Release Notes for Firewall Migration Manager, Release 10.0.0

Contents

Firewall Migration Manager, Release 10.0.0 3
New software features 3
Release features overview video 4
System requirements 4
Supported ASA and Firewall Threat Defense platforms 4
Supported configuration elements for migration 4
Migration limitations 5
Related resources 5
Legal information 5

© 2026 Cisco and/or its affiliates. All rights reserved.

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 10.0.0.

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

Date	Change	Location
2026-07-22	Initial release	_

New software features

Table 2. New software features for Firewall Migration Manager, Release 10.0.0

Product impact	Feature	Description
Base functionality	Auto-detection of target versions	Automatically identifies target device version and information for Secure Firewall Management Center and Secure Firewall Threat Defense to ensure accurate configuration alignment.
	Automated migration workflow	The Firewall Migration Manager reduces manual effort with automated transition of security policies, network objects, and device configurations from your existing environment to Secure Firewall Threat Defense.
	Centralized dashboard support	The Firewall Migration Manager dashboard provides a unified, intuitive interface to streamline your migration journey. Designed to improve visibility and operational efficiency, the dashboard offers the following: • **Migration Summary**: Monitors the status of migration projects in real-time and displays number of Completed, In-Progress, and Failed migrations. • **Recent Alerts**: This section provides visibility into recent migration alerts and project details. You can resume the in-progress migration task from where you left by clicking the **Details** hyperlink. • **Quick links**: You can access critical resources directly from the dashboard, including pre-migration checklists, comprehensive video guides, and one-click support ticket creation. This centralized approach simplifies the transition from third-party or legacy firewalls to next-generation Cisco firewall platforms, ensuring a more organized and manageable migration process.
	Improved GUI	The Firewall Migration Manager provides an intuitive graphical user interface that unifies migration tasks in a wizard-driven orchestration platform. This improves visual clarity, process tasks in parallel, and monitor status proactively.
	Intelligent parsing	This feature automatically scans your configurations to identify items that are either unsupported or unreferenced. This helps you save time by focusing your manual cleanup efforts only on the items that require attention. Parses enterprise-scale configurations efficiently, handling thousands of rules in minutes.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	Migration history retention	Keeps migration history across different projects so you can track and revisit previous migrations.
	Parallel migration support	To improve efficiency, this feature allows you to run up to 10 migration processes simultaneously, enabling bulk handling of your network transitions.
	Pause and resume	The Firewall Migration Manager allows tasks to be paused and resumed at any point without data loss. In-Progress can be accessed from the **Recent Alerts** tile on the home page or by clicking **Migration** under the main menu.

Release features overview video

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.

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 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) or to push policies to the Cloud-hosted Management Center.

Supported ASA and Firewall Threat Defense platforms

To avoid compatibility or deployment issues, ensure that you use only the supported ASA and Firewall Threat Defense platforms for Firewall Migration Manager migration. For more information, see Supported ASA and Threat Defense platforms.

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:

© 2026 Cisco and/or its affiliates. All rights reserved.

Supported ASA configuration: Supported, partially supported and unsupported configurations.

Migration limitations

The following considerations apply when migrating from ASA to Firewall Threat Defense devices using Firewall Migration Manager:

- **Manual tasks**: Certain configurations, such as ASA trustpoint or certificate migration and specific AnyConnect profile uploads, must be performed manually as part of pre-migration activities.
- **Unsupported configurations**: Some configurations, such as user-based access control, specific NAT configurations, or transport mode IPsec, are not supported. These must be configured manually on the Firewall Threat Defense device after migration. Refer to Supported configuration elements for migration for supported configuration.
- **Device pre-staging**: For native Firewall Threat Defense devices, make sure your target device has at least as many physical or port channel interfaces as the source ASA before you start the migration.

For more information, see Migration guidelines and limitations.

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
- 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