multiple devices or models.

Step 6 In the details pane, on the right, go to the **External Links** section.

Step 7 Mouse-over the name of the link to reveal the edit and delete icons.

Step 8 Click the appropriate icon to edit or delete the external link and confirm your action.

Bulk reconnect devices to Security Cloud Control Firewall Management

Security Cloud Control Firewall Management allows an administrator to attempt to reconnect more than one managed device to Security Cloud Control Firewall Management at the same time. When a device Security Cloud Control Firewall Management manages is marked "unreachable," Security Cloud Control Firewall Management can no longer detect out of band configuration changes or manage the device. There could be many different reasons for the disconnect. Attempting to reconnect the devices is a simple first step in restoring Security Cloud Control Firewall Management's management of the device.

Note If you are reconnecting devices having new certificates, Security Cloud Control Firewall Management automatically reviews and accepts the new certificates on the devices and continues to reconnect with them. However, if you are reconnecting with only one device, Security Cloud Control Firewall Management prompts you to review and accept the certificate manually to continue to reconnect with it.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate devices.

Step 3 Click the appropriate device type tab.

Use the filter to look for devices whose connectivity status is "unreachable."

Step 4 From the filtered results, select the devices you want to attempt to reconnect.

Step 5 Click **Reconnect** . Notice that Security Cloud Control only provides command buttons for actions that can be applied to all the selected devices.

Moving devices between organizations

After onboarding devices to a Security Cloud Control Firewall Management organization, you cannot migrate the devices from one Security Cloud Control Firewall Management organization to another. If you want to move your devices to a new organization, you need to remove the devices from the old tenant and re-onboard them to the new organization.

Device certificate expiry detection

The management certificate is used for accessing FDM-managed and ASA devices from Security Cloud Control Firewall Management, while the Cisco Secure Client (formerly AnyConnect) is necessary for using virtual private network features on ASA, FDM-managed, and FTD devices from Security Cloud Control Firewall Management.

Security Cloud Control Firewall Management actively monitors the expiration status of these certificates and notifies the user when these certificates are nearing their expiration date or have expired. This prevents any disruptions in device operations due to certificate expiry. You should renew the corresponding certificate to address this issue.

The management certificate expiry check applies to ASA and FDM-managed devices, while the Secure Client certificate expiry check applies to ASA, FDM-managed, and FTD devices.

View Certificate Expiry Notification

In the top right corner, click the **Notifications** () icon to view the most recent alerts that have occurred or affected the devices you have onboarded to your tenant. The **High Priority** section displays the certificate expiration notifications.

These notifications are sent 30, 14, and 7 days before the certificate expiration date and then every day thereafter until the certificate either expires or is renewed with a valid certificate. You can also subscribe to receive these notifications by email on the **Notification Settings** section of the user preferences page. For more information, see User Notification Preferences.

Write a device note

Use this procedure to create a single, plain-text, note file for a device.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or model you want to create a note for.

Step 5 In the **Management** pane on the right, click **Notes**. Notes.

Step 6 Click the editor button on the right and select the Default text editor, Vim, or Emacs text editors.

Step 7 Edit the Notes page.

Step 8 Click **Save**.
The note is saved in the tab.

Delete a device from Security Cloud Control Firewall Management

Follow these steps to delete a device from Security Cloud Control Firewall Management:

Procedure

Step 1 Choose **Security Devices**.

Step 2 Select the device you want to delete.

Step 3 Click **Remove** in the **Device Actions** pane.

Step 4 To confirm device removal, click **OK**.

To keep the device onboarded, click **Cancel**.

Note
Both devices in an FDM-managed high-availability (HA) pair must be deleted simultaneously. Click the FDM-managed HA pair name instead of selecting individual peers.

Back up Firewall Threat Defense devices

To know how to back up Security Cloud Control-managed Firewall Threat Defense device types, use the following references:

Back Up Firewall Threat Defense devices managed by Cloud-Delivered Firewall Management Center

- In the Security Cloud Control left pane, choose **Administration** > **Firewall Management Center**.
- Choose **Cloud-delivered FMC** under the **FMC** tab.
- Click **Devices** on the right pane to navigate to the Cloud-Delivered Firewall Management Center.
- Continue to follow the steps in Back Up a Threat Defense Device from Cloud-delivered Firewall Management Center.

