Getting Started with the Secure Firewall Migration Tool

- 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 7
- Platform Requirements for the Secure Firewall Migration Tool, on page 7
- Requirements and Prerequisites for the ASA with FPS Configuration File, on page 7
- Requirements and Prerequisites for Threat Defense Devices, on page 8
- ASA with FPS Configuration Support, on page 8
- Guidelines and Limitations, on page 12
- Supported Platforms for Migration, on page 17
- Supported Target Management Center for Migration, on page 18
- Supported Software Versions for Migration, on page 19

About the Secure Firewall Migration Tool

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.

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

The Secure Firewall migration tool converts supported ASA with FPS configurations to a supported threat defense platform. The Secure Firewall migration tool allows you to automatically migrate supported ASA with FPS features and policies to threat defense. You must manually migrate all unsupported features.

The Secure Firewall migration tool gathers ASA with FPS information, parses it, and finally 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:

- ASA with FPS (Firewall Services) configuration items that are fully migrated, partially migrated, unsupported for migration, and ignored for migration.
- ASA with FPS configuration lines with errors that lists the ASA with FPS 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 ASA with FPS interfaces to 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 Reports**, **Post-Migration Reports**, ASA with FPS 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 with FPS 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** page.

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.

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
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: • 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.
3.0.2	The Secure Firewall Migration Tool 3.0.2 includes bug fixes for remote access VPN configuration migration from ASA with FirePOWER Services to Management Center versions 7.2 or higher.
3.0.1	• For ASA with FirePOWER Services, Check Point, Palo Alto Networks, and Fortinet, Secure Firewall 3100 series is only supported as a destination device.

3.0	The Secure Firewall migration tool 3.0 supports:
	• Remote Access VPN migration from ASA with FirePOWER Services 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 with FirePOWER Services.
	• The following must be performed as part of the pre-migration activity:
	  • The ASA with FirePOWER Services 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 with FirePOWER Services to allow retrieval of profiles from the Live Connect ASA.

Version	Supported Features
2.4	The Secure Firewall migration tool supports the migration of the Cisco Firewall Services (FPS) configurations to threat defense if the target management center and threat defense is 6.5 or later. • Migrate ASA with FPS access rules as management center Prefilter rules—Mapping of ASA with FPS access rules to management center for tailor deep inspection by Firewall. The access policy contains rules with IPs and ports. **Note** You can use prefilter and access control policies to block or allow traffic. The access rules from ASA are migrated as management center prefilter rules. The access rules from FPS are migrated into management center as access control policy. • The ASA with FPS rules is migrated as follows: ASA to FPS redirection ACLs are migrated as prefilter rules (conditional). **Note** You can migrate the FPS rules using the Secure Firewall migration tool only if the FPS module is managed through management center. • If the source redirection ACL has **Action=DENY**—migrated as management center Prefilter rule with **Action=Fastpath**. Also, this particular ACL is positioned as the first ACL rule in the DISABLED state. • If the source redirection ACL has**Action=Permit**—will not be migrated by Secure Firewall migration tool. • The Secure Firewall migration tooll does not support migration of ASDM-managed FPS rules into the Secure Firewall migration tool. Therefore you must be aware of the configuration information before you migrate while selecting the source configuration (ASA with FPS). The following ASA VPN configuration migration to 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 management center PKI objects. PKI objects are used in the Secure Firewall migration tool while creating certificate-based VPN topologies.

Licensing for the Secure Firewall Migration Tool

The Secure Firewall migration tool application is free and does not require license. However, the management center must have the required licenses for the related threat defense features to successfully register 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 the ASA with FPS Configuration File

You can obtain an ASA with FPS configuration file either manually or by connecting to a live ASA with FPS from the Secure Firewall migration tool.

ASA with FPS configuration file migration into the Secure Firewall migration tool is a two-step process:

- You can import the ASA with FPS configuration file using the manual method or live-connect method
- You must import the FPS configuration file by connecting to the management center that manages the FPS, and by selecting the required source ACL policy that needs to be migrated.

The ASA with FPS configuration file that you manually import into the Secure Firewall migration tool must meet the following requirements:

- Has a running configuration that is exported from an ASA with FPS device in a single mode configuration or specific context of a multiple context mode configuration. See Export the ASA with FPS Configuration File.
- Includes the version number.
- Contains only valid ASA with FPS CLI configurations.
- Does not contain syntax errors.
- Has a file extension of `.cfg` or `.txt`.
- Uses a file encoding of UTF-8.

