Device Registration

You canmanage devices in the Cloud-Delivered Firewall Management Center.

- Log into the Command-Line Interface on the device, on page 1
- Device registration management, on page 3

Log into the Command-Line Interface on the device

You can log directly into the command-line interface on Firewall Threat Defense devices. If this is your first time logging in, complete the initial setup process using the default **admin** user; see Complete the Initial Configuration of a Secure Firewall Threat Defense Device Using the CLI .

For zero-touch provisioning , if you must access the Firewall Threat Defense CLI and run through the setup script, answer **n** when prompted: `Do you want to configure IPv4? (y/n) [y]:` and `Do you want to configure IPv6? (y/n) [y]:` . You also must accept the default local manager: `Manage the device locally? (yes/no) [yes]:` . These settings will preserve zero-touch provisioning capability.

For the Secure Firewall 200 , the device only supports up to three concurrent CLI sessions. For example, you can have one console session and two SSH sessions to the Management interface (this limitation is separate from SSH to a data interface). If you already have three active SSH sessions and then connect to the console, the console connection is allowed because console access will never be blocked.

Note If a user makes three consecutive failed attempts to log into the CLI via SSH, the system terminates the SSH connection.

Before you begin

- Create additional user accounts that can log into the CLI using the **configure user add** command.
- If you get unreadable characters when connecting to the console port, verify the port settings. If they are correct, try the cable with another device using the same settings. If the cable is good, you might need to replace the hardware for the console port. Also consider trying a different workstation to make the connection.

Procedure

Step 1 Connect to the Firewall Threat Defense CLI, either from the console port or using SSH.

You can SSH to the management interface of the Firewall Threat Defense device. You can also connect to the address on a data interface if you open the interface for SSH connections. SSH access to data interfaces is disabled by default. See Configure secure shell SSH access to allow SSH connections to specific data interfaces.

For physical devices, you can directly connect to the console port on the device. See the hardware guide for your device for more information about the console cable. Use the following serial settings:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

The CLI on the console port is FXOS (with the exception of the ISA 3000, where it is the regular Firewall Threat Defense CLI) . Use the Firewall Threat Defense CLI for basic configuration, monitoring, and normal system troubleshooting. See the FXOS documentation for information on FXOS commands.

Step 2 Log in with the **admin** username and password.

Example:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1
firepower#
```

Step 3 If you used the console port, access the Firewall Threat Defense CLI.

connect ftd

Note
This step does not apply to the ISA 3000.

Example:

```
firepower# connect ftd
>
```

Step 4 At the CLI prompt (>), use any of the commands allowed by your level of command line access.

To return to FXOS on the console port, enter **exit** .

Step 5 (Optional) If you used SSH, you can connect to FXOS.

connect fxos

To return to the Firewall Threat Defense CLI, enter **exit** .

Step 6 (Optional) Access the diagnostic CLI:

system support diagnostic-cli

Use this CLI for advanced troubleshooting. This CLI includes additional **show** and other commands.

This CLI has submodes: user EXEC mode, privileged EXEC mode , and recovery-config mode . More commands are available in privileged EXEC mode than user EXEC mode. To enter privileged EXEC mode, enter the **enable** command; press enter without entering a password when prompted.

Example:

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

To use recovery-config mode, see Access Recovery-Config Mode in the Diagnostic CLI .

To return to the regular CLI, type **Ctrl-a** , **d** .

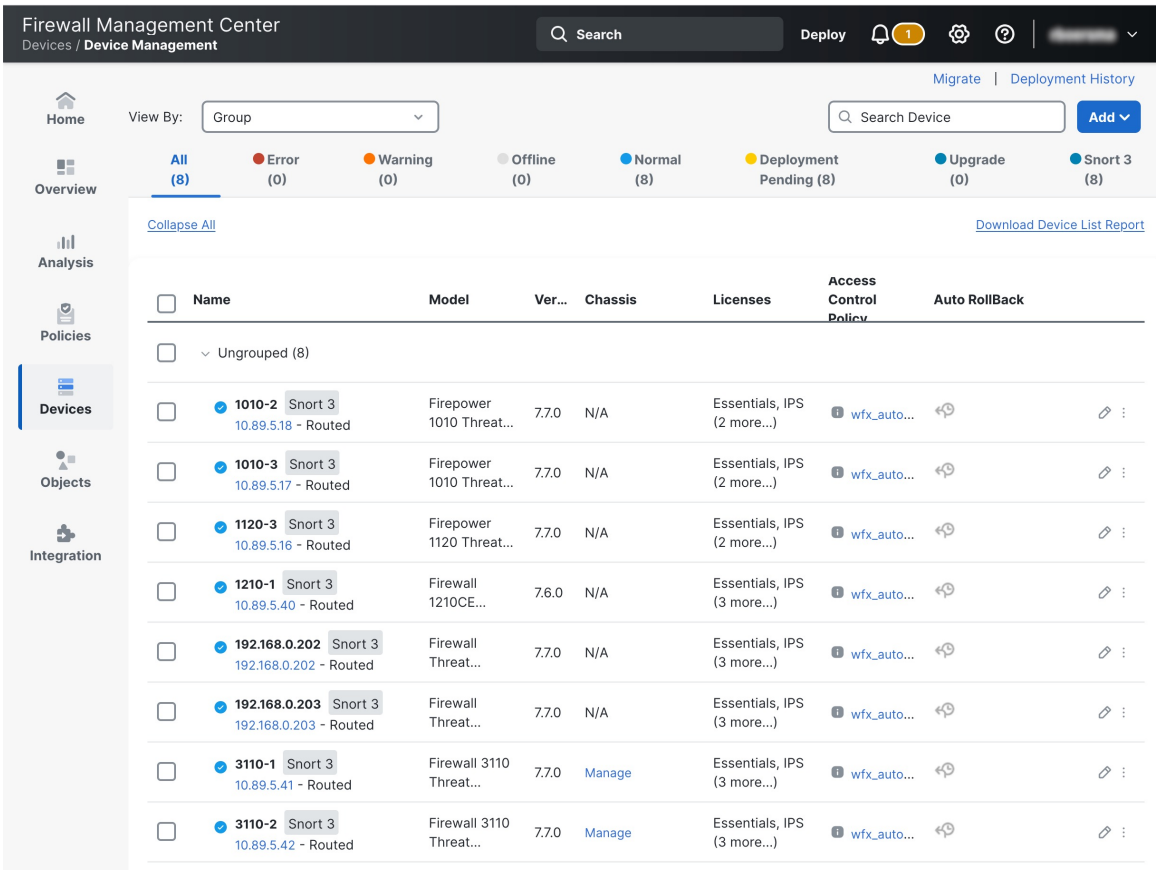
Device registration management

Register and unregister devices to the Cloud-Delivered Firewall Management Center.

About the device management page

The **Devices** > **Device Management** page provides you with range of information and options.

Figure 1: Device management page



- **View By**—View devices based on group, licenses, model, version, or access control policy.
- **Device State**—View devices based on state (**Error**, **Warning**, etc.). You can click on a state icon to view the devices belonging to it. The number of devices belonging to the states are provided within brackets.
- **Search Device**—Search for a device by device name, host name, or IP address.
- **Add**—Add devices and other manageable components.
- Columns—Click the column head to sort by that column.
  - **Name**
  - **Model**
  - **Version**
  - **Chassis**—For supported models, click **Manage** to bring up the integrated Chassis Manager. For the Firepower 4100/9300, the link cross-launches the Firewall Chassis Manager.
  - **Licenses**
  - **Access Control Policy**—Click on the link in the Access Control Policy column to view the policy that is deployed to the device.

- **Auto-Rollback**—Shows whether auto-rollback of the configuration is enabled ( ) or disabled) if the deployment causes the management connection to go down. See Edit Deployment Settings.

- **Edit**—For each device, use the **Edit** ( ) icon to edit the device settings.

  You can also just click on the device name or IP address.

- **More**—For each device, click the **More** ( ) icon to execute other actions:
  - **Packet Tracer**—To navigate to the packet tracer page for examining policy configuration on the device by injecting a model packet into the system.
  - **Packet Capture**—To navigate to the packet capture page, where, you can view the verdicts and actions the system takes while processing a packet.
  - **Revert Upgrade**—To revert the upgrade and configuration changes that were made after the last upgrade. This action results in restoring the device to the version that was before the upgrade.
  - **Health Monitor**—To navigate to the device's health monitoring page.
  - **Troubleshoot Files**—Generate troubleshooting files, where you can choose the type of data to be included in the report.
  - **Generate Template from Device**—Generate a new device template from a registered device. The new template has the same configuration as the device from which it is generated. You can generate a new device template from standalone and HA devices. However, if you generate a template from HA devices, the new template will not contain the failover configurations.

Add a Device Group

The Cloud-Delivered Firewall Management Center allows you to group devices so you can easily deploy policies and install updates on multiple devices. You can expand and collapse the list of devices in the group.

If you add the primary device in a high-availability pair to a group, both devices are added to the group. If you break the high-availability pair, both devices remain in that group.

Groups are not supported in a multidomain environment.

Procedure

Step 1 Choose **Devices** > **Device Management** .

Step 2 From the **Add** drop-down menu, choose **Add Group** .

To edit an existing group, click **Edit** ( ) for the group you want to edit.

Step 3 Enter a **Name** .

Step 4 Under **Available Devices** , choose one or more devices to add to the device group. Use Ctrl or Shift while clicking to choose multiple devices.

Step 5 Click **Add** to include the devices you chose in the device group.

Step 6 Optionally, to remove a device from the device group, click **Delete** ( ) next to the device you want to remove.

Step 7 Click **OK** to add the device group.