Back Up Firewall Threat Defense devices managed by On-Premises Firewall Management Center onboarded to Security Cloud Control Firewall Management

- In the Security Cloud Control left pane, choose **Administration** > **Firewall Management Center**.
- Choose the On-Premises Firewall Management Center whose Firewall Threat Defense devices you want to back up.
- Click **FMC Cross Launch URL** on the right pane to navigate to the on-premises Firewall Management Center or manually log in to the on-premises Firewall Management Center.
- Continue to follow the steps in *Back up a Device from the Management Center* in the Cisco Secure Firewall Management Center Administration Guide.

Back up Firewall Threat Defense devices managed by Firewall Device Managers onboarded to Security Cloud Control Firewall Management

Follow the steps in Back up an FDM-managed Device.

Manage Firewall Threat Defense devices through Security Cloud Control Firewall Management

Before you begin

Security Cloud Control Firewall Management provides a unified interface to manage Firewall Threat Defense devices, both in hardware and virtual formats.

Firewall Threat Defense devices associated with these three management applications can be managed on the Security Cloud Control platform:

- Secure Firewall Device Manager
- Secure Firewall Management Center
- Secure Cloud-Delivered Firewall Management Center

Procedure

Step 1 Log in to the Security Cloud Control platform.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **FTD** tab.

Step 4 Click  at the top-left corner.

Under **Devices/Services**, the filter pane provides filters that display Firewall Threat Defense devices based on the management application through which they are accessed from Security Cloud Control.

- **FDM**: Firewall Threat Defense device managed by Firewall Device Manager
- **FMC-FTD**: Firewall Threat Defense devices managed by Firewall Management Center

- **FTD**: Firewall Threat Defense devices managed by Cloud-Delivered Firewall Management Center

Step 5 To view the Firewall Threat Defense devices under a management application, check the corresponding check box.

Security devices overview

The **Security Devices** page displays all the physical and virtual onboarded devices and the templates created from the onboarded devices. The page classifies devices and templates based on their type and displays them in the corresponding tabs dedicated to each device type.

You can view the following details on the **Security Devices** page:

- The **Devices** tab displays all the live devices that are onboarded to Security Cloud Control.
- The **Templates** tab displays all the template devices created from live devices or configuration files imported to Security Cloud Control.

Filters in security devices

The **Filter** panel on the **Security Devices** page provides multiple options to narrow down results and find devices based on specific attributes, including **Devices/Services, Hardware Versions, Device End-of-Life, Software Versions, Snort Version, Configuration Status, Connectivity States, Conflict Detection, Health Status, Secure Device Connectors, and Labels**.

The Hardware End-of-Life (EoL) Filter

The **Hardware End-of-Life (EoL) filter** allows you to identify devices that are nearing or have reached their last day of hardware support. Running unsupported hardware may pose operational and security risks because Cisco no longer provides software updates, security patches, or technical support after the EoL date.



Note The Hardware EoL filter currently supports Firewall Threat Defense devices managed by on-premises Firewall Management Center and Cloud-Delivered Firewall Management Center, and ASA devices.

Procedure

1. In the **Devices** tab, click the filter icon.
2. From the list of available filters, under **Device End-of-Life**, select **Hardware End-of-Life**.

   The list now displays all devices that are approaching or have reached their hardware end-of-life.
3. Select a device to view more information on the right pane.
4. Scroll down to the **Device End of Life** section to view the following details:
   - The exact end-of-life date.
   - Remaining time until the last day of support.
5. Click **Know more**.

You can view a detailed page that provides the following information:

- Cisco's recommended replacement devices with product specifications, along with links to view the official data sheets.
- Guidance on submitting a request through the Contact Cisco page and options to connect directly with Cisco experts.
- Information on Cisco's product recycling program.

6. Click **Export** to download the device report in CSV format for offline analysis.

Security Cloud Control Firewall Management labels and filtering

Labels are used for grouping devices or objects. You can apply labels to one or more devices during onboarding or any time after onboarding. You can apply labels to objects after creating them. Once you apply labels to devices and objects, you can filter the contents of the device table or objects table using the corresponding label.

Note A label that is applied to a device is not extended to its associated objects, and a label applied to a shared object is not extended to its associated objects.