- Has not been hand coded or manually altered. If you modify the ASA with FPS configuration, we recommend that you test the modified configuration file on the ASA with FPS device to ensure that it is a valid configuration.
- Does not contain the "--More--" keyword as text.

Requirements and Prerequisites for Threat Defense Devices

When you migrate to the management center, it may or may not have a target threat defense device added to it. You can migrate shared policies to a management center for future deployment to a threat defense device. To migrate device-specific policies to a threat defense, you must add it to the management center. As you plan to migrate your ASA with FPS configuration to threat defense, consider the following requirements and prerequisites:

- The target threat defense device must be registered with the management center.
- The threat defense device can be a standalone device or a container instance. It must **not** be part of a cluster or a high availability configuration.
  - 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 ASA with FPS; 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 with FPS; 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.

ASA with FPS Configuration Support

Supported ASA with FPS Configurations

The Secure Firewall migration tool can fully migrate the following ASA with FPS 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 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 which are not migrated
- Physical interfaces
- Secondary VLANs on ASA with FPS interfaces are not migrated to threat defense.
- Subinterfaces (subinterface ID is always 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 the objects to 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-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 threat defense.

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

  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 ASA with FPS to target FTD.
- 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 with FPS, the Secure Firewall migration tool migrates the crypto map to the 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 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 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 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.

Partially Supported ASA with FPS Configurations

The Secure Firewall migration tool partially supports the following ASA with FPS configurations for migration. Some of these configurations include rules with advanced options that are migrated without those options. If the 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 ASA with FPS Configurations

The Secure Firewall migration tool does not support the following ASA with FPS configurations for migration. If these configurations are supported in the management center, you can configure them manually after the migration is complete.

- SGT-based access control policy rules

- SGT-based objects
- User-based access control policy rules
- NAT rules that are configured with the block allocation option
- Objects with an unsupported ICMP type and code
- Tunneling protocol-based access control policy rules

Note Support with a prefilter on Secure Firewall migration tool and 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 management center
- User-based FPS ACLs, are not supported for migration and are migrated as disabled.
- Transparent firewall mode for BGP

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 management center.
- Outbound ACLs are **unsupported** and will not be migrated to management center. If the source firewall has outbound ACLs, it will be reported in the **ignored** section of the **Pre-Migration Report**.
- All supported ASA with FPS crypto map VPN will be migrated as management center point-to-point topology.
- Unsupported or incomplete static crypto map VPN topologies are not migrated.
- User-based FPS ACLs, are not supported for migration and are migrated as disabled.

ASA with FPS Configuration Limitations

Migration of your source ASA with FPS configuration has the following limitations:

- The Secure Firewall migration tool supports migrating individual security contexts from the ASA with FPS as separate 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 ASA with FPS configurations, for example, dynamic routing to threat defense. Migrate these configurations manually.
- You cannot migrate ASA with FPS devices in routed mode with a bridge virtual interface (BVI), redundant interface, or tunneled interface. However, you can migrate ASA with FPS devices in transparent mode with BVI.
- Nested service object-groups or port groups are not supported on the 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 management center rules with the exact same meaning.
- If the source ASA with FPS 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 ASA with FPS, then, on migration to the threat defense, the corresponding rules will not behave in the same way they do on the ASA with FPS. We recommend that you create specific tunnel rules for these in the Prefilter policy, on the threat defense.
- Supported ASA with FPS crypto map will be migrated as point-to-point topology.
- If an AS-Path object with the same name in management center appears, then the migration stops with the following error message:

  "Conflicting AS-Path object name detected in management center, please resolve conflict in management center to proceed further"
- Redistribution from OSPF and Routing Information Protocol (RIP) into EIGRP is not supported.

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 management center. You can make the necessary changes directly on the 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 with FirePOWER Services 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 with FirePOWER Services 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 with FirePOWER Services configuration it is ignored by the Secure Firewall migration tool and the address pool is migrated without the interface.
- ASA with FirePOWER Services 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 with FirePOWER Services configuration with these keywords, it is ignored by the Secure Firewall migration tool and the dhcp-server is pushed without the keywords.
- ASA with FirePOWER Services 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 with FirePOWER Services configuration it is ignored by the Secure Firewall migration tool and the commands are pushed without the interface.
- ASA with FirePOWER Services 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 with FirePOWER Services, it is left empty, and you must add and map it manually on the management center.
- ASA with FirePOWER Services 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 with FirePOWER Services 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.

Firewall Services (FPS) Migration Guidelines

The Secure Firewall migration tool uses best practices for threat defense configurations, including the following:

- The migration of the ACL log option follows the best practices for threat defense. The log option for a rule is enabled or disabled based on the source ASA with FPS 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.
- The ASA with FPS rules are migrated as follows:

  ASA with FPS redirection ACLs are migrated as prefilter rules (conditional).

