

Getting Started with the Secure Firewall Migration Tool

- About This Guide, on page 1
- About the Secure Firewall Migration Tool, on page 1
- What's New in the Secure Firewall Migration Tool, on page 4
- Licensing for the Secure Firewall Migration Tool, on page 23
- Platform Requirements for the Secure Firewall Migration Tool, on page 23
- Requirements and Prerequisites for Threat Defense Devices, on page 23
- Configuration Support, on page 24
- Guidelines and Limitations, on page 28
- Supported Platforms for Migration, on page 33
- Supported Target Management Center for Migration, on page 35
- Supported Software Versions for Migration, on page 37
- Related Documentation, on page 38

About This Guide

This guide contains information on how you can download the Secure Firewall Migration Tool and complete the migration. In addition, it provides you troubleshooting tips to help you resolve migration issues that you may encounter.

About the Secure Firewall Migration Tool

The sample migration procedure (Sample Migration: ASA to Threat defense 2100) included in this book helps to facilitate understanding of the migration process.

The Secure Firewall Migration Tool migrates the supported Cisco Secure Firewall ASA configurations to a supported Secure Firewall Threat Defense platform. The Secure Firewall Migration Tool allows you to automatically migrate the supported ASA features and policies to Firewall Threat Defense.

Note You must review the **Pre-Migration Report** for ignored configurations, if any, and manually configure them after migration.

To know more about the commonly used ASA features and their equivalent threat defense features, see Cisco Secure Firewall ASA to Threat Defense Feature Mapping guide.

The Secure Firewall Migration Tool gathers information, parses it, and pushes it to the Secure Firewall Management Center. During the parsing phase, the Secure Firewall Migration Tool generates a **Pre-Migration Report** that identifies the following:

- Cisco Adaptive Security Appliance (ASA) configuration items that are fully migrated, partially migrated, unsupported for migration, and ignored for migration.
- configuration lines with errors that lists the CLIs which the Secure Firewall Migration Tool cannot recognize; this blocks the migration.

If there are parsing errors, you can rectify the issues, reupload a new configuration, connect to the destination device, map the interfaces to Firewall Threat Defense interfaces, map security zones and interface groups, and proceed to review and validate your configuration. You can then migrate the configuration to the destination device.

Console

The console opens when you launch the Secure Firewall Migration Tool. The console provides detailed information about the progress of each step in the Secure Firewall Migration Tool. The contents of the console are also written to the Secure Firewall Migration Tool log file.

The console must stay open while the Secure Firewall Migration Tool is open and running.



Important When you exit the Secure Firewall Migration Tool by closing the browser on which the web interface is running, the console continues to run in the background. To completely exit the Secure Firewall Migration Tool, exit the console by pressing the Command key + C on the keyboard.

Logs

The Secure Firewall Migration Tool creates a log of each migration. The logs include details of what occurs at each step of the migration and can help you determine the cause if a migration fails.

You can find the log files for the Secure Firewall Migration Tool in the following location:
`<migration_tool_folder>\logs`

Resources

The Secure Firewall Migration Tool saves a copy of the **Pre-Migration Report**, **Post-Migration Report**, ASA configs, and logs in the **Resources** folder.

You can find the **Resources** folder in the following location: *<migration_tool_folder>\resources*

Unparsed File

The Secure Firewall Migration Tool logs information about the configuration lines that it ignored in the unparsed file. This Secure Firewall Migration Tool creates this file when it parses the ASA configuration file.

You can find the unparsed file in the following location:

<migration_tool_folder>\resources

Search in the Secure Firewall Migration Tool

You can search for items in the tables that are displayed in the Secure Firewall Migration Tool, such as those on the **Optimize, Review and Validate** window.

To search for an item in any column or row of the table, click the **Search** ( ) above the table and enter the search term in the field. The Secure Firewall Migration Tool filters the table rows and displays only those that contain the search term.

To search for an item in a single column, enter the search term in the **Search** field that is provided in the column heading. The Secure Firewall Migration Tool filters the table rows and displays only those that match the search term.

Ports

The Secure Firewall Migration Tool supports telemetry when run on one of these 12 ports: ports 8321-8331 and port 8888. By default, Secure Firewall Migration Tool uses port 8888. To change the port, update port information in the *app_config* file. After updating, ensure to relaunch the Secure Firewall Migration Tool for the port change to take effect. You can find the *app_config* file in the following location: *<migration_tool_folder>\app_config.txt*.

Note We recommend that you use ports 8321-8331 and port 8888, as telemetry is only supported on these ports. If you enable Cisco Success Network, you cannot use any other port for the Secure Firewall Migration Tool.

Notifications Center

All the notifications, including success messages, error messages, and warnings that pop up during a migration are captured in the notifications center and are categorized as **Successes**, **Warnings**, and **Errors**. You can click the 

icon on the top right corner any time during the migration and see the various notifications that popped up, along with the time they popped up in the tool.

Cisco Success Network

Cisco Success Network is a user-enabled cloud service. When you enable Cisco Success Network, a secure connection is established between the Secure Firewall Migration Tool and the Cisco cloud to stream usage information and statistics. Streaming telemetry provides a mechanism to select data of interest from the Secure Firewall Migration Tool and to transmit it in a structured format to remote management stations for the following benefits:

- To inform you of available unused features that can improve the effectiveness of the product in your network.
- To inform you of additional technical support services and monitoring that is available for your product.
- To help Cisco improve our products.

The Secure Firewall Migration Tool establishes and maintains the secure connection and allows you to enroll in the Cisco Success Network. You can turn off this connection at any time by disabling the Cisco Success Network, which disconnects the device from the Cisco Success Network cloud.

What's New in the Secure Firewall Migration Tool

Version	Supported Features
10.0.2	This patch release contains bug fixes.
10.0.1	You can now migrate DHCP and DNS configurations using the Secure Firewall Migration Tool. Supported migration: Check Point Firewall to Firewall Threat Defense
	This release introduces comprehensive migration support for Secure Firewall 6100 series devices.
	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
	Added support for migrating firewall configuration from Check Point Small and Medium Business (SMB) devices to Cisco Secure Firewall Threat Defense.
	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
	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.

Version	Supported Features
10.0	This release introduces comprehensive migration support for CSF200 series devices. Supported migration: All
	Migration support for Firewall Management Center and Firewall Threat Defense 10.0 designed to facilitate smooth transitions to this release. Supported migration: All
	This release introduces significant enhancements to telemetry capabilities, improving data collection for analysis and troubleshooting. Supported migration: All
	This release delivers significant enhancements to parsing performance, making the system more responsive and efficient. Supported migration: Check Point Firewall to Firewall Threat Defense, Palo Alto Networks Firewall to Firewall Threat Defense and ASA Firewall to Firewall Threat Defense.
	The Dual Network Address Translation (NAT) feature is enhanced to improve the user experience. See: Check Point Configuration Support Supported migration: Check Point Firewall to Firewall Threat Defense
7.7.10.4	This patch release contains bug fixes.

