Navigating the Cisco Secure Firewall Migration Tool Documentation

First Published: 2020-06-08

Last Modified: 2023-02-02

Navigating the Secure Firewall Migration Tool Documentation

About Secure Firewall Migration Tool

The Secure Firewall migration tool converts the supported ASA, ASA with FPS, FDM-managed devices, Check Point, Palo Alto Network (PAN), and Fortinet Firewall configuration to a supported Secure Firewall Threat Defense platform. While you can automate migration of the supported features and policies, you need to manually configure the unsupported features.

Overview of the Secure Firewall Migration Tool Documentation

Overview of the Secure Firewall migration tool—Information on *Migrating ASA, ASA with FPS, FDM-managed devices, Check Point (CP), Palo Alto Networks (PAN) or Fortinet to threat defense with the Secure Firewall migration tool* refers to the most recent version of Secure Firewall migration tool. Follow the instructions in Download the Secure Firewall Migration Tool from Cisco.com to download the most recent version of the Secure Firewall migration tool.

The Firewall Migration Tool gathers the ASA, ASA with FPS, FDM-managed device, Check Point, PAN, or Fortinet information, parses it, and pushes it to the Secure Firewall Management Center. During the parsing phase, the Secure Firewall migration tool generates a **Pre-Migration Report**. The document covers information about the Secure Firewall migration tool, right from downloading the Firewall migration tool to completing the migration. The document also provides troubleshooting tips to help you overcome migration issues.

Secure Firewall Migration Tool Software Download Page—Download the most recent version of the software from the software download page. For more information, see Download the Secure Firewall Migration Tool from Cisco.com.

Secure Firewall Migration Tool Release Notes

Cisco Secure Firewall Migration Tool Release Notes—This document provides critical and release-specific information.

Migrating Secure Firewall ASA to Threat Defense

You can use the Secure Firewall migration tool to migrate supported source configurations to supported threat defense configurations for firewall releases 6.2.3 and later.

Migrating Secure Firewall ASA to Threat Defense with the Migration Tool—This document describes the procedure to convert the supported ASA configuration to a supported threat defense platform managed by

management center or cloud-delivered Firewall Management Center. With the Secure Firewall migration tool, you can automate the migration of supported ASA features and policies.

The following documents are related to migration of ASA to threat defense:

- Migrating Certificates from ASA to Threat Defense—Describes the procedure to migrate Identity (ID) and Certificate Authority (CA) Certificates from Cisco ASA to the threat defense device.
- Migrating ASA to Threat Defense Site-to-Site VPN Using IKEv1 with Certificates—Describes the procedure to migrate site-to-site IKEv1 VPN tunnels, using certificates (rsa-sig) as a method of authentication, from the existing ASA to threat defense, managed by the management center.
- Migrating ASA to Threat Defense Site-to-Site VPN Using IKEv2 with Certificates—Describes the procedure to migrate site-to-site IKEv2 VPN tunnels, using certificates (rsa-sig) as a method of authentication, from the existing ASA to threat defense, managed by the management center.
- Migrating ASA to Threat Defense Dynamic Crypto Map Based Site-to-Site Tunnel on Threat Defense—Describes the procedure to migrate site-to-site VPN tunnels, based on Dynamic Crypto Maps (with IKEv1 or IKEv2), using pre-shared key and certificate as a method of authentication, from the existing ASA to threat defense, managed by the management center.
- Migrating ASA to Threat Defense Site-to-Site VPN Using IKEv1 with Pre-Shared Key Authentication—Describes the procedure to migrate Site-to-Site IKEv1 VPN tunnels, using pre-shared key (PSK) as a method of authentication, from the existing ASA to threat defense, managed by management center.
- Migrating ASA to Threat Defense Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication—Describes the procedure to migrate site-to-site IKEv2 VPN tunnels, using pre-shared key (PSK) as a method of authentication, from the existing ASA to threat defense, managed by the management center.
- Migrating ASA to Threat Defense Platform Settings—Describes the steps to migrate the platform setting configuration of ASA to threat defense devices.

Migrating an ASA with FirePOWER Services (FPS) Firewall to Threat Defense

Migrating ASA with FirePOWER Services (FPS) to Secure Firewall Threat Defense with the Migration Tool—This document describes the procedure to convert the supported ASA with FPS configuration to a supported threat defense platform managed by management center or cloud-delivered Firewall Management Center. With the Secure Firewall migration tool, you can automate the migration of supported ASA with FPS features and policies.

Migrating an ASA Firewall to an FDM-Managed Device Managed by Cisco Defense Orchestrator

Migrating an ASA to an FDM-Managed Device Using Cisco Defense Orchestrator—This document describes the procedure to migrate the ASA to an FDM-managed device. CDO provides a wizard to help you migrate the elements of the ASA's running configuration to an FDM-managed device template.

Migrating an FDM-Managed Device to Threat Defense

Migrating an FDM-Managed Device to Secure Firewall Threat Defense with the Migration Tool—This document describes the procedure to convert the supported FDM-managed device configuration to a threat defense platform managed by management center or cloud-delivered Firewall Management Center. With the

Secure Firewall migration tool, you can automate the migration of supported FDM-managed device features and policies.

Migrating a Check Point Firewall to Threat Defense

Migrating a Check Point Firewall to Secure Firewall Threat Defense with the Migration Tool—This document describes the procedure to convert the supported Check Point configuration to a supported threat defense platform managed by management center or cloud-delivered Firewall Management Center. With the Secure Firewall migration tool, you can automate the migration of supported Check Point features and policies.

Migrating a Palo Alto Networks (PAN) Firewall to Threat Defense

Migrating a Palo Alto Networks Firewall to Secure Firewall Threat Defense—This document describes the procedure to convert the supported PAN configuration to a supported threat defense platform managed by management center or cloud-delivered Firewall Management Center. With the Secure Firewall migration tool, you can automate the migration of supported PAN features and policies.

Migrating a Fortinet Firewall to Threat Defense

Migrating a Fortinet Firewall to Secure Firewall Threat Defense with the Migration Tool—This document describes the procedure to convert the supported Fortinet configuration to a supported threat defense platform managed by management center or cloud-delivered Firewall Management Center. With the Secure Firewall migration tool, you can automate the migration of supported Fortinet features and policies.

Secure Firewall Migration Tool Compatibility Guide

Secure Firewall Migration Tool Compatibility Guide—This document lists the Secure Firewall migration tool System software and hardware compatibility and requirements.

Secure Firewall Migration Tool Error Messages

Secure Firewall Migration Tool Error Messages—This document provides the error messages and the workarounds for the errors that could occur during the migration.

Secure Firewall Migration Tool Open Source

Secure Firewall Migration Tool Open Source Documentation—This document lists the licenses and notices for open source software used during the migration.