Cisco Secure Firewall Migration Tool Release Notes, 7.7.10.2

First Published: 2025-09-04

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

Release Version	Feature	Descriptions
7.7.10.2	Patch release	This patch release contains bug fixes. See Open and Resolved Issues, on page 6 for more information.

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

Release Features Overview Video

To help you understand the key capabilities and enhancements introduced in this release, we have created a comprehensive video, Cisco Secure Firewall Migration Tool 7.7.10.1, 7.7.10.2 – Release Overview. The video highlights new features, improvements, and practical usage scenarios. It provides a clear and concise way to understand the benefits of the update. We recommend you to watch this video to gain a thorough understanding of the release and optimize your experience with the updated product.

Supported Configurations

The following configuration elements are supported for migration:

- Network objects and groups
- Service objects, except for those service objects configured for a source and destination

Note Although the Secure Firewall migration tool does not migrate extended service objects (configured for a source and destination), referenced ACL and NAT rules are migrated with full functionality.

- Service object groups, except for nested service object groups

Note Because nesting is not supported on the management center, the Secure Firewall migration tool expands the content of the referenced rules. The rules, however, are migrated with full functionality.

- IPv4 and IPv6 FQDN objects and groups
- IPv6 conversion support (Interface, Static Routes, Objects, ACL, and NAT)
- Access rules that are applied to interfaces in the inbound direction and global ACL
- Auto NAT, Manual NAT, and object NAT (conditional)
- Static routes, ECMP routes, and PBR
- Physical interfaces
- Secondary VLANs on ASA or ASA with FirePOWER Services interfaces will not migrate to Firepower Threat Defense.
- Subinterfaces (subinterface ID will always be set to the same number as the VLAN ID on migration)
- Port channels
- Virtual tunnel interface (VTI)
- Bridge groups (transparent mode only)
- IP SLA Monitor

  The Secure Firewall migration tool creates IP SLA objects, maps the objects with the specific static routes, and migrates these objects to FMC.

Note IP SLA Monitor is not supported for non-Firepower Threat Defense flow.

- Object Group Search

Note

- Object Group Search is unavailable for FMC or Firepower Threat Defense version earlier than 6.6.
- Object Group Search will not be supported for non-Firepower Threat Defense flow and will be disabled.

- Time-based objects

Note

- You must manually migrate timezone configuration from source ASA, ASA with FirePOWER Services, and FDM-managed device to target Firepower Threat Defense.
- Time-based object is not supported for non-Firepower Threat Defense flow and will be disabled.
- Time-based objects are supported on FMC version 6.6 and above.

- Site-to-Site VPN Tunnels
  - Site-to-Site VPN—When the Secure Firewall migration tool detects crypto-map configuration in the source ASA and FDM-managed device, the Secure Firewall migration tool migrates the crypto-map to FMC VPN as point-to-point topology
  - Site-to-site VPN from Palo Alto Networks and Fortinet firewalls
  - Crypto map (static/dynamic) based VPN from ASA and FDM-managed device
  - Route-based (VTI) ASA and FDM VPN
  - Certificate-based VPN migration from ASA, FDM-managed device, Palo Alto Networks, and Fortinet firewalls.
  - ASA, FDM-managed device, Palo Alto Networks, and Fortinet trustpoint or certificates migration to FMC must be performed manually and is part of the pre-migration activity.
- Dynamic Route objects, BGP, and EIGRP
  - Policy-List
  - Prefix-List
  - Community-List
  - Autonomous System (AS)-Path
  - Route-Map
- Remote Access VPN
  - SSL and IKEv2 protocol.
  - Authentication methods—AAA only, Client Certificate only, SAML, AAA, and Client Certificate.

- AAA—Radius, Local, LDAP, and AD.
- Connection Profiles, Group-Policy, Dynamic Access Policy, LDAP Attribute Map, and Certificate Map.
- Standard and Extended ACL.
- RA VPN Custom Attributes and VPN load balancing
- As part of pre-migration activity, perform the following:
  - Migrate the ASA, FDM-managed device, Palo Alto Networks, and Fortinet firewall trustpoints manually to the FMC as PKI objects.
  - Retrieve AnyConnect packages, Hostscan Files (Dap.xml, Data.xml, Hostscan Package), External Browser package, and AnyConnect profiles from the source ASA and FDM-managed device.
  - Upload all AnyConnect packages to the FMC.
  - Upload AnyConnect profiles directly to the FMC or from the Secure Firewall migration tool.
  - Enable the **ssh scopy enable** command on the ASA to allow retrieval of profiles from the Live Connect ASA.

- ACL optimization

  ACL optimization supports the following ACL types:

  - Redundant ACL—When two ACLs have the same set of configurations and rules, then removing the non-base ACL will not impact the network.
  - Shadow ACL—The first ACL completely shadows the configurations of the second ACL.
  - Disable ACL—The ACL that has been explicitly turned off in the firewall's configuration. The rules exist in the configuration file, but the Secure Firewall Migration Tool ignores them when processing traffic.

Note ACL optimization is currently not available for Palo Alto Networks and ASA with FirePower Services (FPS).

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

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

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 the following 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 the following 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.

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.

Open and Resolved Issues

Resolved Issues

Bug ID	Description
CSCwq29668	Adaptive Security Appliance (ASA) migration in Secure Firewall Migration Tool fails when the management interface is configured in converged mode.
CSCwq29698	ASA migration in Secure Firewall Migration Tool fails during cleanup, when existing OSPF/EIGRP configurations reference sub-interfaces. The migration fails with the following error: • Object deletion restricted for "inside" • 'The existing configurations on the FMC has caused push failure'
CSCwq48239	FDM-managed device migration in Secure Firewall Migration Tool ignores ports and applications from ACL and NAT during FDM to FMC shared configuration migration.
CSCwq57319	Unable to parse the ASA configuration in Secure Firewall Migration Tool.

Bug ID	Description
CSCwq61828	ASA migration in Secure Firewall Migration Tool fails while mapping FTD interfaces, if FMC is authenticated externally.
CSCwq70453	For Check Point Firewall migration in Secure Firewall Migration Tool, Crypto Extended ACLs fail to migrate to FMC.
CSCwq79523	When migrating from ASA to FTD using the Secure Firewall Migration Tool, the tool deletes Site-to-Site (S2S) VPN topologies from non-targeted FTD devices.
CSCwq91920	When migrating a Check Point (CP) firewall in Secure Firewall Migration Tool, configuration extraction fails during CP live connect.

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.

Related Documentation

- 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 Palo Alto Networks 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
- Migrating Palo Alto Networks Firewall to Cisco Multicloud Defense with the Migration Tool
- Cisco Secure Firewall Migration Tool Compatibility Guide