You can create a label group by using the syntax group name:label, for example, Region:East or Region:West. If you create these two labels, the group label would be Region and you could choose from East or West in that group.

Apply Labels to Devices and Objects

To apply a label to devices, perform these steps:

Procedure

Step 1	To add a label to a device, click **Inventory** in the navigation pane on the left.
Step 2	In the left pane, click **Security Devices**.
Step 3	To add a label to an object, click **Objects** in the navigation pane on the left.
Step 4	In the left pane, click **Objects**.
Step 5	Click the **Devices** tab to locate a device or the **Templates** tab to locate the model device.
Step 6	Click the appropriate device type tab.
Step 7	Select one or more devices.
Step 8	In the **Add Groups and Labels** field on the right, specify a label for the devices.
Step 9	Click the + icon.

Filters on security devices, policies, and objects page

Use filters on the **Security Devices**, **Policies**, and **Objects** pages to find devices and objects. To filter, select the filter icon in the left pane.

On the **Security Devices** page, the filter panel lets you filter devices by criteria such as device type, hardware version, software version, Snort version, configuration status, connection state, conflict detection, Secure Device Connector, and labels. You can apply filters within the selected device type tab.

When the **FTD** tab is open, the filter panel also lets you filter FTD devices by the management application that Security Cloud Control uses to access them.

To filter, click  in the left-hand pane of the Security Devices, Policies, and Objects tabs.



Note When the **FTD** tab is opened, the filter pane provides filters to show FDM-managed devices based on the management application through which the devices are accessed from Security Cloud Control.

- FDM: Devices managed using FTD API or Firewall Device Manager.
- FMC-FTD: Devices managed using Firepower Management Center.
- FTD: Devices managed using FTD Management.

Use Security Cloud Control Firewall Management search functionality

The Security Cloud Control Firewall Management platform has a highly efficient search function that makes it easy to find anything you need. The search bar on each page is tailored to the content of that page, while the global search allows for a comprehensive search across the entire tenant. This saves time and effort, as you can quickly locate the necessary information.

Page Level Search

The page-level search enables you to search specific items on the Security Devices, Policies, Objects, VPN, Change Log, and Jobs pages.

- In the **Security Devices** space, you can simply start typing in the search bar, and devices that fit the search criteria will be displayed. You can type any partial part name of the device, IP address, or the serial number of the physical device to find the device.
- In the **Policies** space, you can search policies by their name, components or objects used in them.
- In the **Objects** space, you can search for an object by typing any partial part of the name of the object, or partial IP Address, port, or protocols.
- In the **VPN** space, you can search by tunnel name, device name, and IP address used in the VPN policies.
- In the **Change log** space, you can search logs based on events, device names, or actions.

Procedure

Step 1 Navigate to the search bar near the top of the interface.

Step 2 Type the search criteria into the Search Bar and the corresponding results will be displayed.

Global Search

The global search feature allows you to quickly locate and navigate to devices managed by Security Cloud Control.

All search results are based on the indexing option you choose. These are the indexing options:

- Full Indexing—Requires that you invoke the full indexing process. This process scans all the devices and objects in the system and displays them in the search index only after you invoke the indexing. To invoke full indexing, you must have administrative privileges.

  For more information, see Initiate Full Indexing, on page 15.

- Incremental Indexing—An event-based indexing process where the search index automatically updates each time that a device or an object is added, modified, or deleted.

The information that you enter in the search field is not case-sensitive. You can perform a global search using these entities:

- Device Name—Supports partial device names, URL, IP address, or range.
- Object Types—Supports object name, object descriptions, and configured values.
- Policy Types—Supports policy name, policy description, rule name, and rule comments.

  Cloud-Delivered Firewall Management Center and on-premises Firewall Management Center managed in Security Cloud Control support the following policy types:

  - Access Control Policy
  - Prefilter Policy
  - Threat Defense NAT Policy

When you type a search expression, the interface begins to display search results and you do not need to press *Enter* to execute a search.

The search results display all devices and objects that match your search terms. If your search term matches more than one device or object, the results appear under categories such as devices, objects, and connected_fmc.

By default, the first item in the search result is highlighted and the related information for that item appears in the right pane. You can scroll through the search results and click any item to view the corresponding information. You can click the arrow icon besides the item to navigate to the corresponding page.

