Device Management

This guide applies to an *on-premises* Secure Firewall Management Center, either as your primary manager or as an analytics-only manager. When using the Cisco Security Cloud Control (Security Cloud Control) cloud-delivered Firewall Management Center as your primary manager, you can use an on-prem management center for analytics. Do not use this guide for cloud-delivered Firewall Management Center management; see Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Security Cloud Control.

You canmanage devices in the Secure Firewall Management Center.

Log Into the Command Line Interface on the Device

You can log directly into the command line interface on 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.

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.

Procedure

Step 1 Connect to the threat defense CLI, either from the console port or using SSH.

You can SSH to the management interface of the 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 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 threat defense CLI). Use the 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 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 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 two sub-modes: user EXEC and privileged EXEC mode. More commands are available in privileged 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 return to the regular CLI, type **Ctrl-a**, **d**.

Manage Devices

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

- **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 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**—

Add a Device Group

The 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.

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.

Register With a New Management Center

This procedure shows how to register with a new management center. You should perform these steps even if the new management center uses the old management center's IP address.

Procedure

Step 1 On the old management center, if present, delete the managed device.

You cannot change the management center IP address if you have an active connection with the management center.

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

Step 3 Configure the new management center.

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

- {*hostname* | *IPv4_address* | *IPv6_address*}—Sets the management center hostname, IPv4 address, or IPv6 address.
- **DONTRESOLVE**—If the 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 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 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 management center when you add the threat defense.
- *nat_id*—Make up an alphanumeric string from 1 to 37 characters used only during the registration process between the 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 management center when you add the 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 CDO as the primary manager and an on-prem 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 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 the Configuration to a New Model

The Secure Firewall Threat Defense model migration wizard enables you to migrate configurations from an old model to a new model. You can map source device interfaces to target device interfaces. Before the migration, the source and target devices are locked.

Supported Devices for Migration

Supported Source Devices

- Cisco Firepower 1120
- Cisco Firepower 1140
- Cisco Firepower 1150
- Cisco Firepower 2110
- Cisco Firepower 2120
- Cisco Firepower 2130
- Cisco Firepower 2140

Note The source devices must be version 7.0 or later.

Supported Target Devices

- Cisco Secure Firewall 3105
- Cisco Secure Firewall 3110
- Cisco Secure Firewall 3120
- Cisco Secure Firewall 3130
- Cisco Secure Firewall 3140

Note The Cisco Secure Firewall 3110, 3120, 3130, and 3140 devices must be version 7.1 or later. Cisco Secure Firewall 3105 must be version 7.3 or later.

License for Migration

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

- You must register the source and the target devices to the management center.
- Your Smart Licensing account must have the license entitlements for the target device.
- We recommend that the target device is a freshly registered device without any configurations.
- Source and target devices must be in the same:
  - Domain
  - Firewall mode: Routed or Transparent
  - Compliance mode
- The target device must not be:
  - In a multi-instance mode
  - Part of a cluster
- The user must have modify permissions on the device.
- The configurations on the source device must be valid and have no errors.
- The source device can have pending deployments. However, deployment, import, or export tasks must not run on either of the devices during the migration.
- If the source device is part of an HA pair, the target device need not be part of an HA pair and vice versa. The migration does not form or break the HA pair.

What Configurations Does the Wizard Migrate?

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

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

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

- Health policies

- NAT policies
- QoS policies
- Remote access VPN policies
- FlexConfig policies
- Access control policies
- Prefilter policies
- IPS policies
- DNS policies
- SSL policies
- Malware and File policies
- Identity policies

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

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

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

- Physical interfaces
- Sub-interfaces
- Etherchannel interfaces
- Bridge group interfaces
- VTI interfaces
- VNI interfaces
- Loopback interfaces

Limitations for Migration

- The wizard does not migrate:
  - Site-to-site VPN policies
  - SNMP configurations

    After the migration, you can configure SNMP using the platform settings for the device.
- You can perform only one migration at a time.
- If the speed, auto-negotiation, and duplex settings of the source interface are valid for the mapped interface of the target device, the values are copied. If not, these parameters are set to the default values.
- Remote access VPN trustpoint certificates are not enrolled. You must manually enroll these certificates before the deployment.
- After migration, by default, the target device uses Snort 3 and not Snort 2, even if the source device uses Snort 2.
- For HA devices:
  - Target Device: You cannot map the interfaces that are part of the failover configuration. These interfaces are disabled in the wizard.
  - Source and Target Devices: The wizard does not migrate HA configurations such as monitored interfaces, failover trigger criteria, and interface MAC addresses. You must manually configure these parameters after the migration if required.