Version	Supported Features
7.7.10.3	Secure Firewall Migration Tool can now identify conflicts caused by duplicate object names or values when deploying the configuration to Firewall Management Center. The tool then prompts the user to take appropriate action to resolve these conflicts. See: Push the Migrated Configuration to Firewall Management Center Supported migrations: All
	The ACL optimization analysis time has been reduced to enhance performance. A banner is displayed on **Optimize, Review and Validate Configuration** window, when you click **Optimize ACL** and then **Proceed,** that shows the approximate time taken for ACL optimization analysis. See: Optimize, Review and Validate the Configuration Supported migrations: All
	You can now view the list of disabled ACLs in the **Optimize, Review and Validate Configuration** > **ACL Optimization** window. This enhancement ensures a more efficient migration process. See: Optimize, Review and Validate the Configuration Supported migrations: All
	To streamline the optimization process during migration, the Secure firewall Migration Tool performs a check to ensure all the attributes are optimized. When you click **Validate** on **Optimize, Review and Validate Configuration** window any attribute that is missed is displayed in the **Optimize Your Configuration** dialog box. See: Optimize, Review and Validate the Configuration Supported migrations: All
7.7.10.2	This patch release contains bug fixes.

Version	Supported Features
7.7.10.1	This release includes the following new features: • The Secure Firewall migration tool now provides an option to select transparent-mode and routed-mode firewall contexts separately that allows you to manage and migrate the contexts independently providing greater flexibility and control during the migration process. See: Select the ASA Security Context Supported migrations: Secure Firewall ASA • The Secure Firewall migration tool now provides an option to edit the source and destination zones of NAT rule on the Optimize, Review and Validate Configuration window. See: Optimize, Review and Validate the Configuration Supported migrations: Secure Firewall ASA • The Secure Firewall migration tool now supports migration of Access Control Entry (ACE) with negate parameters. See: Check Point Configuration Support Supported migrations: Check Point Firewall • The Secure Firewall migration tool now supports interface mapping to inline security zones, enabling granular policy enforcement and traffic control. See: Map PAN Interfaces to Security Zones Interface Groups Supported migrations: Palo Alto Networks Firewall • You can now migrate VLAN Tag objects and other supported object types to your threat defense device by using the Secure Firewall migration tool. See: Optimize, Review and Validate the Configuration Supported migrations: Palo Alto Networks Firewall

Version	Supported Features
7.7.10	This release includes the following new features: • You can now migrate configurations from a Microsoft Azure Native firewall to Firewall Threat Defense using the Secure Firewall migration tool. See Migrating Microsoft Azure Native Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool for more information and migration steps. • You can now migrate configurations from a Check Point firewall to Multicloud Defense using the Secure Firewall migration tool. See Migrating Check Point Firewall to Cisco Multicloud Defense with the Migration Tool for more information and migration steps. • You can now migrate configurations from a Fortinet firewall to Multicloud Defense using the Secure Firewall migration tool. See Migrating Fortinet Firewall to Cisco Multicloud Defense with the Migration Tool with the Migration Tool for more information and migration steps. • The Secure Firewall migration tool now detects existing Security Group Tag object configurations. This detection simplifies security policy management by associating specific tags with users, devices, or systems, and enables dynamic and scalable access control. See: Optimize, Review, and Validate the Configuration Supported migrations: Secure Firewall ASA • You can now edit access rules by adding, deleting or modifying objects or object groups on the **Optimize, Review and Validate Configurations** page. See: Optimize, Review, and Validate the Configuration Supported migrations: All • The pre-migration and post-migration report is enhanced to improve the user experience. You can now download a CSV file for each section for detailed analysis. A comparison chart is introduced in post-migration report that compares the number of configurations in the pre-migration report and the post-migration report for each category. See: Optimize, Review, and Validate the Configuration Supported migrations: All
7.7	This release includes the following new features: • You can now migrate configurations from a Secure Firewall ASA to Multicloud Defense using the Secure Firewall migration tool. See Migrating Cisco Secure Firewall ASA to Cisco Multicloud Defense with the Migration Tool for more information and migration steps. • You can now migration configurations from a Palo Alto Networks firewall to Multicloud Defense using the Secure Firewall migration tool. See Migrating Palo Alto Networks Firewall to Cisco Multicloud Defense with the Migration Tool for more information and migration steps.

Version	Supported Features
7.0.1	

Version	Supported Features
	This release includes the following new features and enhancements: • 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 • 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 • You can now choose to ignore migration-hindering, incorrect configurations and still continue the final push of a migration. Previously, 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 • The Secure Firewall migration tool now detects existing site-to-site VPN configurations in the target threat defense device and 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 • 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 • When migrating thrid-party firewalls, you can now select threat defense devices as target, which are part of a high availability pair. Previously, you could only choose standalone threat defense devices as target devices. Supported migrations: Palo Alto Networks, Check Point, and Fortinet firewall migrations • The Secure Firewall migration tool now provides a more enhanced, intuitive demo mode, with guided migration instructions at every step. In addition, you

Version	Supported Features
	can also see versions of target threat defense devices to choose and test based on your requirements. Supported migrations: All
7.0	This release includes the following new features and enhancements: **Cisco Secure Firewall ASA to Cisco Secure Firewall 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. Choose **Proceed with HA Pair Configuration** on the **Select Target** page and choose an active and a standby device. When selecting the active threat defense device, ensure you have an identical device on the management center for the HA pair configuration to be successful. 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. Click **Add Hub & Spoke Topology** under **Site-to-Site VPN Tunnels** on the **Optimize, Review and Validate Configuration** page. 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.

Version	Supported Features
6.0.1	This release includes the following new features and enhancements: **Cisco Secure Firewall ASA to Cisco Secure Firewall 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. The migration tool identifies objects and groups that have the same value and prompts you to choose which to retain. See Optimize, Review, and Validate the Configuration 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 for more information. **Fortinet Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate URL objects in addition to other object types from a Fortinet firewall to your threat defense device. 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 for more information. **Palo Alto Networks Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate URL objects in addition to other object types 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 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** window in **Optimize, Review and Validate Configuration** page during migration. See Optimize, Review, and Validate the Configuration for more information.