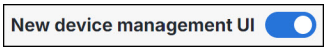
Device management page enhancements

Device management page is enhanced to a new user interface that can be toggled with the legacy version. User interface improvements offer enhanced features including improved search functionality, device status monitoring, and centralized troubleshooting tools.

Device management page enhancement features

Navigation: **Devices** > **Device Management**

Enable the **New device management UI** toggle button to switch between the legacy and the enhanced **Device Management** page.



Note The enhanced user interface is in a preliminary stage and does not include all the legacy user interface features. You can switch back to the legacy **Device Management** user interface by clicking the same toggle button to access the features that are not yet supported in the new user interface.

Key enhancements in the new user interface:

- **Improved search functionality**: Provides a more powerful and granular search experience. Unlike the legacy user interface, which was limited to searching by device name, host name, or IP address, you can now use multiple device-related criteria, to achieve highly refined results.
- **Device status banner**: A status banner at the top of the **Device Management** page displays the number of devices in various states (**Normal**, **Error**, **Offline**). A color-coded legend dynamically reflects these statuses for at-a-glance monitoring.
- **Performance improvements**: The enhanced user interface page loads faster than the legacy version. Pagination has been introduced at the bottom of the page, with each page supporting up to 1,000 devices by default.
- **Device actions and bulk operations**: Details of selected devices are displayed on a side panel in a more user-friendly format. Multiple devices can be selected simultaneously enabling device bulk actions from a centralized location.
- **Centralized troubleshooting panel**: Troubleshooting information has been consolidated into a single pane under Troubleshooting tools, making it easier to access diagnostic tools such as **Packet Tracer** and **Packet Capture**.

Use the enhanced filters in device management page

This task enables you to quickly find specific devices using various search criteria and save frequently used searches for future use.

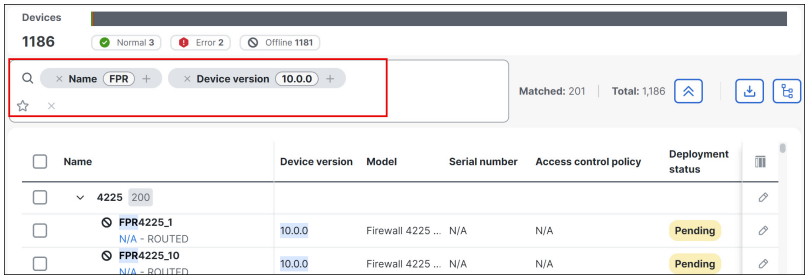
You can use different criteria to instantly search for the devices you want.

Procedure

Step 1 In the **Device Management** page, click the **Type to search** field to perform one of the following actions:

- Enter the filter criteria to search the device. Suggestions are displayed as you type.
- Select a filter and then enter a value in the field. You can add multiple criteria to refine your search results further.

In the example shown in the figure, the filter searches for devices with names that contain "FPR" andare of version of "10.0.0".



Step 2 Click the **Favourite Searches** ( ) icon and do one of the following:

- To save a new search, specify a search name and click **Save as new**.
- To overwrite a saved search, click the **Edit** () icon on next to the saved search that you want to overwrite, and click **Overwrite**.

Note

You can also use the **Favourite Searches** ( ) icon to quickly retrieve the previously executed searches.

The enhanced filters display devices that match your search criteria, and saved searches are available for future use through the Favourite Searches feature.

Add a device group

Create device groups to organize and manage multiple devices efficiently, enabling streamlined policy deployment and update installation across grouped devices.

The Management Center allows you to group devices to easily deploy policies and install updates on multiple devices. You can expand and collapse the list of devices in the group. The new device management user interface provides enhanced functionalities in the context of device groups, improving the way you organize, manage, and interact with them.

The **Manage device groups** dialog box provides two main sections:

- Ungrouped devices: This section lists all the devices that are currently not assigned to any group. A search bar, labeled **Search devices to move** enables you to quickly locate specific devices by device

name or device IP address. The count that is displayed represents the number of ungrouped devices, and not the total number of devices managed by the system.

- Groups: This section displays all the existing device groups. A search bar, **Search by group or device name**, enables you to find specific groups or devices within groups.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Enable the **New Device Management UI** toggle button and click the **Manage Groups** () icon.