Migrate the Secure Firewall Threat Defense

Before you begin

Review the prerequisites and limitations for the migration.

Procedure

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

Step 2 Click **Migrate** on the top-right of the page.

Step 3 Click **Start** on the welcome screen.

Step 4 From the **Source Device** drop-down list, choose a device.

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

Step 5 Click **Next**.

Step 6 From the **Target Device** drop-down list, choose a device.

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

Step 7 Click **Next**.

Step 8 In the **Configure Interfaces** step, map the physical interfaces of the source device with those of the target device.

Mapping of all interfaces is not mandatory. You must map all named interfaces and interfaces that are part of other interfaces. You cannot map interfaces that are part of an HA failover configuration. These interfaces are disabled in the wizard. The wizard creates the logical interfaces according to the interface mapping provided by the user.

- Click **Map Default** to configure default interface mappings.

  For example, Ethernet1/1 in the source device will be mapped to Ethernet1/1 in the target device.

- Click **Clear All** to clear all the mappings.

Step 9 Click **Next**.

Step 10 Click **View Mappings** to verify the interface mappings.

Step 11 Click **Submit** to start the migration.

Step 12 View the migration status in the **Notifications** > **Tasks** page.

What to do next

After a successful migration, you can deploy the device.

Deployment is not mandatory, you can validate the configurations and deploy as required. However, before the deployment ensure that you perform the actions mentioned in Best Practices for Migration, on page 11.

Best Practices for Migration

After a successful migration, we recommend that you perform the following actions before the deployment:

- Change the IP addresses of the interfaces if the source device is live, as they are copied to the target device from the source device.
- 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.
- If you have a HA setup, configure HA parameters such as monitored interfaces, failover trigger criteria, and interface MAC addresses.
- Configure the diagnostic interface as it gets reset after migration.
- (Optional) Configure SNMP using the platform settings for the device.
- (Optional) Configure remote branch deployment configurations.

  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.

- (Optional) Configure site-to-site VPN if required. These configurations are not migrated from the source device.

- View the deployment preview before the deployment. Choose **Deploy > Advanced Deploy** and click the **Preview** ( ) icon for the device.

Hot Swap an SSD on the Secure Firewall 3100/4200

If you have two SSDs, they form a RAID when you boot up. You can perform the following tasks at the threat defense CLI while the firewall is powered up:

- Hot swap one of the SSDs—If an SSD is faulty, you can replace it. Note that if you only have one SSD, you cannot remove it while the firewall is powered on.
- Remove one of the SSDs—If you have two SSDs, you can remove one.
- Add a second SSD—If you have one SSD, you can add a second SSD and form a RAID.

Caution Do not remove an SSD without first removing it from the RAID using this procedure. You can cause data loss.

Procedure

Step 1 Remove one of the SSDs.

a) Remove the SSD from the RAID.

configure raid remove-secure local-disk {**1** | **2**}

The **remove-secure** keyword removes the SSD from the RAID, disables the self-encrypting disk feature, and performs a secure erase of the SSD. If you only want to remove the SSD from the RAID and want to keep the data intact, you can use the **remove** keyword.

Example:

```
> configure raid remove-secure local-disk 2
```

b) Monitor the RAID status until the SSD no longer shows in the inventory.

show raid

After the SSD is removed from the RAID, the **Operability** and **Drive State** will show as **degraded**. The second drive will no longer be listed as a member disk.