Version	Supported Features
6.0	

Version	Supported Features
	This release includes the following new features and enhancements: **Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense Migration** • You can now migrate WebVPN configurations on your Secure Firewall ASA to Zero Trust Access Policy configurations on a threat defense device. Ensure that you check the **WebVPN** checkbox in **Select Features** page and review the new **WebVPN** tab in the **Optimize, Review and Validate Configuration** page. The threat defense device and the target management center must be running on Version 7.4 or later and must be operating Snort3 as the detection engine. • You can now migrate Simple Network Management Protocol (SNMP) and Dynamic Host Configuration Protocol (DHCP) configurations to a threat defense device. Make sure that you check the **SNMP** and **DHCP** checkboxes in the **Select Features** page. If you have configured DHCP on your Secure Firewall ASA, note that the DHCP server, or relay agent and DDNS configurations can also be selected to be migrated. • You can now migrate the equal-cost multipath (ECMP) routing configurations when performing a multi-context ASA device to a single-instance threat defense merged context migration. The **Routes** tile in the parsed summary now includes ECMP zones also, and you can validate the same under the **Routes** tab in the **Optimize, Review and Validate Configuration** page. • You can now migrate dynamic tunnels from the dynamic virtual tunnel interface (DVTI) configurations from your Secure Firewall ASA to a threat defense device. You can map them in the **Map ASA Interfaces to Security Zones, Interface Groups, and VRFs** page. Ensure that your ASA Version is 9.19 (x) and later for this feature to be applicable. **FDM-managed Device to Cisco Secure Firewall Threat Defense Migration** • You can now migrate the Layer 7 security policies including SNMP and HTTP, and malware and file policy configurations from your FDM-managed device to a threat defense device. Ensure that the target management center Version is 7.4 or later and that **Platform Settings** and **File and Malware Policy** checkboxes in **Select Features** page are checked. **Check Point Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate the site-to-site VPN (policy-based) configurations on your Check Point firewall to a threat defense device. Note that this feature applies to Check Point R80 or later versions, and management center and threat defense Version 6.7 or later. Ensure that the **Site-to-Site VPN Tunnels** checkbox is checked in the **Select Features** page. Note that, because this is a device-specific configuration, the migration tool does not display these configurations if you choose to **Proceed without FTD**. **Fortinet Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now optimize your application access control lists (ACLs) when migrating configurations from a Fortinet firewall to your threat defense device.

Version	Supported Features
	Use the **Optimize ACL** button in the **Optimize, Review and Validate Configuration** page to see the list of redundant and shadow ACLs and also download the optimization report to see detailed ACL information.
5.0.1	This release includes the following new features and enhancements: • The Secure Firewall migration tool now supports migration of multiple transparent firewall-mode security contexts from Secure Firewall ASA devices to threat defense devices. You can merge two or more transparent firewall-mode contexts that are in your Secure Firewall ASA device to a transparent-mode instance and migrate them. In a VPN-configured ASA deployment where one or more of your contexts have VPN configurations, you can choose only one context whose VPN configuration you want to migrate to the target threat defense device. From the contexts that you have not selected, only the VPN configuration is ignored and all other configurations are migrated. See Select the ASA Security Context for more information. • You can now migrate site-to-site and remote access VPN configurations from your Fortinet and Palo Alto Networks firewalls to threat defense using the Secure Firewall migration tool. From the **Select Features** pane, select the VPN features that you want to migrate. See the Specify Destination Parameters for the Secure Firewall Migration Tool section in Migrating Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Migration Tool and Migrating Fortinet Firewall to Secure Firewall Threat Defense with the Migration Tool guides. • You can now select one or more routed or transparent firewall-mode security contexts from your Secure Firewall ASA devices and perform a single-context or multi-context migration using the Secure Firewall migration tool.

Version	Supported Features
5.0	• Secure Firewall migration tool now supports migration of multiple security contexts from Secure Firewall ASA to threat defense devices. You can choose to migrate configurations from one of your contexts or merge the configurations from all your routed firewall mode contexts and migrate them. Support for merging configurations from multiple transparent firewall mode contexts will be available soon. See Select the ASA Primary Security Context for more information. • The migration tool now leverages the virtual routing and forwarding (VRF) funtionality to replicate the segregated traffic flow observed in a multi-context ASA environment, which will be part of the new merged configuration. You can check the number of contexts the migration tool has detected in a new **Contexts** tile and the same after parsing, in a new **VRF** tile in the **Parsed Summary** page. In addition, the migration tool displays the interfaces to which these VRFs are mapped, in the **Map Interfaces to Security Zones and Interface Groups** page. • You can now try the whole migration workflow using the new demo mode in Secure Firewall migration tool and visualize how your actual migration looks like. See Using the Demo Mode in Firewall Migration Tool for more information. • With new enhancements and bug fixes in place, Secure Firewall migration tool now provides an improved, faster migration experience for migrating Palo Alto Networks firewall to threat defense.
4.0.3	The Secure Firewall migration tool 4.0.3 includes bug fixes and the following new enhancements: • The migration tool now offers an enhanced **Application Mapping** screen for migrating PAN configurations to threat defense. See Map Configurations with Applications in *Migrating Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Migration Tool* guide for more information.
4.0.2	The Secure Firewall migration tool 4.0.2 includes the following new features and enhancements: • Secure Firewall Migration Tool now supports migration of site-to-site VPN filter configurations and the extended access list objects pertaining to those configurations when the destination management center and threat defense versions are 7.1 and later. Earlier, site-to-site VPN filter configurations were not migrated and had to be manually configured after migration. • The migration tool now has an always-on telemetry; however, you can now choose to send limited or extensive telemetry data. Limited telemetry data inludes few data points, whereas extensive telemetry data sends a more detailed list of telemetry data. You can change this setting from **Settings** > **Send Telemetry Data to Cisco?**.

Version	Supported Features
4.0.1	The Secure Firewall migration tool 4.0.1 includes the following new features and enhancements: The Secure Firewall migration tool now analyzes all objects and object groups based on both their name and configuration, and reuses objects that have the same name and configuration. Only network objects and network object groups were analyzed based on their name and configuration before. Note that the XML profiles in remote access VPNs are still validated only using their name.
4.0	Secure Firewall migration tool 4.0 supports: • Migration of Policy Based Routing (PBR) from ASA if the destination management center and threat defense version are 7.3 and later. **Note** For PBR migration, the existing flex configuration must be removed from the management center before proceeding with the migration. • Migration of Remote Access VPN custom attributes and VPN load balancing from ASA if the destination management center is 7.3 or later. You can perform Remote Access VPN migration with or without a firewall. However, if you chose to perform the migration with a firewall, then the threat defense version must be 7.0 and later. **Note** To migrate Remote Access VPN with a targeted firewall, you must select the target firewall and add any one of the following licenses to the targeted firewall: • AnyConnect Plus • AnyConnect Apex • AnyConnect VPN Only • Migration of Equal Cost Multi-Path (ECMP) routes from ASA if the destination management center is 7.1 and later and the threat defense version is 6.5 and later.
3.0.2	The Secure Firewall Migration Tool 3.0.2 includes bug fixes for remote access VPN configuration migration from ASA to Firewall Management Center versions 7.2 or higher.

