Cisco Secure Firewall Migration Tool Compatibility Guide

First Published: 2020-10-29

Last Modified: 2023-11-09

Secure Firewall Migration Tool Compatibility Guide

This guide provides Cisco Secure Firewall software and hardware compatibility, including operating system and hosting environment requirements.

Supported Platforms for Migration

The Secure Firewall migration tool supports the following ASA, ASA with FPS, FDM-managed devices, and target threat defense platforms:

Supported Source ASA Platforms

You can use the Secure Firewall migration tool to migrate the configuration from the following single or multi-context ASA platforms:

Note The Secure Firewall migration tool supports migration of standalone ASA devices to a standalone threat defense device only.

- ASA 5510
- ASA 5520
- ASA 5540
- ASA 5550
- ASA 5580
- ASA 5506
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X

- ASA 5525-X
- ASA 5545-X
- ASA 5555-X
- ASA 5585-X with ASA only (the Secure Firewall migration tool does not migrate the configuration from the ASA FirePOWER module)
- Firepower 1000 Series
- Firepower 2100 Series
- Firewall 3100 Series
- Firepower 4100 Series
- Firepower 9300 Series
  - SM-24
  - SM-36
  - SM-40
  - SM-44
  - SM-48
  - SM-56
- ASA Virtual on VMware, deployed using VMware ESXi, VMware vSphere Web Client, or vSphere standalone client

Supported Source ASA models for ASA with FPS migration:

The Cisco ASA FirePOWER module is deployed on the following devices:

Note The Secure Firewall migration tool supports migration of standalone ASA with FPS devices to a standalone threat defense device only.

- ASA5506-X
- ASA5506H-X
- ASA5506W-X
- ASA5508-X
- ASA5512-X
- ASA5515-X
- ASA5516-X
- ASA5525-X

- ASA5545-X
- ASA5555-X
- ASA5585-X-SSP-10
- ASA5585-X-SSP-20
- ASA5585-X-SSP-40
- ASA5585-X-SSP-60

Supported Source FDM-Managed Device Platforms

You can use the Secure Firewall migration tool to migrate the configuration from the following FDM-managed device platforms:

- Firepower 1000 Series
- Firepower 2100 Series
- Firewall 3100 Series
- Firepower 4100 Series
- Firepower 9300 Series
- FDM virtual on VMware, AWS, Azure, and KVM

Supported Target Threat Defense Platforms

You can use the Secure Firewall migration tool to migrate a source ASA, ASA with FPS, Check Point, PAN, and Fortinet configuration to the standalone or container instance of the following threat defense platforms:

- Firepower 1000 Series
- Firepower 2100 Series
- Firewall 3100 Series
- Firepower 4100 Series
- Firewall 4200 Series
- Firepower 9300 Series that includes:
  - SM-24
  - SM-36
  - SM-40
  - SM-44
  - SM-48
  - SM-56

- The threat defense virtual on VMware, deployed using VMware ESXi, VMware vSphere Web Client, or vSphere standalone client
- The threat defense virtual on AWS, Azure, and KVM

Supported Software Versions for Migration

The following are the ASA, ASA with FPS, Check Point, PAN, Fortinet, and threat defense versions for migration:

Supported ASA Firewall Versions

The Secure Firewall migration tool supports migration from a device that is running ASA software version 8.4 and later.

Supported ASA with FPS Firewall Versions

The Secure Firewall migration tool supports migration from a device that is running ASA with FPS software version 9.2.2+ and later.

For more details, see ASA FirePOWER Module Compatibility section in the Cisco ASA Compatibility guide.

Supported Device Manager Versions

The Secure Firewall migration tool supports migration from a device manager that is running version 7.2 or later.

Supported Check Point Firewall Versions

The Secure Firewall migration tool now supports migration to threat defense that is running Check Point OS version r75–r77.30 and r80–r80.40. Select the appropriate Check Point version in the **Select Source** page.

Note VSX is not supported.

The Secure Firewall migration rool now supports migration from the Check Point Platform Gaia.

Supported Palo Alto Networks Firewall Versions

The Secure Firewall migration tool supports migration to threat defense that is running PAN firewall OS version 6.1.x and later.

Supported Fortinet Firewall Versions

The Secure Firewall migration tool supports migration to threat defense that is running Fortinet firewall OS version 5.0 and later.

Supported Secure Firewall Management Center Versions for source ASA Configuration

For ASA, the Secure Firewall migration tool supports migration to a threat defense device managed by a management center that is running version 6.2.3 or 6.2.3+.

Note Some features are supported only in the later versions of management center and threat defense.

Note For optimum migration times, we recommend that you upgrade management center to the suggested release version that can be downloaded from: software.cisco.com/downloads.

Supported Management Center Versions for source ASA with FPS Configuration

For ASA with FPS, the Secure Firewall migration tool supports migration to a threat defense device managed by a management center that is running version 6.5+.

Supported Management Center Versions for source FDM-Managed Device Configuration

For FDM-managed devices, the Secure Firewall migration tool supports migration to a management center that is running version 7.3+.

Supported Management Center Versions for source Check Point, PAN, and Fortinet Firewall Configuration

For Check Point, PAN and Fortinet firewall, the Secure Firewall migration tool supports migration to a threat defense device managed by a management center that is running version 6.2.3.3 or later.

Note Some features are supported only in the later versions of management center and threat defense. For example, Time-based ACLs in Fortinet is supported from management center 6.6 or later.

Note The migration to 6.7 threat defense device is currently not supported. Hence, migration may fail if the device is configured with data interface for management center access.

Supported Threat Defense Versions

The Secure Firewall migration tool recommends migration to a device that is running threat defense, version 6.2.3 and later.

For detailed information about the Secure Firewall software and hardware compatibility information, including operating system and hosting environment requirements, for threat defense, see the Cisco Secure Firewall Compatibility Guide.

Platform Requirements for the Secure Firewall Migration Tool

The Secure Firewall migration tool has the following infrastructure and platform requirements:

- Runs on a Microsoft Windows 10 64-bit operating system or on a macOS version 10.13 or higher
- Has Google Chrome as the system default browser

- (Windows) Has Sleep settings configured in Power & Sleep to Never put the PC to Sleep, so the system does not go to sleep during a large migration push
- (macOS) Has Energy Saver settings configured so that the computer and the hard disk do not go to sleep during a large migration push

Related Documentation

This section summarizes the Secure Firewall migration tool related documentation.

- Cisco Secure Firewall Threat Defense Compatibility Guide—Describes Cisco Firewall software and hardware compatibility, including operating system and hosting environment requirements.
- Cisco ASA Compatibility—Lists the Cisco ASA software and hardware compatibility and requirements.
- Cisco Firepower 4100/9300 FXOS Compatibility—Lists software and hardware compatibility information for the FXOS, Cisco Firepower 9300 and Cisco Firepower 4100 series security appliances, and supported logical devices.