

Release Notes for Firewall Migration Manager, Release 10.1.0

Contents

Firewall Migration Manager, Release 10.1.0..... 3

New software features 3

Release features overview video..... 3

System requirements 4

Supported platforms 4

Supported configuration elements for migration 4

Migration limitations..... **Error! Bookmark not defined.**

Related resources..... 4

Legal information 5

Firewall Migration Manager, Release 10.1.0

Firewall Migration Manager is a network security application with functionality that supports firewall infrastructure transitions, including configuration parsing, feature mapping, policy deployment, and validation. The application includes automated workflows, intelligent rule optimization, and a unified wizard-driven interface to help ensure accuracy, efficiency, and consistency in your network security modernization efforts.

This document describes new features, release-specific details, limitations, and guidelines for the Firewall Migration Manager, Release 10.1.0.

Table 1. Change history to this document since its initial release

Date	Change
July 22, 2026	Initial release
August 18, 2026	Support for Palo Alto Networks firewall to Firewall Threat Defense migration
October 15, 2026	<ul style="list-style-type: none">• Support for Check Point firewall to Firewall Threat Defense migration• Support for Fortinet firewall to Firewall Threat Defense migration

New software features for Release 10.1.0

Firewall Migration Manager, Release 10.1.0 supports:

- Check Point firewall to Firewall Threat Defense migration
- Fortinet firewall to Firewall Threat Defense migration
- Improved site-to-site (S2S) VPN migration
- Network address translation (NAT) zone mapping with route lookup
- External dynamic list (EDL) migration for Palo Alto Networks firewalls
- Panorama-based policy hierarchy migration for Palo Alto Networks firewalls
- Virtual IP (VIP) group migration for Fortinet firewalls

Overview video of Firewall Migration Manager

Watch the release overview video to learn about the new capabilities, features, and benefits included in this update. Access the video here: [Firewall Migration Manager – Release Overview](#).

We recommend you watch this video to gain a thorough understanding of the release and optimize your experience with the new product.

Download the Firewall Migration Manager

Step 1. Browse to [Cisco Software Download Center](#) and click **Firewall Migration Manager**.

Step 2. Download the most recent version of the Firewall Migration Manager.

System requirements

These system requirements must be met to use the Firewall Migration Manager and to deploy features successfully to the target Firewall Management Center:

- **Operating System:** Microsoft Windows 11 (64-bit) or macOS (version 14 or later).
Note: If you want to perform migration in an air-gapped or isolated environment without internet access, contact Cisco TAC to obtain the air-gapped Firewall Migration Manager installer.
- **Browser:** Google Chrome (must be set as the system default).
- **Licensing:** The Firewall Migration Manager application is free. However, the target Firewall Management Center must be properly licensed for the Firewall Threat Defense features you intend to deploy.
- **Connectivity:** IP network connectivity is required to extract configurations (Live Connect).

Supported platforms

To avoid compatibility or deployment issues, ensure that you use only the supported platforms for Firewall Migration Manager migration. Refer:

- For more information on supported platforms for ASA to Threat Defense migration, refer to [Supported ASA and Threat Defense platforms](#).
- For information on supported platforms for Palo Alto Networks firewall to Threat Defense migration, see [Supported platforms and versions](#).
- For information on supported platforms for Check Point to Threat Defense migration, refer to [Supported platforms and versions](#).
- For information on supported platforms for Fortinet to Threat Defense migration, refer to [Supported platforms and versions](#).

Note: Refer to the [Cisco Secure Firewall Management Center Compatibility Guide](#) and [Cisco Secure Firewall Threat Defense Compatibility Guide](#) for the most granular list of supported hardware and software versions.

Supported configuration elements for migration

For information on the supported configurations of the Firewall Migration Manager, refer to the link below:

- [Supported ASA configurations](#)
- [Supported Palo Alto Networks firewall configurations](#)
- [Supported Check Point firewall configurations](#)
- [Supported Fortinet configurations](#)

Related resources

This section lists the resources that provide important information for working with Firewall Migration Manager.

Links to Firewall Migration Manager documents:

-
- [Migrating Firewall ASA to Cisco Secure Firewall Threat Defense Using Firewall Migration Manager](#)
 - [Migrating Firewall PAN to Cisco Secure Firewall Threat Defense Using Firewall Migration Manager](#)
 - [Migrating Check Point Firewall to Cisco Secure Firewall Threat Defense Using Firewall Migration Manager](#)
 - [Migrating Fortinet Firewall to Cisco Secure Firewall Threat Defense Using Firewall Migration Manager](#)
 - [Firewall Migration Manager Troubleshooting Guide](#)

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2026 Cisco Systems, Inc. All rights reserved