Version	Supported Features
3.0.1	Secure Firewall Migration Tool 3.0.1 supports: • Migration of Enhanced Interior Gateway Routing Protocol (EIGRP) from ASA if the destination management center is version 7.2 and later and the threat defense version is 7.0 and later. **Note** You cannot migrate EIGRP from ASA and ASA with FirePOWER Services without a threat defense device. • The Cisco Secure Firewall 3100 series is supported as a source or destination device for migrations from ASA.

3.0	The Secure Firewall migration tool 3.0 supports:
	• Remote Access VPN migration from ASA if the destination management center is 7.2 or later. You can perform RA VPN migration with or without Secure Firewall Threat Defense. If you select the migration with threat defense, then the threat defense version must be 7.0 or later.
	• Site-to-Site VPN pre-shared key automation from ASA.
	• The following must be performed as part of the pre-migration activity:
	  • The ASA trustpoints must be manually migrated to the management center as PKI objects.
	  • AnyConnect packages, Hostscan Files (Dap.xml, Data.xml, Hostscan Package), External Browser package, and AnyConnect profiles must be retrieved from source ASA.
	  • AnyConnect packages must be uploaded to the management center.
	  • AnyConnect profiles must be directly uploaded to the management center or from the Secure Firewall migration tool.
	  • The **ssh scopy enable** command must be enabled on the ASA to allow retrieval of profiles from the Live Connect ASA.
	• Migration to Cloud-delivered Firewall Management Center from ASA if the destination management center is 7.2 or later.

Version	Supported Features
2.5.2	The Secure Firewall migration tool 2.5.2 provides support to identify and segregate ACLs that can be optimized (disabled or deleted) from the firewall rule base without impacting the network functionality from Firewalls. The 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** Optimization is available for the ASA only for ACP rule action. The Secure Firewall migration tool 2.5.2 supports Border Gateway Protocol (BGP) and Dynamic-Route Objects migration if the destination Firewall Management Center is 7.1 or later.
2.5.1	The Secure Firewall migration tool 2.5.1 supports Border Gateway Protocol (BGP) and Dynamic-Route Objects migration if the destination Firewall Management Center is 7.1 or later.
2.5	The Secure Firewall migration tool 2.5 provides support to identify and segregate ACLs that can be optimized (disabled or deleted) from the firewall rule base without impacting the network functionality. The 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** Optimization is available for the Source ASA only for ACP rule action. Discontinuous network mask (Wildcard mask) objects are supported if the destination Firewall Management Center version is 7.1 or later.

Version	Supported Features
2.4	The following ASA VPN configuration migration to Firewall Threat Defense: • Crypto map (static/dynamic) based VPN from ASA • Route-based (VTI) based ASA VPN • Certificate-based VPN migration from ASA **Note** • ASA trustpoint or certificates is migrated manually and part of pre-migration activity. • ASA trustpoint must be migrated as Firewall Management Center PKI objects. PKI objects are used in Secure Firewall migration tool while creating certificate-based VPN topologies.
2.3.5	The Secure Firewall migration tool supports the migration of the following Virtual Tunnel Interface (VTI) configurations to Firewall Threat Defense if the target Firewall Management Center and Firewall Threat Defense is 6.7 or later: • VTI interface and the related static routes • Route-based (VTI) pre-shared key authentication type VPN configuration to Firewall Management Center and Firewall Threat Defense. • Create routed security zone, add VTI interfaces, and then define access control rules for the decrypted traffic control over VTI tunnel.
2.3.4	The Secure Firewall migration tool allows you to migrate the following ASA VPN configuration elements to Firewall Threat Defense: • Supports migration of policy-based (crypto map) pre-shared key authentication type VPN configuration to the Firewall Management Center. • VPN Objects—Creates VPN Objects (IKEv1/IKEv2 Policy, IKEv1/IKEv2 IPsec-Proposal), maps the VPN objects with the specific Site-to-Site VPN topologies, and migrates the objects to the Firewall Management Center. Verify the VPN objects against the rules in the **Review and Validate Configuration** page. • Site-to-Site VPN Topology—The crypto map related configurations in source ASA config are migrated with respective VPN objects. Policy-based (crypto map) VPN Topology are supported on Firewall Management Center version 6.6 and above. **Note** In this release, Secure Firewall migration tool supports migration of static crypto map only. All supported ASA crypto map VPN will be migrated as Firewall Management Center point-to-point topology.

Version	Supported Features

1.3	• The Secure Firewall migration tool allows you to connect to an ASA using the admin credentials and **Enable Password** as configured on the ASA.
	If ASA is not configured with **Enable Password**, you can leave the field blank on the Secure Firewall migration tool.
	• You can now configure the batch size limit for Bulk Push in the `app_config` file as follows:
	  • For Objects, the batch size cannot exceed 500. The Secure Firewall migration tool resets the value to 50 and proceeds with the bulk push.
	  • For ACLs, Routes, and NAT, the batch size cannot exceed 1000 each. The Secure Firewall migration tool resets the value to 1000 and proceeds with the bulk push.
	• The Secure Firewall migration tool allows you to parse the CSM or ASDM managed configurations.
	When you opt to clear the inline grouping or ASDM managed configurations, the predefined objects are replaced with the actual object or member name.
	If you do not clear the CSM or ASDM managed configurations, the predefined object names will be retained for migration.
	• Provides customer support to download log files, dB, and configuration files during a migration failure. You can also raise a support case with the technical team through an email.
	• Support for migration of IPv6 configurations in Objects, Interfaces, ACL, NAT, and Routes.
	• The Secure Firewall migration tool allows you to map an ASA interface name to a physical interface on the Firewall Threat Defense object types—Physical interfaces, port channel, and subinterfaces. For example, you can map a port channel in ASA to a physical interface in Firewall Management Center.
	• The Secure Firewall migration tool provides support to skip migration of the selected NAT rules and Route interfaces. The previous versions of the Secure Firewall migration tool provided this option for Access Control rules only.
	• You can download the parsed Access Control, NAT, Network Objects, Port Objects, Interface, and Routes configuration items from the **Optimize, Review and Validate Configuration** screen in an excel or CSV format.
	Note
	You cannot import a CSV file.