Note

- Global search does not display duplicate search results. For objects, the unique identifier of the shared object is used to navigate to the Object view.
- If you delete a device from Security Cloud Control, all associated objects are removed from the global search index.
- If you delete an object from the policy and retain the device before you initiate full indexing, the object remains in the global search index because it is associated with the device.

Initiate Full Indexing

Procedure

Step 1 In the left pane, choose **Administration** > **General Settings**.

Step 2 In the left pane, click **Administration** > **General Settings**.

Step 3 In Global Search, click **Initiate Full Indexing** to trigger indexing.



Note
Initiating full indexing clears existing indexing of the Security Cloud Control tenant.

Step 4 Click **here** to view the global search workflow.

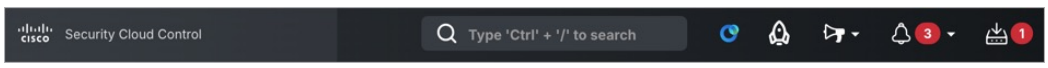
Perform a Global Search

Procedure

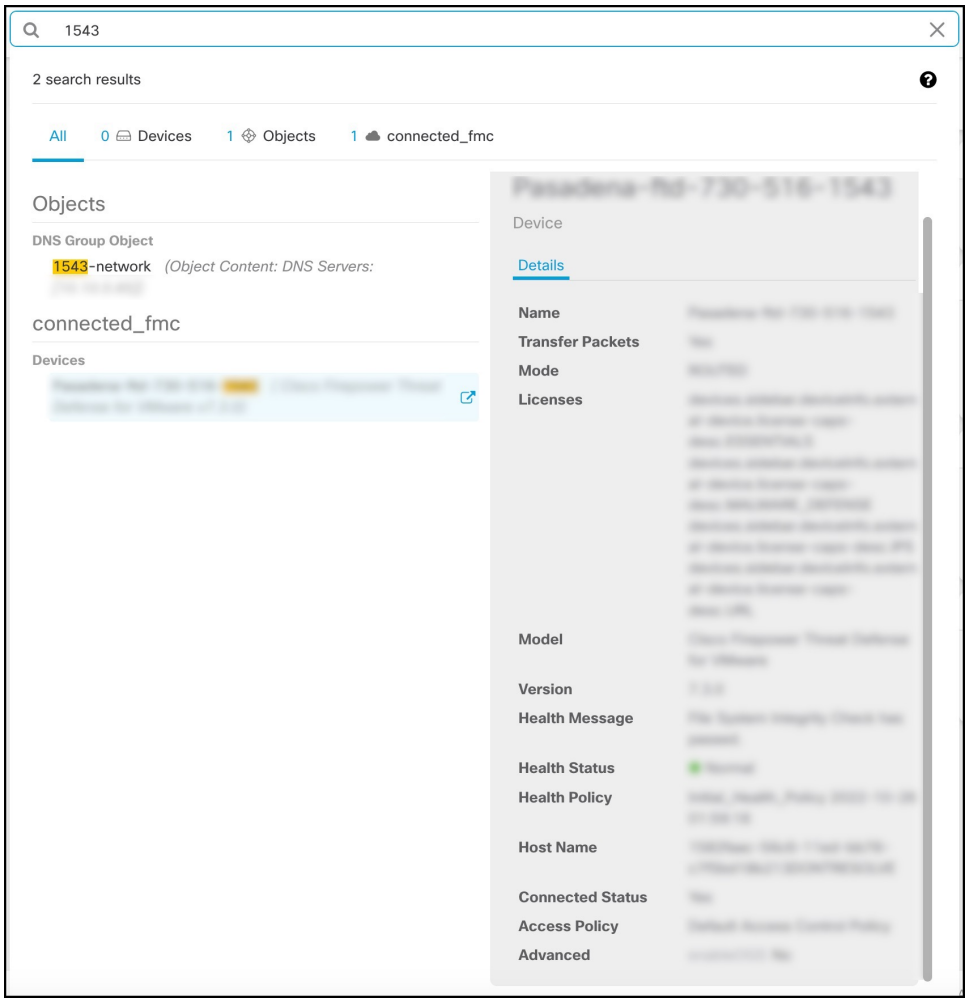
Step 1 Log into Security Cloud Control.