Step 3 Click **Create Group**.

Step 4 Enter a name and click  .

The group is created.

Step 5 Select the devices that you want to add to the newly created group.

Step 6 Under **Groups** locate the newly created group.

You can use the **Search by group or device name** field to search for the group.

Step 7 Click **Add selection to group**.

The selected devices are added to the group.

Note
You can also delete a group. However, deleting a group does not remove the devices from the Management Center. Instead, all the devices assigned to the deleted group will be automatically moved back to the Ungrouped devices section.

A new device group is created with the selected devices assigned to it. The devices appear under the group in the Groups section and are removed from the Ungrouped devices section.

Move devices to another group

Moving devices to another group allows you to reorganize your device management structure and ensure devices are properly categorized for administrative purposes.

The device must first be moved to Ungrouped Devices. Next, move it to the group you want.

Procedure

Step 1 Click the **Manage Groups** icon.

Step 2 Under **Groups**, expand the group from which you want to move the device.

Step 3 Click the X button to remove the device from the group.

The device is moved to **Ungrouped Groups**.

Step 4 Select the device that you want to add.

Step 5 Under **Groups** locate the group.

You can use the **Search by group or device name** field to search for the group.

Step 6 Click **Add selection to group**.

The selected device is added to the group.

Managed device list download

A managed device list download is a data export feature that enables administrators to obtain device inventory information in multiple file formats for offline analysis and reporting purposes.

Download process

Click  to download the device list in CSV or PDF format. Click **Download CSV** or **Download PDF** to download the report in the corresponding format.

Register with a new management center

This procedure shows how to register with a new Cloud-Delivered Firewall Management Center . You should perform these steps even if the new Cloud-Delivered Firewall Management Center uses the old Cloud-Delivered Firewall Management Center 's IP address.

Procedure

Step 1 On the old Cloud-Delivered Firewall Management Center , if present, delete the managed device.

You cannot change the Cloud-Delivered Firewall Management Center IP address if you have an active connection with the Cloud-Delivered Firewall Management Center .

Step 2 Connect to the device CLI, for example using SSH.

Step 3 Configure the new Cloud-Delivered Firewall Management Center .

configure manager add { *hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*] [*display_name*]

- { *hostname* | *IPv4_address* | *IPv6_address* }—Sets the Cloud-Delivered Firewall Management Center hostname, IPv4 address, or IPv6 address.
- **DONTRESOLVE** —If the Cloud-Delivered Firewall Management Center is not directly addressable, use **DONTRESOLVE** instead of a hostname or IP address. If you use **DONTRESOLVE** , then a *nat_id* is required. When you add this device to the Cloud-Delivered Firewall Management Center , make sure that you specify both the device IP address and the *nat_id* ; one side of the connection needs to specify an IP address, and both sides need to specify the same, unique NAT ID.

- *regkey* —Make up a registration key to be shared between the Cloud-Delivered Firewall Management Center and the device during registration. You can choose any text string for this key between 1 and 37 characters; you will enter the same key on the Cloud-Delivered Firewall Management Center when you add the Firewall Threat Defense .
- *nat_id* —Make up an alphanumeric string from 1 to 37 characters used only during the registration process between the Cloud-Delivered Firewall Management Center and the device when one side does not specify an IP address. This NAT ID is a one-time password used only during registration. Make sure the NAT ID is unique, and not used by any other devices awaiting registration. Specify the same NAT ID on the Cloud-Delivered Firewall Management Center when you add the Firewall Threat Defense .
- *display_name* —Provide a display name for showing this manager with the **show managers** command. This option is useful if you are identifying Security Cloud Control as the primary manager and an on-prem Cloud-Delivered Firewall Management Center for analytics only. If you don't specify this argument, the firewall auto-generates a display name using one of the following methods:
  - *hostname* | *IP_address* (if you don't use the **DONTRESOLVE** keyword)
  - **manager-** *timestamp*

Example:

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
>
```