Version	Supported Features
1.2	• Supports migration to Firewall Management Center 6.3 • Supports migration of IPv4 FQDN Objects and Groups • Supports the **show tech-support** command in the manual upload method for Multiple-Context ASA • Supports migration to the container type Firewall Threat Defense (MI) registered on Firewall Management Center. • Rule Action Mapping Support (Allow, Trust, Monitor, Block, or Block with Reset) on the migrated access control rules in the Access Control table. • Version check for Secure Firewall migration tool to ensure that you are using the most recent version of the Secure Firewall migration tool.
1.1	• Bulk push for objects, NAT, static routes significantly reduce the time that is taken to push the configuration to a Firewall Management Center. • Extracting configuration from a production ASA • Selective feature migration (shared policy and device-specific policy) • Rule optimization • Map migrating ASA Access Control Rules to a list of configured Intrusion Prevention System and File Policies on the Firewall Management Center. • Migrate only those objects that are referenced in policies. This optimizes migration times and cleans out unused objects during configuration. • Migration support for **running-config** or **sh run** from one of Data Contexts of ASA running in multiple-context mode. • Support on macOS version 10.13 and higher • Support to modify logging actions (enable or disable, logging at beginning or end) for migrated Access Control Rules. • Migration to Firewall Threat Defense devices configured within domains on the Firewall Management Center. • Bulk edits capability for object names. • Telemetry support with Cisco Success Network

Version	Supported Features
1.0	• Validation throughout the migration, including parse and push operations. • Object re-use capability • Object conflict resolution • Interface mapping • Autocreation or reuse of interface objects (ASA name if to the security zone and interface group mapping) • Support for a bulk migration of ACLs

Licensing for the Secure Firewall Migration Tool

The Secure Firewall migration tool application is free and does not require license. However, the Firewall Management Center must have the required licenses for the related Firewall Threat Defense features to successfully register Firewall Threat Defense devices and deploy policies to it.

Platform Requirements for the Secure Firewall Migration Tool

The Secure Firewall migration tool has the following infrastructure and platform requirements:

- Runs on a Microsoft Windows 10 64-bit operating system or on a macOS version 10.13 or higher
- Has Google Chrome as the system default browser
- (Windows) Has Sleep settings configured in Power & Sleep to Never put the PC to Sleep, so the system does not go to sleep during a large migration push
- (macOS) Has Energy Saver settings configured so that the computer and the hard disk do not go to sleep during a large migration push

Requirements and Prerequisites for Threat Defense Devices

When you migrate to the management center, it is not mandatory to have a target threat defense device added to it. You can migrate policies to a management center for future deployment to a threat defense device.

If threat defense device is added to the management center, to migrate your ASA configuration to threat defense, consider the following requirements and prerequisites:

- The target threat defense device must be registered with the management center.
- The target threat defense device can be in a high availability configuration.
- The threat defense device can be a standalone device or a container instance. It must **not** be part of a cluster.
    - The target native threat defense device must have at least an equal number of used physical data and port channel interfaces (excluding ‘management-only’ and subinterfaces) as that of the ; if not

you must add the required type of interface on the target threat defense device. Subinterfaces are created by the Secure Firewall migration tool that are based on physical or port channel mapping.

- If the target threat defense device is a container instance, at minimum it must have an equal number of used physical interfaces, physical subinterfaces, port channel interfaces, and port channel subinterfaces (excluding 'management-only') as that of the ASA; if not you must add the required type of interface on the target threat defense device.

Note

- Subinterfaces are not created by the Secure Firewall migration tool, only interface mapping is allowed.
- Mapping across different interface types is allowed, for example: physical interface can be mapped to a port channel interface.

Configuration Support

Supported Configurations

The Secure Firewall migration tool can fully migrate the following configurations:

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

Note Though 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 Since nesting is not supported on the Firewall 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
- DHCP configurations including server, relay, and DDNS

- SNMP
- Physical interfaces
- Secondary VLANs on interfaces are not migrated to Firewall Threat Defense.
- Subinterfaces (subinterface ID is always set to the same number as the VLAN ID on migration)
- Port channels
- Virtual tunnel interface (VTI)
- Dynamic VTI and IPv6
- 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 the objects to Firewall Management Center.

  IP SLA monitor defines a connectivity policy to a monitored IP address and tracks the availability of a route to the IP address. The static routes are periodically checked for availability by sending ICMP echo requests and waiting for the response. If the echo requests are timed-out, the static routes are removed from the routing table and replaced with a backup route. SLA monitoring jobs start immediately after deployment and continue to run unless, you remove the SLA monitor from the device configuration, that is, they do not age out. The IP SLA monitor objects are used in the Route Tracking field of an IPv4 static route policy. IPv6 routes do not have the option to use SLA monitor through route tracking.



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

- Object Group Search

  Enabling object group search reduces memory requirements for access control policies that include network objects. We recommend you to enable object group search that enhances optimal memory utilization by access policy on Firewall Threat Defense.



Note

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

- Security Group Tag-based objects

  Security Group Tag (SGT) objects enables scalable and dynamic network security through the use of policy-based access control. When the Secure Firewall migration tool detects SGT-based objects, verify the objects against the rules in the **Review and Validate Configuration** page.

  To migrate the SGT objects configuration, ensure that the management center and threat defense version are 7.0 or later.

- Time-based objects

When the Secure Firewall migration tool detects time-based objects that are referenced with access-rules, the Secure Firewall migration tool migrates the time-based objects and maps them with respective access-rules. Verify the objects against the rules in the **Review and Validate Configuration** page.

Time-based objects are access-list types that allow network access on the basis of time period. It is useful when you must place restrictions on outbound or inbound traffic on the basis of a particular time of the day or particular days of a week.



Note

- You must manually migrate timezone configuration from source to target FTD.
- Time-based object is not supported for non-Firewall Threat Defense flow and will be disabled.
- Time-based objects are supported on Firewall 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 , the Secure Firewall migration tool migrates the crypto map to the Firewall Management Center VPN as point-to-point topology.
  - Crypto map (static/dynamic) based VPN from ASA
  - Route-based (VTI) ASA VPN
  - Certificate-based VPN migration from ASA
  - ASA trustpoint or certificates migration to the Firewall 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
- 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 trustpoints manually to the Firewall 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.
  - Upload all AnyConnect packages to the Firewall Management Center.
  - Upload AnyConnect profiles directly to the Firewall 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.

- WebVPN
  - Group security policies SSL clientless VPN tunnel protocols
  - Tunnel groups related to group policies that use Security Assertion Markup Language (SAML) as the authentication method
  - Tunnel groups containing HTTPS-based application URLs



Note If the aforementioned criteria are met, the SAML configurations and application URLs are migrated.

Partially Supported Configurations

The Secure Firewall migration tool partially supports the following configurations for migration. Some of these configurations include rules with advanced options that are migrated without those options. If the Firewall Management Center supports those advanced options, you can configure them manually after the migration is complete.