Example:

```
> show raid
Virtual Drive
ID:                           1
Size (MB):                    858306
Operability:                  operable
Presence:                     equipped
Lifecycle:                    available
Drive State:                  optimal
```

```
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) Physically remove the SSD from the chassis.

Step 2 Add an SSD.

a) Physically add the SSD to the empty slot.

b) Add the SSD to the RAID.

configure raid add local-disk {**1** | **2**}

It can take several hours to complete syncing the new SSD to the RAID, during which the firewall is completely operational. You can even reboot, and the sync will continue after it powers up. Use the **show raid** command to show the status.

If you install an SSD that was previously used on another system, and is still locked, enter the following command:

configure raid add local-disk {**1** | **2**} *psid*

The *psid* is printed on the label attached to the back of the SSD. Alternatively, you can reboot the system, and the SSD will be reformatted and added to the RAID.

Disable the USB Port

By default, the type-A USB port is enabled. You might want to disable USB port access for security purposes. Disabling USB is supported on the following models:

- Firepower 1000 Series
- Secure Firewall 3100
- Secure Firewall 4200

Guidelines

- Enabling or disabling the USB port requires a reboot.
- If the USB port is disabled and you downgrade to a version that does not support this feature, the port will remain disabled, and you cannot re-enable it without erasing the NVRAM (the FXOS local-mgmt **erase secure all** command).
- If you perform a ROMMON **factory-reset** or FXOS local-mgmt **erase secure**, the USB port will be re-enabled.
- For high availability or clustering, you must disable or re-enable the port individually on each unit.

Note This feature does not affect the USB console port, if present.

Disable the USB Port on a Device

To disable the USB port on a device, you can do so at the threat defense CLI.

Procedure

Step 1 Disable the USB port.

system support usb configure disable

reboot

To re-enable the USB port, enter **system support usb configure enable**.

Example:

```
>system support usb configure disable
USB Port Admin State set to 'disabled'.
Please reboot the system to apply any control state changes.

>reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': YES
```

Step 2 View the port status.

system support usb show

The Admin State shows the USB port configuration. The Oper State shows the current operation. For example, if you disable the USB port but do not reload, the Admin State will show disabled while the Oper State would will enabled.

Example:

```
>system support usb show
USB Port Info
---------------
Admin State: disabled
Oper State: disabled
```

Disable the USB Port in Multi-Instance Mode

To disable the USB port in multi-instance mode, you can do so at the FXOS CLI.

Procedure

Step 1 Disable the USB port and reboot for the change to take effect.

a) Disable the USB port.

scope fabric-interconnect

disable usb-port

commit buffer

b) Reboot the chassis.

connect local-mgmt

reboot

Example:

```
firepower-4245 /fabric-interconnect # disable usb-port
Note: USB enablement or disablement changes are effected only after FXOS reboot.
```

```
Confirm change? (yes/no) [yes]:
device /fabric-interconnect* # commit buffer
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:yes
firepower-4245 /fabric-interconnect # connect local-mgmt
firepower-4245(local-mgmt)# reboot
Before rebooting, please take a configuration backup.
Do you still want to reboot? (yes/no):yes
Broadcast message from admin@firepower-4245 (Wed Feb 21 05:59:55 2024):
All shells being terminated due to system /sbin/reboot
```

Step 2 Enable the USB port and reboot for the change to take effect.

a) Enable the USB port.

scope fabric-interconnect

enable usb-port

commit buffer

b) Reboot the chassis.

connect local-mgmt

reboot

Example:

```
firepower-4245 /fabric-interconnect # enable usb-port
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:
device /fabric-interconnect* # commit buffer
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:yes
firepower-4245 /fabric-interconnect # connect local-mgmt
firepower-4245(local-mgmt)# reboot
Before rebooting, please take a configuration backup.
Do you still want to reboot? (yes/no):yes
Broadcast message from admin@firepower-4245 (Wed Feb 21 05:59:55 2024):
All shells being terminated due to system /sbin/reboot
```

Step 3 View the USB port status.

scope fabric-interconnect

show usb-port

The Admin State shows the USB port configuration. The Oper State shows the current operation. For example, if you disable the USB port but do not reload, the Admin State will show Disabled while the Oper State would will Enabled.

Example:

```
firepower-4245# scope fabric-interconnect
firepower-4245 /fabric-interconnect # show usb-port
Usb Port:
Equipment         Admin State Oper State
----------------- ----------- ----------
A                 Disabled    Disabled
```