Step 4 Add the device to the Cloud-Delivered Firewall Management Center .

Shut down or restart the device

It's important that you shut down your system properly. Simply unplugging the power or pressing the power switch can cause serious file system damage. Remember that there are many processes running in the background all the time, and unplugging or shutting off the power does not allow the graceful shutdown of your firewall.

See the following task to shut down or restart your system properly.

Note After restarting your device, you may see an error that the management connection could not be reestablished. In some cases, the connection is attempted before the Management interface on the device is ready. The connection will be retried automatically and should come up within 15 minutes.

Procedure

Step 1 Choose **Devices** > **Device Management** .

Step 2 Next to the device that you want to restart, click **Edit** (✎) .

Step 3 Click **Device** .

Step 4 To restart the device:

a) Click **Restart Device** ( ) .
b) When prompted, confirm that you want to restart the device.

Step 5 To shut down the device:

a) Click **Shut Down Device** ( ) in the **System** section.
b) When prompted, confirm that you want to shut down the device.
c) If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

If you do not have a console connection, wait approximately 3 minutes to ensure the system has shut down.

For the ISA 3000, when shutdown is complete, the System LED will turn off. Wait at least 10 seconds before you remove the power.

Download the managed device list

You can download a report of all the managed devices.

Before you begin

To perform the following task, you must be an Admin user.

Procedure

Step 1 Choose **Devices** > **Device Management** .

Step 2 Click the **Download Device List Report** link.

Step 3 You can download the device list in CSV or PDF format. Choose **Download CSV** or **Download PDF** to download the report.

Migrate Firewall Threat Defense devices

The Secure Firewall Threat Defense model migration wizard enables you to migrate configurations from an earlier Firewall Threat Defense model. After the migration, all routing and interface configurations from the source Firewall Threat Defense device are available in the target Firewall Threat Defense.

Supported devices and capabilities

The wizard supports multiple models as source and target devices, for more information see Supported Devices for Migration, on page 12.

When you migrate Firepower 4100 and 9300 Series devices to the supported models, you can now configure interface attributes according to your requirements. You can map the source device interfaces to the target device interfaces. The migration locks the source and target devices.

Supported Devices for Migration

Documents the supported migration paths and device compatibility for Cisco Firepower and Secure Firewall models.

Supported Migration Paths

The following table lists the supported target Firewall Threat Defense models that you can migrate to from your source Firewall Threat Defense model.

Source Devices	Source Device Version	Target Devices	Target Device Version
Cisco Firepower 1010 Series: 1010, 1010E	7.3.x and later	Cisco Secure Firewall 1200 Series:1210CE, 1210CP, 1210CX	7.6 and later
Cisco Firepower 1010 Series: 1010, 1010E	7.3.x and later	Cisco Firewall 200 Series: 220	10.0 and later
Cisco Firepower 1100 Series: 1120, 1140, 1150	7.3.x and later	Cisco Secure Firewall 3100 Series: 3105, 3110, 3120, 3130, 3140	7.4.1 and later
Cisco Firepower 2100 Series: 2110, 2120, 2130, 2140	7.3.x and later	Cisco Secure Firewall 3100 Series: 3105, 3110, 3120, 3130, 3140	7.4.1 and later
Cisco Firepower 4100 Series: 4110, 4112, 4115, 4120, 4125, 4140, 4145, 4150	7.3.x and later	Cisco Secure Firewall 3100 Series: 3105, 3110, 3120, 3130, 3140	7.4.1 and later
		Cisco Secure Firewall 4200 Series: 4215, 4225, 4245	7.4.1 and later
		Cisco Secure Firewall 6100 Series: 6160, 6170	10.0 and later
Cisco Firepower 9300 Series: SM-40, SM-48, SM-56	7.3.x and later	Cisco Secure Firewall 3100 Series: 3105, 3110, 3120, 3130, 3140	7.4.1 and later
		Cisco Secure Firewall 4200 Series: 4215, 4225, 4245	7.4.1 and later
		Cisco Secure Firewall 6100 Series: 6160, 6170	10.0 and later

Source Devices	Source Device Version	Target Devices	Target Device Version
Cisco ASA 5500 Series: 5508, 5516	7.0.x	Cisco Secure Firewall 1200 Series:1210CE, 1210CP, 1210CX	7.6 and later

License for Firewall Threat Defense migration

You must meet licensing requirements for Firewall Threat Defense migration.