- Access control policy rules that are configured with advanced logging settings, such as severity and time-interval.
- Static routes that are configured with the track option.
- Certificate-based VPN migration.
- Dynamic-Route Objects, EIGRP, and BGP
  - Route-Map

Unsupported Configurations

The Secure Firewall migration tool does not support the following configurations for migration. If these configurations are supported in the Firewall Management Center, you can configure them manually after the migration is complete.

- User-based access control policy rules

- NAT rules that are configured with the block allocation option
- Tunneling protocol-based access control policy rules



Note Support with a prefilter on Secure Firewall migration tool and Firewall Management Center 6.5.

- NAT rules that are configured with SCTP
- NAT rules that are configured with host ‘0.0.0.0’
- Default route obtained through DHCP or PPPoE with SLA tracking
- SLA monitor schedule
- Transport mode IPsec transform-set
- ASA trustpoint migration into Firewall Management Center
- Transparent firewall mode for BGP
- In an ASA WebVPN to Zero Trust Application (ZTA) policy migration, the following are not supported:
  - Importing WebVPN bookmarks
  - Local, RADIUS, and LDAP authentication methods
- Access list remarks

Guidelines and Limitations

During conversion, the Secure Firewall migration tool creates a one-to-one mapping for all supported objects and rules, whether they are used in a rule or policy. The Secure Firewall migration tool provides an optimization feature that allows you to exclude migration of unused objects (objects that are not referenced in any ACLs and NATs).

The Secure Firewall migration tool deals with unsupported objects and rules as follows:

- Unsupported objects and NAT rules are not migrated.
- Unsupported ACL rules are migrated as disabled rules into the Firewall Management Center.
- Outbound ACLs are **unsupported** and will not be migrated to Firewall Management Center. If the source firewall has outbound ACLs, it will be reported in the **ignored** section of the **Pre-Migration Report**.
- All supported crypto map VPN will be migrated as Firewall Management Center point-to-point topology.
- Unsupported or incomplete static crypto map VPN topologies are not migrated.
- In an ASA multicontext to a single instance threat defense migration, the equal-cost multipath (ECMP) routing configurations are migrated to the corresponding virtual routing and forwarding (VRF) configurations:
  - Interfaces in two different security contexts with the same name are renamed by adding an underscore and the context name.

- Security zones in two different security contexts with the same name are renamed by adding an underscore and the context name.
- If ECMP routing configurations are present with VPN configurations, they are migrated to the global router (global VRF).

Configuration Limitations

Migration of your source configuration has the following limitations:

- The Secure Firewall migration tool supports migrating individual security contexts from the as separate Firewall Threat Defense devices.
- The system configuration is not migrated.
- The Secure Firewall migration tool does not support migration of a single ACL policy that is applied to **over** 50 interfaces. Manually migrate ACL policies that are applied to 50 or more interfaces.
- You cannot migrate some configurations, for example, dynamic routing to Firewall Threat Defense. Migrate these configurations manually.
- You cannot migrate devices in routed mode with a bridge virtual interface (BVI), redundant interface, or tunneled interface. However, you can migrate devices in transparent mode with BVI.
- Nested service object-groups or port groups are not supported on the Firewall Management Center. As part of conversion, the Secure Firewall migration tool expands the content of the referenced nested object-group or port group.
- The Secure Firewall migration tool splits the extended service object or groups with source and destination ports that are in one line into different objects across multiple lines. References to such access control rules are converted into Firewall Management Center rules with the exact same meaning.
- If the source configuration has access control rules that do not refer to specific tunneling protocols (like GRE, IP-in-IP and IPv6-in-IP), but these rules match unencrypted tunnel traffic on the , then, on migration to the Firewall Threat Defense, the corresponding rules will not behave in the same way they do on the . We recommend that you create specific tunnel rules for these in the Prefilter policy, on the Firewall Threat Defense.
- Supported crypto map will be migrated as point-to-point topology.
- If an AS-Path object with the same name in Firewall Management Center appears, then the migration stops with the following error message:

  "Conflicting AS-Path object name detected in Firewall Management Center, please resolve conflict in Firewall Management Center to proceed further"
- Redistribution from OSPF and Routing Information Protocol (RIP) into EIGRP is not supported.
- For PBR, ASA configuration has route-maps whereas management center does not use route-maps. The Secure Firewall migration tool migrates the configuration inside a route-map applied to an interface.
- For route-maps with multiple sequence numbers, only the first sequence number will be migrated. All other sequence numbers will be ignored and shown in the pre-migration report.

Limitations for RA VPN Migration

Remote Access VPN migration is supported with the following limitations:

- SSL settings migration is not supported due to API limitations.
- LDAP server is migrated with encryption type as "none".
- DfltGrpPolicy is not migrated as the policy is applicable for the entire Firewall Management Center. You can make the necessary changes directly on the Firewall Management Center.
- For a radius server, if dynamic authorization is enabled, the AAA server connectivity should be through an interface and not dynamic routing. If ASA configuration is found with AAA server with dynamic authorization enabled without interface, the Secure Firewall migration tool ignores dynamic authorization. You must enable dynamic-authorization manually after selecting an interface on the management center.
- ASA configuration can have an interface while calling address pool under tunnel-group. But the same is not supported on the management center. If there an interface is detected in the ASA configuration it is ignored by the Secure Firewall migration tool and the address pool is migrated without the interface.
- ASA configuration can have keyword **link-selection/subnet-selection** for dhcp-server under tunnel group. But the same is not supported on the management center. If a dhcp server is detected in the ASA configuration with these keywords, it is ignored by the Secure Firewall migration tool and the dhcp-server is pushed without the keywords.
- ASA configuration can have an interface while calling authentication server group, secondary authentication server group, authorization server group under tunnel group. But the same is not supported on the management center. If an interface is detected in the ASA configuration it is ignored by the Secure Firewall migration tool and the commands are pushed without the interface.
- ASA configuration does not map Redirect ACL to a radius server. Thus, there is no way to retrieve it from the Secure Firewall migration tool. If redirect ACL is used in the ASA, it is left empty, and you must add and map it manually on the management center.
- ASA supports value from 0-720 for vpn-addr-assign local reuse delay. But the management center supports value from 0-480. If a value higher than 480 is found in the ASA configuration, it is set to maximum supported value 480 on the management center.
- Configuring IPv4 pool and DHCP useSecondaryUsernameforSession settings to the connection profile is not supported due to API issues.
- Bypass access control sysopt permit-vpn option is not enabled under RA VPN policy. However, if required, you can enable it from the management center.
- AnyConnect client module and profile values can be updated under group policy only when the profiles are uploaded from Secure Firewall migration tool to the management center.
- You need to map the certificates directly on the management center.
- IKEv2 parameters are not migrated by default. You must add them through the management center.