Step 2 Click the search icon in the Security Cloud Control page and enter the search strings in the search field that appears.

Alternatively, you can press and hold the **Ctrl** key and the **/** key simultaneously on Windows, or the **Command** key and **/** key on Mac, to open the search bar.



The search results display a list of possible items as you begin entering the search strings. The search results appear under four categories: All, Devices, Objects, Policies, and Cloud-Delivered Firewall Management Center. The right pane displays information for a selected search result.



Step 3 From the search result, select a device or an object, and click the arrow icon to navigate from the search results to the corresponding device and object page. From the search result, select an item, and click the arrow icon to navigate from the search results to the corresponding page.

Note
Selecting a search result for devices in the Cloud-Delivered Firewall Management Center, allows you to navigate to the Cloud-Delivered Firewall Management Center user interface within Security Cloud Control.

For information on Cloud-Delivered Firewall Management Center, see Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control.

Step 4 Click **X** to close the search bar.

Security devices overview

The **Security Devices** page displays all the physical and virtual onboarded devices and the templates created from the onboarded devices. The page classifies devices and templates based on their type and displays them in the corresponding tabs dedicated to each device type.

You can view the following details on the **Security Devices** page:

- The **Devices** tab displays all the live devices that are onboarded to Security Cloud Control.
- The **Templates** tab displays all the template devices created from live devices or configuration files imported to Security Cloud Control.

Filters in security devices

The **Filter** panel on the **Security Devices** page provides multiple options to narrow down results and find devices based on specific attributes, including **Devices/Services, Hardware Versions, Device End-of-Life, Software Versions, Snort Version, Configuration Status, Connectivity States, Conflict Detection, Health Status, Secure Device Connectors, and Labels**.

The Hardware End-of-Life (EoL) Filter

The **Hardware End-of-Life (EoL) filter** allows you to identify devices that are nearing or have reached their last day of hardware support. Running unsupported hardware may pose operational and security risks because Cisco no longer provides software updates, security patches, or technical support after the EoL date.



Note The Hardware EoL filter currently supports Firewall Threat Defense devices managed by on-premises Firewall Management Center and Cloud-Delivered Firewall Management Center, and ASA devices.

Procedure

1. In the **Devices** tab, click the filter icon.
2. From the list of available filters, under **Device End-of-Life**, select **Hardware End-of-Life**.

   The list now displays all devices that are approaching or have reached their hardware end-of-life.
3. Select a device to view more information on the right pane.
4. Scroll down to the **Device End of Life** section to view the following details:
   - The exact end-of-life date.
   - Remaining time until the last day of support.
5. Click **Know more**.

   You can view a detailed page that provides the following information:
   - Cisco's recommended replacement devices with product specifications, along with links to view the official data sheets.
   - Guidance on submitting a request through the Contact Cisco page and options to connect directly with Cisco experts.

- Information on Cisco's product recycling program.

6. Click **Export** to download the device report in CSV format for offline analysis.

Security Cloud Control Firewall Management labels and filtering

Labels are used for grouping devices or objects. You can apply labels to one or more devices during onboarding or any time after onboarding. You can apply labels to objects after creating them. Once you apply labels to devices and objects, you can filter the contents of the device table or objects table using the corresponding label.

Note A label that is applied to a device is not extended to its associated objects, and a label applied to a shared object is not extended to its associated objects.

You can create a label group by using the syntax group name:label, for example, Region:East or Region:West. If you create these two labels, the group label would be Region and you could choose from East or West in that group.

Apply Labels to Devices and Objects

To apply a label to devices, perform these steps:

Procedure

Step 1 To add a label to a device, click **Inventory** in the navigation pane on the left.

Step 2 In the left pane, click **Security Devices**.

Step 3 To add a label to an object, click **Objects** in the navigation pane on the left.

Step 4 In the left pane, click **Objects**.

Step 5 Click the **Devices** tab to locate a device or the **Templates** tab to locate the model device.

Step 6 Click the appropriate device type tab.

Step 7 Select one or more devices.

Step 8 In the **Add Groups and Labels** field on the right, specify a label for the devices.

Step 9 Click the + icon.

Filters on security devices, policies, and objects page

Use filters on the **Security Devices**, **Policies**, and **Objects** pages to find devices and objects. To filter, select the filter icon in the left pane.