- Your Smart Licensing account must have the license entitlements for the target device.
- You must register and enroll the device with the Smart Licensing account. The migration copies the source device licenses to the target device.

Prerequisites for migration

This reference provides comprehensive prerequisites that must be satisfied to successfully migrate configurations from a source device to a target device in Secure Firewall Management Center environments.

General device prerequisites

- Register the source and the target devices to the Cloud-Delivered Firewall Management Center.
- Ensure that the target device is a newly registered device without any configurations.
- Source and target devices must be in the same state and modes:
  - Domain
  - Firewall mode: Routed or Transparent
  - Compliance mode (CC or UCAPL)
  - Management state

    Devices must have the same type of manager access interfaces (management interface or data interface).
  - Multi-instance mode or appliance mode
- Ensure that you have permission for modifications on the devices.
- Ensure that the configurations on the source device are valid and have no errors.
- Deployment, import, or export tasks must not run on either of the devices during the migration. The source device can have pending deployments.

Prerequisites for change management

- Ensure that source and target devices are not locked by a change management ticket.
- Ensure that shared policies assigned to the source device are not locked by a change management ticket.

Prerequisites for HA devices

- Migrate a device only from an active Cloud-Delivered Firewall Management Center.

Prerequisites for devices in multi-instance mode

- Ensure that the source and target devices are in multi-instance mode.
- Manually migrate the chassis configurations. Create instances before migrating the instance configuration to the target instances. The target device must have compatible interfaces. For example, on the target device, you must create EtherChannel interfaces, and also create tagged, untagged, dedicated, or shared interfaces for these interfaces on the target device.

Prerequisite for devices with out-of-band configurations

- Ensure that you acknowledge out-of-band changes and match the configurations within the Cloud-Delivered Firewall Management Center. You cannot migrate devices with these configurations. To view out-of-band configurations:

  1. Choose **Devices** > **Device Management**.
  2. Click the edit icon next to the device and click the **Interfaces** tab.

  or

  1. Click the edit icon next to the device and click the **Devices** tab.
  2. Verify the **Out-of-band configuration status** in the **Health** tile.

Prerequisites for devices with manager access interfaces

Ensure that the devices are not in Data Transit or Management Transit states. You cannot migrate if devices are in these states.

- Data Transit state: Device state when the manager access interface changes from data interface to management interface without deploying the changes on the device.
- Management Transit state: Device state when the manager access interface changes from management interface to data interface without deploying the changes on the device.

Prerequisite for devices with merged management and diagnostic interfaces

Ensure that the target device is always in merged mode.

Configurations that the wizard migrates

The migration wizard copies configurations from the source device to the target device, including licenses, interfaces, policies, routing settings, and other essential device configurations.

General configurations

The migration wizard copies these configurations from the source device to the target device:

- Licenses

- Interface configurations
- Inline sets configurations
- Routing configurations
- DHCP and DDNS configurations
- Policies
- Associated objects and object overrides
- Platform settings
- Remote branch deployment configurations

Policy configurations

The migration wizard copies these policy configurations from the source device to the target device:

- Health policy
- NAT and QoS policy
- Remote access VPN policy
- FlexConfig policy
- Access control and prefilter policy
- IPS and DNS policy
- Malware and File policy
- SSL and Identity policy
- Shared policy

Routing configurations

The migration wizard copies these routing configurations from the source device to the target device:

- ECMP
- BFD
- OSPFv2/v3
- EIGRP
- RIP
- BGP
- Policy Based Routing
- Static and Multicast Route
- Virtual Router

Interface configurations

The migration wizard copies these interfaces from the source device to the target device:

- Physical interfaces
- Sub-interfaces
- EtherChannel interfaces
  - On a standalone device, the wizard copies the EtherChannels from the source device to the target device.
  - For devices in multi-instance mode, you must create EtherChannels on the chassis and assign them to the instance.
- Bridge group interfaces
- VTI interfaces
- VNI interfaces
- Loopback interfaces
- VXLAN tunnel endpoint (VTEP) interfaces

The migration wizard retains the device group of the target device.