Note You can migrate the FPS rules using the Secure Firewall migration tool only if the FPS module is managed through management center.

- If the source redirection ACL has **Action=DENY**—migrated as management center Prefilter rule with **Action=Fastpath**. Also, this particular ACL is positioned as the first ACL rule in DISABLED state.
- If the source redirection ACL has **Action=Permit**—will not be migrated by the Secure Firewall migration tool.

Object Migration Guidelines

ASA with FPS and threat defense have different configuration guidelines for objects. For example, one or more objects can have the same name in ASA with FPS 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 threat defense. To accommodate such differences, the Secure Firewall migration tool analyzes all ASA with FPS objects and handles their migration in one of the following ways:

- Each ASA with FPS object has a unique name and configuration—The Secure Firewall migration tool migrates the objects successfully without changes.
- The name of an ASA with FPS object includes one or more special characters that are not supported by the 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 ASA with FPS object has the same name and configuration as an existing object in the 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 ASA with FPS object.
- An ASA with FPS 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 ASA with FPS object for migration purposes.
- Multiple ASA with FPS 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 Threat Defense Devices

As you plan to migrate your ASA with FPS configuration to threat defense, consider the following guidelines and limitations:

- If there are any existing device-specific configurations on the 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 with FPS configuration.

Note To prevent any undesirable loss of device (target 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 threat defense device based on the ASA with FPS configuration. Manually create interfaces and port channel interfaces on the target threat defense device before starting migration. For example, if your ASA with FPS configuration is assigned with the following interfaces and port channels, you must create them on the target threat defense device before the migration:
  - Five physical interfaces
  - Five port channels
  - Two management-only interfaces

Note For container instances of 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 threat defense device that is based on the ASA with FPS configuration. Manually create interfaces and port channel interfaces on the target threat defense device before starting migration. For example, if your ASA with FPS configuration is assigned with the following interfaces and port channels, you must create them on the target threat defense device before the migration:
  - Five physical interfaces
  - Five port channels
  - Two management-only interfaces

Note For container instances of 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 with FPS and threat defense platforms are supported for migration with the Secure Firewall migration tool. For more information about the supported threat defense platforms, see Cisco Secure Firewall Compatibility Guide.

Note The Secure Firewall migration tool supports migration of standalone ASA with FPS devices to a standalone threat defense device only.

Supported Source ASA models for ASA with FPS migration:

The Cisco ASA FirePOWER module is deployed on the following devices:

- ASA5506-X
- ASA5506H-X
- ASA5506W-X
- ASA5508-X
- ASA5512-X
- ASA5515-X
- ASA5516-X
- ASA5525-X
- ASA5545-X
- ASA5555-X
- ASA5585-X-SSP-10
- ASA5585-X-SSP-20
- ASA5585-X-SSP-40
- ASA5585-X-SSP-60

Supported Target Threat Defense Platforms

You can use the Secure Firewall migration tool to migrate a source ASA with FPS configuration to the following standalone or container instance of the threat defense platforms:

- Firepower 1000 Series
- Firepower 2100 Series
- Secure Firewall 3100 Series
- Firepower 4100 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 threat defense virtual in Azure, see Getting Started with Secure Firewall Threat Defense Virtual and Azure.
- For pre-requisites and pre-staging of 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 management center in Microsoft Azure or AWS Cloud, and then migrate the configuration to the management center in the Cloud.

Note The pre-requisites of pre-staging the 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 migrate the manually uploaded configuration to the 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 19.
- You have obtained and installed smart licenses for threat defense that include all features that you plan to migrate from the ASA with FPS 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 management center for REST API.

    On the 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 management center to enable REST API. For more information on management center user roles, see User Roles.

Supported Software Versions for Migration

The following are the supported Secure Firewall migration tool, ASA with FPS and threat defense versions for migration:

Supported Secure Firewall Migration Tool Versions

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

Supported ASA with FPS Versions

The Secure Firewall migration tool supports migration from a device that is running ASA with FPS software version 9.2.2+ and later.

For more details, see ASA FirePOWER Module Compatibility section in the Cisco ASA Compatibility guide.

Supported Management Center Versions for source ASA with FPS Configuration

For ASA with FPS, the Firewall Migration Tool supports migration to a threat defense device managed by a management center that is running version 6.5+.

Supported Threat Defense Versions

The Secure Firewall migration tool recommends migration to a device that is running 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 threat defense, see the Cisco Firewall Compatibility Guide.