ASA Migration Guidelines

The migration of the ACL log option follows the best practices for Firewall Threat Defense. The log option for a rule is enabled or disabled based on the source ASA configuration. For rules with an action of **deny**, the Secure Firewall migration tool configures logging at the beginning of the connection. If the action is **permit**, the Secure Firewall migration tool configures logging at the end of the connection.

Object Migration Guidelines

and Firewall Threat Defense have different configuration guidelines for objects. For example, one or more objects can have the same name in with one object name in lowercase and the other object name in uppercase, but each object must have a unique name, regardless of case, in Firewall Threat Defense. To accommodate such differences, the Secure Firewall migration tool analyzes all objects and handles their migration in one of the following ways:

- Each object has a unique name and configuration—The Secure Firewall migration tool migrates the objects successfully without changes.
- The name of an object includes one or more special characters that are not supported by the Firewall Management Center—The Secure Firewall migration tool renames the special characters in the object name with a "_" character to meet the Management Center object naming criteria.
- An object has the same name and configuration as an existing object in the Firewall Management Center—The Secure Firewall migration tool reuses the Secure Firewall Management Center object for the Secure Firewall Threat Defense configuration and does not migrate the object.
- An object has the same name but a different configuration than an existing object in Secure Firewall Management Center—The Secure Firewall migration tool reports object conflict and allows you to resolve the conflict by adding a unique suffix to the name of the object for migration purposes.
- Multiple objects have the same name but in different cases—The Secure Firewall migration tool renames such objects to meet the Secure Firewall Threat Defense object naming criteria.



Important The Secure Firewall migration tool analyzes both name and configuration of all objects and object groups. However, XML profiles in remote-access VPN configurations are analyzed only using the name.



Note The Secure Firewall migration tool supports discontiguous network mask (Wildcard mask) objects migration if the destination Firewall Management Center is 7.1 or later.

```
ASA example:
object network wildcard2
subnet 2.0.0.2 255.0.0.255
```

Guidelines and Limitations for ASA WebVPN to ZTA Migration

Before attempting an ASA WebVPN to ZTA migration, make sure you read the following points thoroughly:

- The target management center and threat defense device must be running Version 7.4 or later.
- The target threat defense device must be using Snort3 as the detection engine.
- The ASA trustpoint certificates (IdP and pre-authentication) must be manually uploaded to the target management center before migration.
- The application SSL certificates, along with their private keys, must be uploaded to the target management center before migration.
- Local, RADIUS, and LDAP authentication methods are not supported.

- You can assign only one ZTA policy to a threat defense device.

Guidelines and Limitations for Firewall Threat Defense Devices

As you plan to migrate your ASA configuration to Firewall Threat Defense, consider the following guidelines and limitations:

- If there are any existing device-specific configurations on the Firewall Threat Defense such as routes, interfaces, and so on, during the push migration, the Secure Firewall migration tool cleans the device automatically and overwrites from the ASA configuration.



Note To prevent any undesirable loss of device (target Firewall Threat Defense) configuration data, we recommend you to manually clean the device before migration.

During migration, the Secure Firewall migration tool resets the interface configuration. If you use these interfaces in policies, the Secure Firewall migration tool cannot reset them and hence the migration fails.

- The Secure Firewall migration tool can create subinterfaces on the native instance of the Firewall Threat Defense device based on the ASA configuration. Manually create interfaces and port channel interfaces on the target Firewall Threat Defense device before starting migration. For example, if your ASA configuration is assigned with the following interfaces and port channels, you must create them on the target Firewall Threat Defense device before the migration:
  - Five physical interfaces
  - Five port channels
  - Two management-only interfaces



Note For container instances of Firewall Threat Defense devices, subinterfaces are not created by the Secure Firewall migration tool, only interface mapping is allowed.

- The Secure Firewall migration tool can create subinterfaces and Bridge-Group Virtual Interfaces (transparent mode) on the native instance of the Firewall Threat Defense device that is based on the ASA configuration. Manually create interfaces and port channel interfaces on the target Firewall Threat Defense device before starting migration. For example, if your ASA configuration is assigned with the following interfaces and port channels, you must create them on the target Firewall Threat Defense device before the migration:
  - Five physical interfaces
  - Five port channels
  - Two management-only interfaces



Note For container instances of Firewall Threat Defense devices, subinterfaces are not created by the Secure Firewall migration tool, only interface mapping is allowed.

Supported Platforms for Migration

The following ASA and Firewall Threat Defense platforms are supported for migration with the Secure Firewall migration tool. For more information about the supported Firewall Threat Defense platforms, see Cisco Secure Firewall Compatibility Guide.

Note The Secure Firewall migration tool supports migration of standalone ASA devices to a standalone Firewall Threat Defense device only.

Supported Source ASA Platforms

You can use the Secure Firewall migration tool to migrate the configuration from the following single or multi-context ASA platforms:

- ASA 5510
- ASA 5520
- ASA 5540
- ASA 5550
- ASA 5580
- ASA 5506
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X
- ASA 5585-X with ASA only (the Secure Firewall migration tool does not migrate the configuration from the) ASA FirePOWER module
- Firepower 1000 Series
- Firepower 2100 Series
- Secure Firewall 3100 Series
- Firepower 4100 Series
- Secure Firewall 4200 Series

- Firepower 9300 Series
  - SM-24
  - SM-36
  - SM-40
  - SM-44
  - SM-48
  - SM-56
- ASA Virtual on VMware, deployed using VMware ESXi, VMware vSphere Web Client, or vSphere standalone client

Supported Target Firewall Threat Defense Platforms

You can use the Secure Firewall migration tool to migrate a source ASA configuration to the following standalone or container instance of the Firewall Threat Defense platforms:

- ASA 5506
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X
- Firepower 1000 Series
- Firepower 2100 Series
- Secure Firewall 220 Series
- Secure Firewall 3100 Series
- Secure Firewall 3200 Series
- Firepower 4100 Series
- Secure Firewall 4200 Series
- Secure Firewall 6100 Series
- Firepower 9300 Series that includes:
  - SM-24

- SM-36
- SM-40
- SM-44
- SM-48
- SM-56

- Threat Defense on VMware, deployed using VMware ESXi, VMware vSphere Web Client, or vSphere standalone client
- Threat Defense Virtual on Microsoft Azure Cloud or AWS Cloud

Note

- For pre-requisites and pre-staging of Firewall Threat Defense Virtual in Azure, see Getting Started with Secure Firewall Threat Defense Virtual and Azure.
- For pre-requisites and pre-staging of Firewall Threat Defense Virtual in AWS Cloud, see Threat Defense Virtual Prerequisites.

For each of these environments, once pre-staged as per the requirements, the Secure Firewall migration tool requires network connectivity to connect to the Firewall Management Center in Microsoft Azure or AWS Cloud, and then migrate the configuration to the Firewall Management Center in the Cloud.

