Cisco Secure Firewall Migration Tool Release Notes

First Published: 2023-03-14

Last Modified: 2024-10-21

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 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
7.0.1	Support for Cisco Secure Firewall 1200 Series devices	You can now migrate configurations from your Cisco firewalls such as ASA and FDM-managed devices, and third-party firewalls to Cisco Secure Firewall 1200 Series devices. See: Cisco Secure Firewall 1200 Series
	Bulk update preshared keys for site-to-site VPN migrations	You can now update the preshared keys for more than one site-to-site VPN tunnel configuration at once. Export the site-to-site VPN table in the **Optimize, Review and Validate Configuration** page to an Excel sheet, specify the preshared keys in the respective cells, and upload the sheet back. The migration tool reads the preshared keys from the Excel and updates the table. See: Optimize, Review, and Validate the Configuration Supported migrations: All
	Configuration push enhancements	You can now choose to ignore migration-hindering, incorrect configurations and still continue the final push of a migration. In earlier releases, the whole migration failed even if a single object's push failed because of errors. You also now have the control to abort the migration manually to fix the error and retry migration. See: Push the Migrated Configuration to Management Center Supported migrations: All
	Improved site-to-site VPN migrations	The Secure Firewall migration tool now detects existing site-to-site VPN configurations in the target threat defense device. It prompts you to choose if you want them deleted, without having to log in to the management center. You could choose **No** and manually delete them from the management center to continue with the migration. See: Optimize, Review, and Validate the Configuration Supported migrations: All
	Improved site-to-site VPN migrations	If you have an existing hub and spoke topology configured on one of the threat defense devices managed by the target management center, you could choose to add your target threat defense device as one of the spokes to the existing topology right from the migration tool, without having to manually do it on the management center. See: Optimize, Review, and Validate the Configuration Supported migrations: Secure Firewall ASA

Release Version	Feature	Descriptions
	High-availability support for third-party firewall migrations	When migrating thrid-party firewalls, you can now select threat defense devices as target, which are part of a high availability pair. In earlier releases, you could only choose standalone threat defense devices as target devices. Supported migrations: Palo Alto Networks, Check Point, and Fortinet firewall migrations
	Enhanced demo mode	The Secure Firewall migration tool now provides a more enhanced, intuitive demo mode, with guided migration instructions at every step. In addition, you can also see versions of target threat defense devices to choose and test based on your requirements. Supported migrations: All
7.0.0.1	Patch release	This patch release contains bug fixes. See Open and Resolved Issues for more information.
7.0	Secure Firewall ASA migration enhancements	• You can now configure a threat defense high availability (HA) pair on the target management center and migrate configurations from a Secure Firewall ASA HA pair to the management center. See Specify Destination Parameters for the Secure Firewall Migration Tool in the *Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool* book for more information. • You can now configure a site-to-site hub and spoke VPN topology using threat defense devices when migrating site-to-site VPN configurations from an ASA device. See Optimize, Review, and Validate the Configuration in the *Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool* book for more information.
	Fortinet firewall migration enhancements	You can now migrate IPv6 and multiple interface and interface zones in SSL VPN and central SNAT configurations from a Fortinet firewall to your threat defense device. See Fortinet Configuration Support in *Migrating Fortinet Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool* book 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

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 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 management center.

Note IP SLA Monitor is not supported for non-threat defense flow.

- Object Group Search

Note

- Object Group Search is unavailable for management center or threat defense version earlier than 6.6.
- Object Group Search will not be supported for non-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 threat defense.
- Time-based object is not supported for non-threat defense flow and will be disabled.
- Time-based objects are supported on management center 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 management center 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 management center 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 management center 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 management center.
  - Upload AnyConnect profiles directly to the management center 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.

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 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

Open Issues

Bug ID	Description
CSCwm86791	ASA virtual routing and forwarding interfaces clean fails during migration.
CSCwm85574	ASA relay interfaces clean fails during migration.
CSCwm86781	ASA security zones push error

Resolved Issues

This list includes all the caveats that were resolved as part of 7.0.1 release of the Cisco Secure Firewall Migration Tool.

Bug ID	Description
CSCwk98316	Migration of ASA remote access VPN configurations fails at parsing stage.

Bug ID	Description
CSCwk84332	ASA migration error while migrating interface configurations. 'Invalid value for VLAN ID' error message is shown.
CSCwk84159	ASA migration error while migrating interface configurations. 'Duplicate subinterface ID' error message is shown.
CSCwk81346	ASA remote access VPN dynamic access policies do not get migrated to FMC.
CSCwk73500	Migration of access lists containing multiple security zones fails.
CSCwm12311	Fortinet migration fails at parsing stage.
CSCwm65269	FDM-managed device migration does not let the original destination be configured as any/any-ipv4/any-ipv6. .
CSCwm65285	ASA migration fails while pushing policy-based routing configurations.
CSCwm65415	ASA migration throws error while parsing.

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

- 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 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 an ASA to an FDM-Managed Device Using Cisco Defense Orchestrator
- Navigating the Cisco Secure Firewall Migration Tool Documentation
- Cisco Secure Firewall Migration Tool Compatibility Guide
- Cisco Secure Firewall Migration Tool Error Messages
- Open Source Used in Cisco Secure Firewall Migration Tool