On the **Security Devices** page, the filter panel lets you filter devices by criteria such as device type, hardware version, software version, Snort version, configuration status, connection state, conflict detection, Secure Device Connector, and labels. You can apply filters within the selected device type tab.

When the **FTD** tab is open, the filter panel also lets you filter FTD devices by the management application that Security Cloud Control uses to access them.

To filter, click  in the left-hand pane of the Security Devices, Policies, and Objects tabs.



Note When the **FTD** tab is opened, the filter pane provides filters to show FDM-managed devices based on the management application through which the devices are accessed from Security Cloud Control.

- FDM: Devices managed using FTD API or Firewall Device Manager.
- FMC-FTD: Devices managed using Firepower Management Center.
- FTD: Devices managed using FTD Management.

Use Security Cloud Control Firewall Management search functionality

The Security Cloud Control Firewall Management platform has a highly efficient search function that makes it easy to find anything you need. The search bar on each page is tailored to the content of that page, while the global search allows for a comprehensive search across the entire tenant. This saves time and effort, as you can quickly locate the necessary information.

Page Level Search

The page-level search enables you to search specific items on the Security Devices, Policies, Objects, VPN, Change Log, and Jobs pages.

- In the **Security Devices** space, you can simply start typing in the search bar, and devices that fit the search criteria will be displayed. You can type any partial part name of the device, IP address, or the serial number of the physical device to find the device.
- In the **Policies** space, you can search policies by their name, components or objects used in them.
- In the **Objects** space, you can search for an object by typing any partial part of the name of the object, or partial IP Address, port, or protocols.
- In the **VPN** space, you can search by tunnel name, device name, and IP address used in the VPN policies.
- In the **Change log** space, you can search logs based on events, device names, or actions.

Procedure

Step 1 Navigate to the search bar near the top of the interface.

Step 2 Type the search criteria into the Search Bar and the corresponding results will be displayed.

Global Search

The global search feature allows you to quickly locate and navigate to devices managed by Security Cloud Control.

All search results are based on the indexing option you choose. These are the indexing options:

- Full Indexing—Requires that you invoke the full indexing process. This process scans all the devices and objects in the system and displays them in the search index only after you invoke the indexing. To invoke full indexing, you must have administrative privileges.

  For more information, see Initiate Full Indexing, on page 15.

- Incremental Indexing—An event-based indexing process where the search index automatically updates each time that a device or an object is added, modified, or deleted.

The information that you enter in the search field is not case-sensitive. You can perform a global search using these entities:

- Device Name—Supports partial device names, URL, IP address, or range.
- Object Types—Supports object name, object descriptions, and configured values.
- Policy Types—Supports policy name, policy description, rule name, and rule comments.

  Cloud-Delivered Firewall Management Center and on-premises Firewall Management Center managed in Security Cloud Control support the following policy types:

  - Access Control Policy
  - Prefilter Policy
  - Threat Defense NAT Policy

When you type a search expression, the interface begins to display search results and you do not need to press *Enter* to execute a search.

The search results display all devices and objects that match your search terms. If your search term matches more than one device or object, the results appear under categories such as devices, objects, and connected_fmc.

By default, the first item in the search result is highlighted and the related information for that item appears in the right pane. You can scroll through the search results and click any item to view the corresponding information. You can click the arrow icon besides the item to navigate to the corresponding page.

Note

- Global search does not display duplicate search results. For objects, the unique identifier of the shared object is used to navigate to the Object view.
- If you delete a device from Security Cloud Control, all associated objects are removed from the global search index.
- If you delete an object from the policy and retain the device before you initiate full indexing, the object remains in the global search index because it is associated with the device.

Initiate Full Indexing

Procedure

Step 1 In the left pane, choose **Administration** > **General Settings**.

Step 2 In the left pane, click **Administration** > **General Settings**.

Step 3 In Global Search, click **Initiate Full Indexing** to trigger indexing.



Note
Initiating full indexing clears existing indexing of the Security Cloud Control tenant.

Step 4 Click **here** to view the global search workflow.

