

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 3
- Licensing for the Secure Firewall Migration Tool, on page 17
- Platform Requirements for the Secure Firewall Migration Tool, on page 17
- Requirements and Prerequisites for the Fortinet firewall Configuration File, on page 17
- Requirements and Prerequisites for Threat Defense Devices, on page 17
- Fortinet Configuration Support, on page 18
- Guidelines and Limitations for Fortinet Firewall Configurations, on page 20
- Supported Platforms for Migration, on page 21
- Supported Target Management Center for Migration, on page 23
- Supported Software Versions for Migration, on page 24

About the Secure Firewall Migration Tool

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

The Secure Firewall Migration Tool migrates the supported Fortinet configurations to a supported Secure Firewall Threat Defense platform. The Secure Firewall Migration Tool allows you to automatically migrate the supported Fortinet 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.

The Secure Firewall Migration Tool gathers Fortinet 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:

- Fortinet configuration items that are fully migrated, partially migrated, unsupported for migration, and ignored for migration

- Fortinet configuration lines with errors, and Fortinet CLIs that the Secure Firewall Migration Tool cannot recognize (this blocks migration).

If there are parsing errors, you can rectify the issues, re-upload a new configuration, connect to the destination device, map the interfaces to Firewall 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 Report**, **Post-Migration Report**, Fortinet 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 Fortinet 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.

Version	Supported Features
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.
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

Version	Supported Features
7.7.10.4	This patch release contains bug fixes.
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: • 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?**.
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 Fortinet 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 Fortinet 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 Fortinet 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.
2.3	• Provides support for Fortinet firewall OS versions: 5.0 and later • The Secure Firewall migration tool allows you to migrate the following Fortinet configuration elements to Firewall Threat Defense: • Interfaces • Zones • Static Routes • Network Objects and Groups • Service Objects and Groups • Access Control Lists • NAT dependent objects (IP pool, Virtual IP) • NAT Rules • VDOM • 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. **Note** Time-based objects are supported on Firewall Management Center version 6.6 and above.

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 the Fortinet firewall Configuration File

You can obtain a Fortinet firewall configuration file manually.

The Fortinet firewall 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 a Fortinet device. Configuration backup from both the Global and per–VDOM export is supported in the Firewall Migration Tool. For more information, see Export the Fortinet Configuration File.
- Contains only valid Fortinet firewall 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 Fortinet firewall configuration, we recommend that you test the modified configuration file on the Fortinet firewall device to ensure that it is a valid configuration.

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 Fortinet firewall 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.
  - 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 Fortinet firewall; 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.

Fortinet Configuration Support

Supported Fortinet Firewall Configurations

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

- Network objects and groups (except Wildcard FQDN, Wildcard Mask, Fortinet Dynamic Objects)
- Service objects
- Service object groups (except for nested service object groups)

Note Because nesting is not supported on the management center, the Secure Firewall migration tool expands the content of the referenced rules. The rules, however, are migrated with full functionality.

- URL objects
- IPv4 and IPv6 FQDN objects and groups
- IPv6 conversion support (Interface, Static Routes, Objects, ACL, and NAT)
- IPv6 SSL VPN
- Multiple interfaces and intetface zones in an SSL VPN configuration
- Central SNAT

- Access rules
- NAT rules
- Static routes, ECMP routes which are not migrated
- Physical interfaces
- Subinterfaces (subinterface ID will always be set to the same number as the VLAN ID on migration)
- Aggregate Interfaces (Port channels)
- The Secure Firewall migration tool supports migration of individual VDOMs from the Fortinet firewall as separate Threat Defense devices.
- 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 the respective access-rules. Verify the objects against the rules in the **Optimize, Review and Validate Configuration** page.

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



Note

- You must manually migrate timezone configuration from source Fortinet to the target threat defense.
- Time-based objects are not supported for non-threat defense flows and will be disabled.
- Time-based objects are supported on the management center version 6.6 and later.

Partially Supported Fortinet Firewall Configurations

The Secure Firewall migration tool partially supports the following Fortinet firewall 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.

- Address Group that contains unsupported Address Objects.
- Service group that contains service objects with protocols containing TCP or UDP, and SCTP.



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

Unsupported Fortinet Firewall Configurations

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

- User-based, Device-based, and Internet-Service ID based access control policy rules
- Service Objects with an unsupported ICMP type and code
- Tunneling protocol-based access control policy rules
- NAT rules that are configured with the block allocation option
- NAT rules that are configured with SCTP
- NAT rules that are configured with host ‘0.0.0.0’
- NAT rule with an FQDN object in the source or destination
- FQDN objects that begin with a special character or that contain a special character
- Wildcard FQDNs
- Fortinet firewall allows configuring policy that combines IPv4 and IPv6 (consolidated policy). However, the migration tool does not support migrating such configurations.

Guidelines and Limitations for Fortinet Firewall Configurations

During conversion, the Secure Firewall migration tool creates a one-to-one mapping for all supported objects and rules, irrespective of 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 of the ACLs and NATs).

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

- Unsupported interfaces, objects, NAT rules, and routes are not migrated.
- Unsupported ACL rules are migrated into the management center as disabled rules.

Fortinet Firewall Configuration Limitations

Migration of the source Fortinet firewall configuration has the following limitations:

- The system configuration is not migrated.
- The Secure Firewall migration tool does not support migration of a single ACL policy that is applied to 50 or more interfaces. You have to manually migrate ACL policies that are applied to 50 or more interfaces.
- Fortinet firewall interfaces that are of type virtual wire, redundant interface, tunnel interface, vdom-link and SDwan-interface or zone are unsupported and are not migrated.

  Fortinet Hardware or Software-switch logical interface will be migrated as threat defense L3-interfaces. Hardware or Software-switch member interfaces will not be migrated using the Secure Firewall migration tool.

- Migration of objects such as Wildcard FQDN, Wildcard IP, Dynamic objects, and Exclusion groups are unsupported.
- Fortinet firewall devices in Transparent mode or Transparent VDOM cannot be migrated.
- Nested service object-groups and port groups are not supported on the management center. As part of the 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 exact same meaning.

Fortinet Firewall Migration Guidelines

The Secure Firewall migration tool uses best practices for threat defense configurations.

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 Fortinet firewall 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.

Guidelines and Limitations for Threat Defense Devices

As you plan to migrate your 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 configuration.



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

- Fortinet Hardware or Software-switch logical interface will be migrated as threat defense L3-interfaces. Hardware or Software-switch member interfaces will not be migrated using Secure Firewall migration tool.

  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

Supported Platforms for Migration

The following Fortinet 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.

Supported Target Firewall 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 Firewall Threat Defense platforms:

- 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.

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 24.
- You have obtained and installed smart licenses for Firewall Threat Defense that include all features that you plan to migrate from the Fortinet 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/
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, Fortinet 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 Fortinet Firewall Versions

The Secure Firewall Migration Tool supports migration to Firewall Threat Defense that is running Fortinet firewall OS version 5.0 and later.

Supported Firewall Management Center Versions for source Fortinet Firewall Configuration

For Fortinet firewall, the Secure Firewall Migration Tool supports migration to a Firewall Threat Defense device managed by a Firewall Management Center that is running version 6.2.3.3 or later.

Note The migration to 6.7 Firewall Threat Defense device is currently not supported. Hence, migration may fail if the device is configured with data interface for Firewall Management Center access.

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.