Cisco Secure Firewall Threat Defense Model Migration Guide, Version 7.6.1

Revised: July 23, 2025

About Secure Firewall Threat Defense Model Migration

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

The wizard supports multiple models as source and target devices. For more information see Supported Devices for Migration, on page 2.

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

Supported Source Devices

- Cisco Firepower 1120
- Cisco Firepower 1140
- Cisco Firepower 1150
- Cisco Firepower 2110
- Cisco Firepower 2120
- Cisco Firepower 2130
- Cisco Firepower 2140
- Cisco Firepower 4110
- Cisco Firepower 4120
- Cisco Firepower 4140
- Cisco Firepower 4150
- Cisco Firepower 9300 Series SM-24
- Cisco Firepower 9300 Series SM-36
- Cisco Firepower 9300 Series SM-44

Note 'The source devices must be Version 7.2.x and later.

Supported Target Devices

- Cisco Secure Firewall 3105
- Cisco Secure Firewall 3110
- Cisco Secure Firewall 3120
- Cisco Secure Firewall 3130
- Cisco Secure Firewall 3140
- Cisco Firepower 4215
- Cisco Firepower 4225
- Cisco Firepower 4245

Note The target devices must be Version 7.4.1 and later.

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 Model	Target Model			
	Cisco Secure Firewall 3100 Series	Cisco Secure Firewall 4200 Series	Instance in Secure Firewall 3100 Series	Instance in Secure Firewall 4200 Series
Firepower 1100 Series	Yes	—	—	—
Firepower 2100 Series	Yes	—	—	—
Firepower 4100 Series	Yes	Yes	—	—
Firepower 9300 Series	Yes	Yes	—	—
Instance from Firepower 4100 Series	—	—	Yes	Yes
Instance from Firepower 9300 Series	—	—	Yes	Yes

License for 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

- **General device prerequisites**
  - Register the source and the target devices to the 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 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 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.
- **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.

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

- Identity policy
- Shared policy

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
  - 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
- Inline interfaces
- VXLAN tunnel endpoint (VTEP) interfaces

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

Guidelines and Limitations for Migration

Guidelines

- **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 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**:
  - If target device has Snort 3, after migration it will have Snort 3.
  - If the source and target devices have Snort 2, after migration the target device will have Snort 2.
- **For devices using diagnostic interfaces**:

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

Limitations

- 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

Before you begin

Ensure you review Prerequisites for Migration, on page 4 and Guidelines and Limitations for Migration, on page 6.

Procedure

Step 1 Choose **Firewall 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 Firewall Management Center only recieves and displays the events (analytics-only 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 Firewall Management Center.
- Ensure you select the correct chassis manager for the source device, as 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.

Firepower 4100 and 9300 Series devices in appliance mode:

For these devices, the 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 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.

Step 10 View the migration status on the **Notifications > Tasks** page.

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 10.
- 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, we recommend that you perform the following actions before the deployment:

- 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 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.
- 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.
- 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.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.