Note The pre-requisites of pre-staging the Firewall Management Center or threat defense virtual is required to be completed before using the Secure Firewall migration tool, to have a successful migration.

Note The Secure Firewall migration tool requires network connectivity to any devices hosted in the cloud to either extract the source configuration (ASA Live Connect) or migrate the manually uploaded configuration to the Firewall Management Center in the cloud. Hence, as a pre-requisite, IP network connectivity is required to be pre-staged before using the Secure Firewall migration tool.

Supported Target Management Center for Migration

The Secure Firewall migration tool supports migration to threat defense devices managed by the management center and cloud-delivered Firewall Management Center.

Management Center

The management center is a powerful, web-based, multi-device manager that runs on its own server hardware, or as a virtual device on a hypervisor. You can use both On-Prem and Virtual management center as a target management center for migration.

The management center should meet the following guidelines for migration:

- The Management Center software version that is supported for migration, as described in Supported Software Versions for Migration, on page 37.
- You have obtained and installed smart licenses for Firewall Threat Defense that include all features that you plan to migrate from the ASA interface, as described in the following:
  - The Getting Started section of Cisco Smart Accounts on Cisco.com.
  - Register the Firewall Management Center with the Cisco Smart Software Manager.
  - Licensing the Firewall System
  - You have enabled Firewall Management Center for REST API.

    On the Firewall Management Center web interface, navigate to **System** > **Configuration** > **Rest API Preferences** > **Enable Rest API** and check the **Enable Rest API** check box.



Important You need to have an administrator user role in Firewall Management Center to enable REST API. For more information on management center user roles, see User Roles.

Cloud-Delivered Firewall Management Center

The cloud-delivered Firewall Management Center is a management platform for threat defense devices and is delivered via Security Cloud Control (formerly, Cisco Defense Orchestrator). The cloud-delivered Firewall Management Center offers many of the same functions as a management center.

You can access the cloud-delivered Firewall Management Center from Security Cloud Control. Security Cloud Control connects to cloud-delivered Firewall Management Center through the Secure Device Connector (SDC). For more information about cloud-delivered Firewall Management Center, see Managing Cisco Secure Firewall Threat Defense Devices with Cloud-Delivered Firewall Management Center.

The Secure Firewall migration tool supports cloud-delivered Firewall Management Center as a destination management center for migration. To select the cloud-delivered Firewall Management Center as destination management center for migration, you need to add the Security Cloud Control region and generate the API token from Security Cloud Control portal.

Security Cloud Control Regions

Security Cloud Control is available in three different regions and the regions can be identified with the URL extension.

Table 1: Security Cloud Control Regions and URL

Region	Security Cloud Control URL
Europe	https://eu.manage.security.cisco.com/

Region	Security Cloud Control URL
US	https://us.manage.security.cisco.com/
APJC	https://apj.manage.security.cisco.com/
Australia	https://au.manage.security.cisco.com/
India	https://in.manage.security.cisco.com/

Supported Software Versions for Migration

The topic lists the supported Secure Firewall Migration Tool, ASA and Firewall Threat Defense versions for migration:

Supported Secure Firewall Migration Tool Versions

The versions posted on software.cisco.com are the versions that are formally supported by our engineering and support organizations. We strongly recommend you download the latest version of the Secure Firewall Migration Tool from software.cisco.com.

Supported ASA Versions

The Secure Firewall Migration Tool supports migration from a device that is running ASA software version 8.4 and later.

Supported Firewall Management Center Versions for source ASA Configuration

For ASA, the Secure Firewall Migration Tool supports migration to a Firewall Threat Defense device managed by a Firewall Management Center that is running version 6.2.3 or 6.2.3+.

Note Some features are supported only in the later versions of Firewall Management Center and Firewall Threat Defense.

Note For optimum migration times, We recommend that you upgrade Firewall Management Center to the suggested release version provided here: software.cisco.com/downloads.

Supported Firewall Threat Defense Versions

The Secure Firewall Migration Tool recommends migration to a device that is running Firewall Threat Defense version 6.5 and later.

For detailed information about the Cisco Firewall software and hardware compatibility, including operating system and hosting environment requirements, for , see the Cisco Firewall Compatibility Guide.

Related Documentation

This section summarizes the ASA to Firewall Threat Defense migration related documentation.

- Cisco Secure Firewall ASA to Threat Defense Feature Mapping—Lists the commonly used ASA features and their equivalent threat defense capabilities. For each ASA feature, the equivalent threat defense feature with a UI path to configure it in the Secure Firewall Management Center or the cloud-delivered Firewall Management Center is listed.
- Migrating Certificates from ASA to Firepower Threat Defense—Describes the procedure to migrate Identity (ID) and Certificate Authority (CA) Certificates from Cisco ASA to a Secure Firewall Threat Defense device.
- Migrating ASA to Firepower Threat Defense Site-to-Site VPN Using IKEv1 with Certificates—Describes the procedure to migrate site-to-site IKEv1 VPN tunnels, using certificates (rsa-sig) as a method of authentication, from the existing Cisco ASA to Firewall Threat Defense, managed by Firewall Management Center.
- Migrating ASA to Firepower Threat Defense Site-to-Site VPN Using IKEv2 with Certificates—Describes the procedure to migrate site-to-site IKEv2 VPN tunnels, using certificates (rsa-sig) as a method of authentication, from the existing ASA to Firewall Threat Defense, managed by Firewall Management Center.
- Migrating ASA to Firepower Threat Defense Dynamic Crypto Map Based Site-to-Site Tunnel on FTD—Describes the procedure to migrate a Dynamic Crypto Map based site-to-site VPN tunnels (with IKEv1 or IKEv2), using pre-shared key and certificate as a method of authentication, from the existing ASA to Firewall Threat Defense, managed by Firewall Management Center.
- Migrating ASA to Firepower Threat Defense Site-to-Site VPN Using IKEv1 with Pre-Shared Key Authentication—Describes the procedure to migrate Site-to-Site IKEv1 VPN tunnels, using pre-shared key (PSK) as a method of authentication, from the existing ASA to Firewall Threat Defense, managed by Firewall Management Center.
- Migrating ASA to Firepower Threat Defense Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication—Describes the procedure to migrate site-to-site IKEv2 VPN tunnels, using pre-shared key (PSK) as a method of authentication, from the existing ASA to Firewall Threat Defense, managed by Firewall Management Center.
- Migrating ASA to Firepower Threat Defense Platform Settings—Describes the steps to migrate the platform setting configuration of ASA to Firewall Threat Defense devices.
- Cisco ASA FirePOWER Module Quick Start Guide—Describes how the ASA FirePOWER Module Works with the ASA.