Guidelines and limitations for migration

Follow these guidelines to ensure successful migration of secure firewall threat defense models:

- **For devices in multi-instance mode**:

  During migration, ensure that you map the interfaces according to the table below:

Source Device	Target Device
Physical interface	Physical interface
EtherChannel interface	EtherChannel interface
Supervisor-provisioned subinterface	Supervisor-provisioned subinterface
Tagged interface	Tagged interface
Untagged interface	Untagged interface
Shared interface	Shared and dedicated interface
Dedicated interface	Dedicated interface

  You cannot map a supervisor-provisioned subinterface to a subinterface created by an instance.

- **For HA devices**, you can migrate:
  - Source HA device to target HA device.
  - Source HA device to target standalone device.

- **For devices in remote branch deployment**:
  - Map the source manager access interface to the target manager access interface.
  - Ensure that the manager access interfaces of the source and target Cloud-Delivered Firewall Management Centers are of the same IP address type (static or DHCP).
  - Both manager access interfaces must have IPv4 or IPv6 addresses.
  - If the manager access interfaces have static IP addresses, ensure that they are in the same subnet.
- **For Snort**:

  By default, after migration, the target device will use Snort 3, even if the source device uses Snort 2.
- **For devices using diagnostic interfaces**:

  Only merged management interfaces are available on the target devices after migration.

Limitations

Be aware of these limitations when using the migration wizard:

- The migration wizard does not migrate:
  - Site-to-site VPN policies
  - SNMP device configurations for Firepower 2100 Series

    After the migration, you can configure SNMP using the platform settings for the device.
- You can perform only one migration at a time.
- Remote access VPN trustpoint certificates are not enrolled after migration.
- For HA devices:
  - Target device: You cannot migrate a standalone device to an HA device.
- Clustering is not supported.
- For devices in remote branch deployment:
  - The wizard does not migrate a single WAN manager access data interface to a dual WAN manager access data interface.

Migrate a secure Firewall Threat Defense

Migrate a Secure Firewall Threat Defense device from a source to a target Firewall, preserving configurations and minimizing disruptions.

Before you begin

Ensure you review Prerequisites for migration, on page 13 and Guidelines and limitations for migration, on page 16 .

Procedure

Step 1 Choose **Devices** > **Device Management** .

Step 2 Click **Migrate** in the top right corner of the page.

Step 3 In **Select source and target devices** :

a) From the **Source device** drop-down list, choose a device.

b) From the **Target device** drop-down list, choose a device.

The source and target devices can have these tags:

- Routed: Devices in routed firewall mode.
- Transparent: Devices in transparent firewall mode.
- Container: Devices in multi-instance mode.
- High Availability: Devices in high availability mode.
- Analytics Only: Devices managed by Security Cloud Control and the Cloud-Delivered Firewall Management Center only recieves and displays the events (analytics-only Cloud-Delivered Firewall Management Center).

If the device is part of an HA pair, only the HA pair name appears.

Step 4 Click **Next** .

Step 5 (Only for Firepower 4100 and 9300 Series devices in appliance mode) In **Chassis manager details** :

a) Check the **Skip chassis manager** check box, if required.

b) In the **Chassis hostname or IP address** field, enter the values.

Note

- Verify that the Secure Firewall Chassis Manager is reachable from the Cloud-Delivered Firewall Management Center .
- Ensure you select the correct chassis manager for the source device, as Cloud-Delivered Firewall Management Center does not validate your choice.

c) Click **Verify certificate** to verify the chassis manager's certificate.

d) In the **Username** and **Password** fields, enter the credentials of the chassis manager.

Step 6 Click **Next** .

Step 7 In **Configure interfaces** :

By default, the source and target interfaces are mapped using the interface hardware name. You must map named interfaces, logical interfaces, and interfaces that are part of other interfaces. Mapping of all other interfaces is not mandatory. The wizard creates the logical interfaces according to the interface mapping that you provide.

You cannot map interfaces that are part of an HA failover configuration. These interfaces are disabled in the wizard.

