Getting Started with the Secure Firewall Migration Tool

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: PAN to Threat defense 2100) included in this book helps to facilitate understanding of the migration process.

The Secure Firewall migration tool converts supported PAN configurations to a supported Secure Firewall Threat Defense platform. The Secure Firewall migration tool allows you to automatically migrate the supported PAN features and policies to threat defense. You must manually migrate all unsupported features.

The Secure Firewall migration tool gathers PAN 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:

- PAN configuration XML lines with errors

- PAN lists the PAN XML lines that the Secure Firewall migration tool cannot recognize. Report the XML configuration lines under error section in the **Pre-Migration Report** and the console logs; this blocks migration

If there are parsing errors, you can rectify the issues, reupload a new configuration, connect to the destination device, map the interfaces to threat defense interfaces, map applications, map security zones 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**, PAN configs, and logs in the **Resources** folder.

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

Unparsed 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
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.

Version	Supported Features
4.0.2	The Secure Firewall migration tool 4.0.2 includes the following new features and enhancements: • Secure Firewall migration tool now supports splitting of access control lists (ACLs) with applications per rule. When your Palo Alto Networks firewall configuration contains ACLs with one rule configured to more than one application, you can use the **Split ACLs with applications per rule** option to split the rule into multiple rules with one application per rule. The migration tool creates new rules such that one rule is configured to one application, which ensures more clarity in reviewing and validating the configuration. • The migration tool now validates the NAT configuration in your source firewall for dynamic IP or port-fallback addresses and migrates the configurations only if the fallback address is same as the destination zone address. This is because the Secure Firewall Management Center can have only the destination address as the dynamic IP or port-fallback interface. • 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?**.
4.0.1	The Secure Firewall migration tool 4.0.1 includes the following new features and enhancements: • The Secure Firewall migration tool now supports Network Address Translation (NAT) rules with fully qualified domain name (FQDN) objects in the translated destination when migrating to a management center version 7.1 or higher. **Important** NAT rules with FQDN objects or FQDN object groups in the translated source, NAT rules with FQDN objects and FQDN object groups both in the original source and destination, and NAT rules with FQDN object groups in the translated destination are not supported. • The ACL optimization is now enhanced to include a new **Application** column in the post-migration report, which lists the optimized applications.
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 provides support to migrate to Cloud-delivered Firewall Management Center from Palo Alto Networks if the destination management center is 7.2 or later.

Version	Supported Features
2.1	• Provides support for PAN OS versions 6.1.x and later • The Secure Firewall migration tool allows you to migrate the following PAN configuration elements to threat defense: • Interfaces • Static Routes • Network Objects and Groups • Port Objects and Port Groups • Access Control Lists (Policies) • Zones • Applications • NAT Rules • Content-based search capability that is enabled on **Review and Validate** page • A progress bar is provided as part of UI enhancement

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 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 PAN 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.

  - 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 PAN; 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.

Guidelines and Limitations

The Secure Firewall migration tool creates a one-to-one mapping for all the supported objects and rules, whether they are used in a rule or policy during conversion.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 does not migrate unsupported objects, NAT rules, and routes.

PAN Configuration Limitations

Migration of the source PAN configuration has the following limitations:

- The Secure Firewall migration tool allows migration of multi-vsys.

- The system configuration is not migrated.

- Nested service object groups or port group are not supported in 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 objects 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 same meaning.

PAN 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 PAN 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.

Supported PAN Configurations

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

- Network objects and groups

- Zones (Layer 2, Layer 3, Virtual wire)

- Service objects

- 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)

- Access rules

- NAT rules

Note All the policies with service as "application-default" will be migrated as "any" as threat defense does not have an equivalent feature.

Translated source and original destination do not have pre-defined "any" object on management center. Hence, an object with 0.0.0.0/0 named Obj_0.0.0.0 will be created and pushed.

- NAT rules with an FQDN object in the translated destination, when migrating to Secure Firewall Threat Defense running version 7.1 or higher

- Physical interfaces

- Subinterfaces (subinterface ID is always set to the same number as the VLAN ID on migration)

- Aggregate Interface (Port channels)

- Static routes, except for those configured with Next Hop as Next VR and ECMP routes which are not migrated

Note If the source firewall (PAN) has connected routes that are configured as static routes, it results in a push failure. management center does not allow you to create static routes for connected routes. Remove any such route and proceed with the migration.

Note Virtual wire interface will not be migrated whereas virtual wire zone will be migrated. You must manually create BVI interface on threat defense after migration.

Partially Supported PAN Configurations

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

- Access control policy rules using profiles
- Service-Group that contains service objects with protocols containing TCP, UDP, and SCTP.

Note The SCTP type will be removed and the service-group will be migrated partially.

- Object-group that contains supported and unsupported object will be migrated by removing the unsupported objects.

Unsupported PAN Configurations

The Secure Firewall migration tool does not support the following PAN configurations for migration. You can configure the configurations manually after the migration is complete, if these configurations are supported in the management center:

- Time-based access control policy rules
- User-based access control policy rules
- Service-object using protocol SCTP
- FQDN objects that begin with a special character or that contains a special character
- Wildcard FQDNs
- NAT rules that are configured with SCTP
- NAT rule with an FQDN object and FQDN object group in the translated source
- NAT rule with an FQDN object and FQDN object group in both original source and destination
- NAT rule with an FQDN object group in the translated destination
- IPv6 NAT
- Policies that use URL filtering

To configure unsupported features on threat defense, see Threat Defense Configuration Guide.

Note All policies that are either supported or unsupported are migrated to management center. The unsupported policies are migrated as disabled. You can enable these policies after the workaround or configuring them as permanagement center.

Policy with profile URL filtering, User-ID, source, or destination negate is **Unsupported**.

Guidelines and Limitations for Threat Defense Devices

As you plan to migrate your PAN configuration to threat defense, 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 PAN configuration.

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

Supported Platforms for Migration

The following PAN 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.

Supported Target Threat Defense Platforms

You can use the Secure Firewall migration tool to migrate a source 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

- Secure Firewall 4200 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.

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 15.

- The management center software version that is supported for migration for PAN is 6.1.x and later.

- You have obtained and installed smart licenses for threat defense that include all features that you plan to migrate from the PAN 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.

Cloud-Delivered Firewall Management Center

The cloud-delivered Firewall Management Center is a management platform for threat defense devices and is delivered via 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 CDO. CDO 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 CDO region and generate the API token from CDO portal.

CDO Regions

CDO is available in three different regions and the regions can be identified with the URL extension.

Table 1: CDO Regions and URL

Region	CDO URL
Europe Region	https://defenseorchestrator.eu/
US Region	https://defenseorchestrator.com/
APJC Region	https://www.apj.cdo.cisco.com/

Supported Software Versions for Migration

The following are the supported Secure Firewall migration tool, PAN 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 Palo Alto Networks Firewall Versions

The Secure Firewall migration tool supports migration to threat defense that is running PAN firewall OS version 6.1.x and later.

Supported Management Center Versions for source PAN Firewall Configuration

For PAN firewall, the Secure Firewall migration tool supports migration to a management center device managed by a management center that is running version 6.2.3.3 or later.

Note The migration to 6.7 threat defense device is currently not supported. Hence, migration may fail if the device is configured with data interface for management center access.

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.