Cisco Secure Firewall Migration Tool Release Notes, 10.0.1

First Published: 2026-01-23

About Secure Firewall Migration Tool

The Secure Firewall Migration Tool enables you to migrate your firewall configurations to a supported Secure Firewall Threat Defense managed by a management center. The migration tool supports migration from Secure Firewall ASA, ASA with FirePOWER Services (FPS), FDM-managed devices, as well as third-party firewalls from Microsoft Azure, Check Point, Palo Alto Networks, and Fortinet.

This document provides critical and release-specific information about the Secure Firewall Migration Tool. Even if you are familiar with Secure Firewall releases and have previous experience with the migration process, we recommend that you read and thoroughly understand this document.

New Features

Note Currently the new features are available only on the cloud version of the Cisco Secure Firewall Migration Tool hosted on Firewall in Security Cloud Control platform.

Release Version	Feature	Descriptions
10.0.1	Support for Migrating DHCP and DNS Configurations	You can now migrate DHCP and DNS configurations using the Secure Firewall Migration Tool. Supported migration: Check Point Firewall to Firewall Threat Defense
	Application Detector Support	The migration tool now features an enhanced Application Mapping screen. This improvement simplifies the migration of application configurations to Firewall Threat Defense. Supported migration: Check Point Firewall to Firewall Threat Defense
	Migration Support for Check Point SMB Devices	Added support for migrating firewall configuration from Check Point Small and Medium Business (SMB) devices to Cisco Secure Firewall Threat Defense.
	Attribute Count Removed from Parsed Summary Page	The Firewall Migration Tool does not display attribute counts on the **Parsed Summary** page during the pre-parsing phase. This change improves clarity and streamlines the migration process. Supported migration: All
	Migration Support for ASA 55XX-X Series Devices Running Firewall Threat Defense to Firewall Threat Defense Devices.	You can now migrate configurations from Cisco Adaptive Security Appliance (ASA) 55XX-X Series devices running Firewall Threat Defense to Firewall Threat Defense devices, such as Cisco Firewall 1000, 2000, 3000, 4000, 6000, and 9000 Series devices.

Open and Resolved Issues

Resolved Issues

Bug ID	Description
CSCwq41034	When migrating from Check Point to Firewall Threat Defense using the Firewall Migration Tool, the **Map FTD Interface** page displays incorrect port channel details. The **Optimize, Review and Validate Configuration** page displays the correct port channel details.
CSCwq32261	Migration from ASA to Firewall Threat Defense using the Firewall Migration Tool fails at the parsing stage.
CSCwr02050	The **Object Group Search** functionality is not working as expected.

Open and Resolved Caveats

The open caveats for this release can be accessed through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you don't have one, you can register for an account on Cisco.com. For more information on Bug Search Tool, see Bug Search Tool Help.

Use the Open and Resolved Caveats dynamic query for an up-to-date list of open and resolved caveats in Secure Firewall migration tool.

Supported Configurations

For information on the supported configurations of the Secure Firewall Migration Tool, refer to the links below:

- Supported Azure Configurations
- Supported ASA Configurations
- Supported ASA with FirePOWER Services Configurations
- Supported Check Point Configurations
- Supported PAN Configurations
- Supported Fortinet Configuration
- Supported FDM-Managed Device Configuration

Infrastructure and Platform Requirements

The Secure Firewall migration tool requires the following infrastructure and platform:

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

Tip We recommend that you use full screen mode on the browser when using the migration tool.

- A single instance of the Secure Firewall migration tool per system
- Management Center and Threat Defense must be version 6.2.3.3 or later

Note Remove the previous build before downloading the newer version.

Related Documentation

For information on the history of Secure Firewall Migration Tool, see:

- History of the ASA Firewall Migration Tool
- History of the ASA with FirePOWER Services Firewall to Threat Defense with the Firewall Migration Tool
- History of the Check Point Firewall Migration Tool
- History of the Palo Alto Networks Firewall Migration Tool
- History of the Fortinet Firewall Migration Tool
- History of the FDM-Managed Device Migration Tool

Migration Workflow

For information on the migration workflow of the Secure Firewall migration tool, see:

- Export the ASA Configuration File
- Export the ASA with FirePOWER Services Configuration File
- Export the Microsoft Azure Native Firewall Configuration File
- Export the Check Point Configuration Files
- Export the Configuration from Palo Alto Networks Firewall
- Export the Configuration from Fortinet Firewall
- Export the FDM-Managed Device Configuration File

Migration Reports

The Secure Firewall migration tool provides these reports in HTML format with details of the migration:

- Pre-Migration Report
- Post-Migration Report

Secure Firewall Migration Tool Capabilities

The Secure Firewall migration tool provides these capabilities:

- Validation throughout the migration, including parse and push operations
- Object re-use capability
- Object conflict resolution

- Interface mapping
- Auto-creation or reuse of interface objects (ASA name if to security zones and interface groups mapping)
- Auto-creation or reuse of interface objects
- Auto-zone mapping
- User-defined security zone and interface-group creation
- User-defined security zone creation
- Subinterface limit check for the target threat defense device
- Platforms supported:
  - ASA Virtual to Threat Defense Virtual
  - FDM Virtual to Threat Defense Virtual
  - Same hardware migration (X to X device migration)
  - X to Y device migration (Y having higher number of interfaces)
- ACL optimization for source ASA, FDM-managed device, Fortinet, and Checkpoint for ACP rule action.

Link to Firewall Migration Tool Documents

- Navigating the Cisco Secure Firewall Migration Tool Documentation
- Migrating ASA Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating ASA Firewall with FirePOWER Services to Firewall Threat Defense with the Secure Firewall Migration Tool
- Cisco Secure Firewall ASA to Threat Defense Feature Mapping
- Migrating an FDM-Managed Device to Secure Firewall Threat Defense with the Migration Tool
- Migrating Microsoft Azure Native Firewall to Cisco Secure Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating Check Point Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating Fortinet Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating Cisco Secure Firewall ASA to Cisco Multicloud Defense with the Migration Tool
- Palo Alto Networks to Cisco Secure Firewall Threat Defense Migration Prerequisites Guide
- Migrating Palo Alto Networks Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating Palo Alto Networks Firewall to Cisco Multicloud Defense with the Migration Tool
- Cisco Secure Firewall Migration Tool Compatibility Guide
- Secure Firewall Migration Tool Best Practices Guide