Only data interfaces are available for interface mapping. Management, eventing, and diagnostic interfaces are not available for the interface mapping.

Firepower 4100 and 9300 Series devices in appliance mode :

For these devices, the Cloud-Delivered Firewall Management Center fetches interface attributes such as speed, duplex, and auto-negotiation from the chassis manager.

a) Click one of the following options to configure these interface attributes on the target device:

- **Retain target device values** : (Default) Retains the interface attributes configured on the target device.
- **Copy from source device** : Copies the interface attributes from the source device.

  This option is enabled only when Cloud-Delivered Firewall Management Center successfully connects to the chassis manager. We recommend that you use this option. The speed, duplex, and auto-negotiation values of physical interfaces are set to default values if they are incompatible in the target device.
- **Customize device values** —Allows you to configure the values of the required interface attributes on the target device.

b) To change the interface mapping from the default ones, choose an interface from the **Mapped interface** drop-down list.

c) For EtherChannels, you can configure interface attributes and click **Add member interface** to add member interfaces.

   Interface attributes of an EtherChannel is configured based on the first member interface's interface attributes.You can add up to 16 member interfaces.

Firepower 1100 and 2100 Series devices, and Firepower 4100 and 9300 Series devices in multi-instance mode :

For these devices, you must map the source device interfaces to target device interfaces.

For Firepower 4100 and 9300 Series devices in multi-instance mode, you can only perform the interface mapping and you cannot configure the interface attributes such as speed, duplex, auto-negotiation, and FEC mode.

If you want to change the interface mapping from the default ones, choose an interface from the **Mapped interface** drop-down list.

Click **Reset** to configure the default interface mappings. For example, the wizard maps Ethernet1/1 in the source device to Ethernet1/1 in the target device.

The interfaces can have the following tags:

- Tagged: Physical interfaces on the chassis.
- Untagged: Physical interfaces on the chassis that have sub-interfaces.
- Dedicated: Interfaces that are assigned to specific instances and are not shared across multiple instances.
- Shared: Interfaces that are shared by multiple instances.
- Manager access: Data interface is the manager access interface.

Check the **Ignore warning** check box, if required.

Step 8 Click **Next** .

Step 9 Click **Submit** to start the migration.

To view the migration status, click **Notifications** (Message Center), and then click the **Tasks** tab.

A **Device Model Migration** report is generated after the migration is completed. You will see a link to this report in the **Notifications** > **Tasks** page.

What to do next

After a successful migration, you must complete these tasks:

- Review the recommendations in Best practices for Threat Defense device migration, on page 20 .
- Validate the configurations.
- Deploy the configurations on the device.

In case of a migration failure, the target device is rolled back to the initial state.

Best practices for Threat Defense device migration

After a successful migration, perform these actions before deployment to ensure proper device configuration and functionality.

- IP addresses of the interfaces are copied to the target device from the source device. Change the IP addresses of the target device interfaces if the source device is live
- Ensure that you update your NAT policies with the modified IP addresses.
- Configure the interface speeds if they are set to default values after migration.
- Re-enroll the device certificates, if any, on the target device.
- (Optional) Configure SNMP for Firepower 1100 and 2100 using the platform settings for the device.
- (Optional) Configure remote branch deployments.

  If the source or target device had manager access through a data interface, after the migration, the manager access will be lost. Update the manager access configuration on the target device. For more information, see the *Change the Manager Access Interface from Management to Data* topic in the Cisco Secure Firewall Management Center Device Configuration Guide or the Online Help.

- Configure site-to-site VPN, if required. These configurations are not migrated from the source device.
- View the deployment preview before the deployment. From the **Deploy** drop-down menu, click **Advanced Deploy**, and then click the **Preview** ( ) icon for the device.
- Monitor the health of the device in the health monitor (choose **Troubleshooting** > **Health** > **Monitor**). After migration, the health policy of the source device becomes the health policy of the target device. You can also configure a new health policy for the device.

  After migration, the device monitoring dashboard may temporarily display redundant colored lines because the device has different UUIDs before and after migration. This redundancy appears only during the migration time. An hour after migration, the dashboard will show a single line per metric.

Use the Security Cloud Control command line interface tool

You can use the Security Cloud Control command line interface (CLI) for troubleshooting the Firewall Threat Defense and other device types.

Additional information

For more information, see the Security Cloud Control configuration guide.