Cisco Secure Firewall Migration Tool Release Notes

First Published: 2023-03-14

Last Modified: 2024-09-05

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	New Features
7.0.0.1	This patch release contains bug fixes. See Open and Resolved Issues for more information.
7.0	**Cisco Secure Firewall ASA to Threat Defense Migration** • 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 to Cisco Secure Firewall Threat Defense Migration** • 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.

Release Version	New Features
6.0.1	**Notifications Center** You can use the new notifications center to go back and check all the notification messages that the Firewall Migration Tool sent you at any point during your migration. These notifications are categorized as **Successes**, **Warnings**, and **Errors**, and also indicate the time they were sent.
	Cisco Secure Firewall ASA to Threat Defense Migration You can now optimize network and port objects when you migrate configurations from Secure Firewall ASA to threat defense. Review these objects in their respective tabs in the **Optimize, Review and Validate Configuration** page and click **Optimize Objects and Groups** to optimize your list of objects before migrating them to the target management center. See Optimize, Review, and Validate the Configuration in the *Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool* guide for more information.
	FDM-Managed Device to Cisco Secure Firewall Threat Defense Migration You can now migrate DHCP, DDNS, and SNMPv3 configurations from your FDM-managed device to a threat defense device. Ensure you check the **DHCP** checkbox and **Server**, **Relay**, and **DDNS** checkboxes on the **Select Features** page. See Optimize, Review, and Validate the Configuration in the *Migrating an FDM-Managed Device to Cisco Secure Firewall Threat Defense with the Migration Tool* guide for more information.
	Fortinet Firewall to Cisco Secure Firewall Threat Defense Migration You can now migrate URL objects from a Fortinet firewall to your threat defense device. Review the **URL Objects** tab in the **Objects** tab in **Optimize, Review and Validate Configuration** page during migration. See Optimize, Review, and Validate the Configuration in the *Migrating Fortinet Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool* guide for more information.
	Palo Alto Networks Firewall to Cisco Secure Firewall Threat Defense Migration You can now migrate URL objects from a Palo Alto Networks firewall to your threat defense device. Ensure you review the **URL Objects** tab in the **Objects** window in **Optimize, Review and Validate Configuration** page during migration. See Optimize, Review, and Validate the Configuration in the *Migrating Palo Alto Networks Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool* guide for more information.
	Check Point Firewall to Cisco Secure Firewall Threat Defense Migration You can now migrate port objects, FQDN objects, and object groups from a Check Point Firewall to your threat defense device. Review the **Objects** tab in **Optimize, Review and Validate Configuration** page during migration. See Optimize, Review, and Validate the Configuration in the *Migrating Check Point Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool* guide 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
CSCwj57359	Fortigate configurations with bulk ACLs and objects cause performance issues with migration.
CSCwk79064	ASA migration fails at parsing stage because of errors in route map interfaces in policy-based routing configurations.

Resolved Issues

This list includes all the caveats that were resolved as part of 7.0 and 7.0.0.1 releases of the Cisco Secure Firewall Migration Tool.

Bug ID	Description
CSCwk38736	PAN migration shows 'NoneType object has no attribute id' error.
CSCwk88888	FDM migration shows parsing error, 'cannot unpack non-interable NoneType object'.
CSCwk82480	Terminal freezes at preparsing stage when migrating Fortinet firewall configurations.
CSCwk94186	PAN migrations fail at parsing stage.
CSCwk98316	ASA migrations fail at parsing stage.
CSCwm27959	ASA migrations fail at parsing stage with error 'list index out of range'.
CSCwm28043	Multicontext ASA migrations show default route as unsupported and does not migrate them .
CSCwm30744	ASA HA migrations fail at configuration push stage.
CSCwm30823	ASA migrations fail after configuration push to FMC.
CSCwm12311	Fortinet migration shows error at parsing stage.
CSCwm10557	PAN migration shows the error 'the source PAN configuration has error'.
CSCwj31384	'Next' option in ASA migration greyed out
CSCwk19689	Fortinet SSL VPN migration issue
CSCwk30675	PFS is enabled even if it is not selected during ASA migration
CSCwk31971	ASA migration is failing if routed mode firewall has bridge virtual tunnel interface
CSCwk33718	EIGRP passive interface configurations are not getting migrated during ASA migrations
CSCwk33741	ACL rules are missing after the configuration parsing in an ASA hub and spoke topology creation migration
CSCwk35097	Discrepancies in IKEv2 authentication method in an ASA hub and spoke topology creation migration

Bug ID	Description
CSCwk35362	Extended ACL configurations show `Object name already exists. Enter new name` error in ASA migrations
CSCwk37249	Security zones migration fails for FDM migrations
CSCwk40661	ASA migration fails at parsing stage for FQDN objects
CSCwk40683	ASA with FPS migration stops at **Select FTD** step
CSCwk52533	**Next** option is grayed out at **Select Features** in ASA migration
CSCwk53966	Error when remote access VPN objects are migrated in ASA migration
CSCwk54982	Configuration pull from ASA fails with **Block** error in ASA migration
CSCwk55095	Extended and standard ACL objects are not getting migrated in ASA migration
CSCwk56461	**Optimize, Review, and Validate** page shows error message for HA pair creation for ASA migration
CSCwk56930	ASA migration to cloud-delivered Firewall Management Center fails
CSCwk67199	ASA migration demo mode does not display HA pair
CSCwk67210	ASA migration demo mode allows selection of nonidentical devices for HA creation
CSCwk68857	Wrong AnyConnect file in ASA remote access VPN migration
CSCwk73519	Remote access VPN configuration is not getting migrated in ASA migration
CSCwk74805	The migration tool gets terminated after configuration parsing stage in Fortinet migration
CSCwk76628	Interface migration fails for a duplicate logical name in ASA migration
CSCwk76748	Unsupported VPN crypto ACLs get migrated to FMC in ASA migration
CSCwk77827	Remote access VPN connection profile is listed as unsupported configuration
CSCwk79245	Interface migration fails when management is in converged mode

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