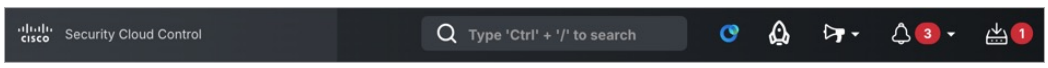
Perform a Global Search

Procedure

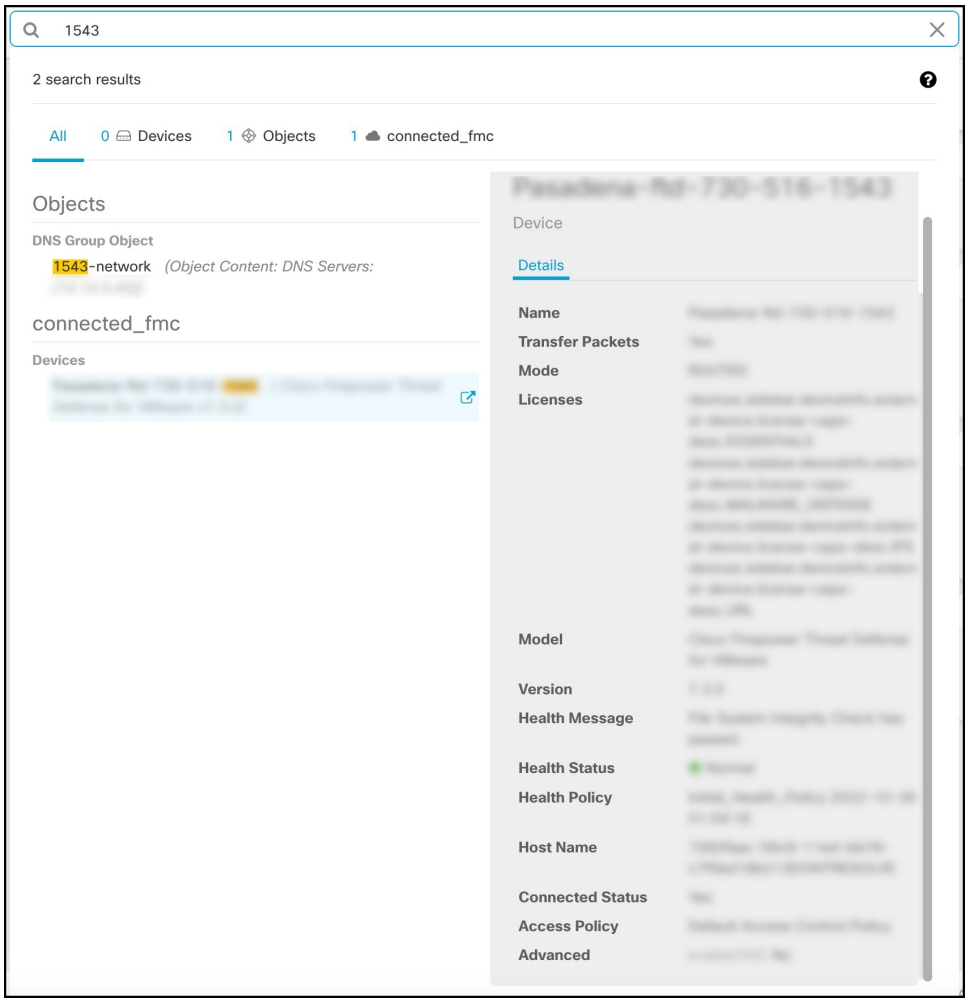
Step 1 Log into Security Cloud Control.

Step 2 Click the search icon in the Security Cloud Control page and enter the search strings in the search field that appears.

Alternatively, you can press and hold the **Ctrl** key and the **/** key simultaneously on Windows, or the **Command** key and **/** key on Mac, to open the search bar.



The search results display a list of possible items as you begin entering the search strings. The search results appear under four categories: All, Devices, Objects, Policies, and Cloud-Delivered Firewall Management Center. The right pane displays information for a selected search result.



Step 3 From the search result, select a device or an object, and click the arrow icon to navigate from the search results to the corresponding device and object page. From the search result, select an item, and click the arrow icon to navigate from the search results to the corresponding page.

Note
Selecting a search result for devices in the Cloud-Delivered Firewall Management Center, allows you to navigate to the Cloud-Delivered Firewall Management Center user interface within Security Cloud Control.

For information on Cloud-Delivered Firewall Management Center, see Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control.

Step 4 Click **X** to close the search bar.