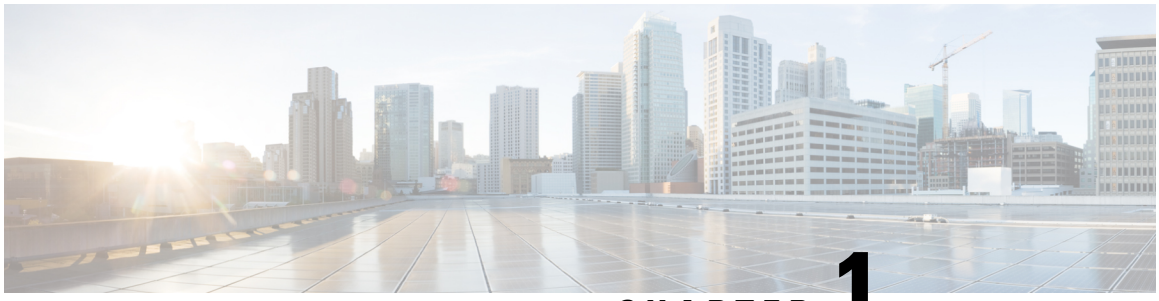
Migrating Fortinet Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool

First Published: 2022-11-22

Last Modified: 2024-04-29

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

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

The Secure Firewall migration tool converts 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 threat defense. You must manually migrate all unsupported features.

The Secure Firewall migration tool gathers Fortinet 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:

- Fortinet configuration items that are fully migrated, partially migrated, unsupported for migration, and ignored for migration
- Fortinet configuration lines with errors, lists the Fortinet CLIs that the Secure Firewall migration tool cannot recognize; 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**, Fortinet 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.

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
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 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 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 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 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 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 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 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 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 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 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.

- URL objects
- IPv4 and IPv6 FQDN objects and groups
- IPv6 conversion support (Interface, Static Routes, Objects, ACL, and NAT)
- 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 allows configuring policy that combines IPv4 and IPv6 (consolidated policy).

Note This policy is not supported by the Secure Firewall migration tool.

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 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 17.

- You have obtained and installed smart licenses for 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 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, Fortinet 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 Fortinet Firewall Versions

The Secure Firewall migration tool supports migration to threat defense that is running Fortinet firewall OS version 5.0 and later.

Supported Management Center Versions for source Fortinet Firewall Configuration

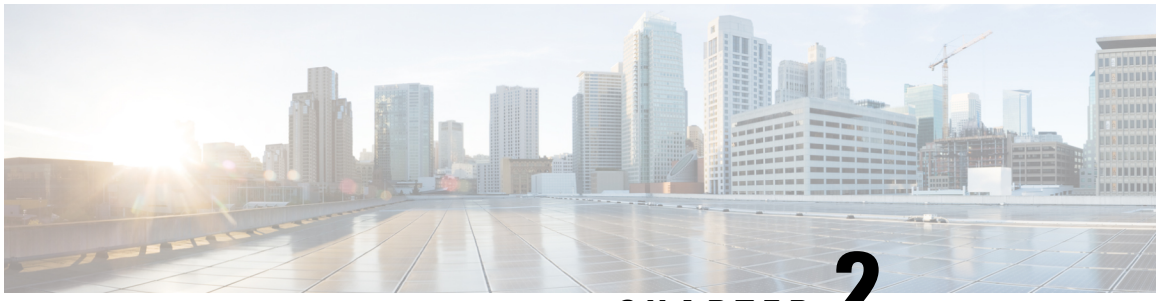
For Fortinet firewall, the Secure Firewall migration tool supports migration to a threat defense device managed by a management center that is running version 6.2.3.3 or later.

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.

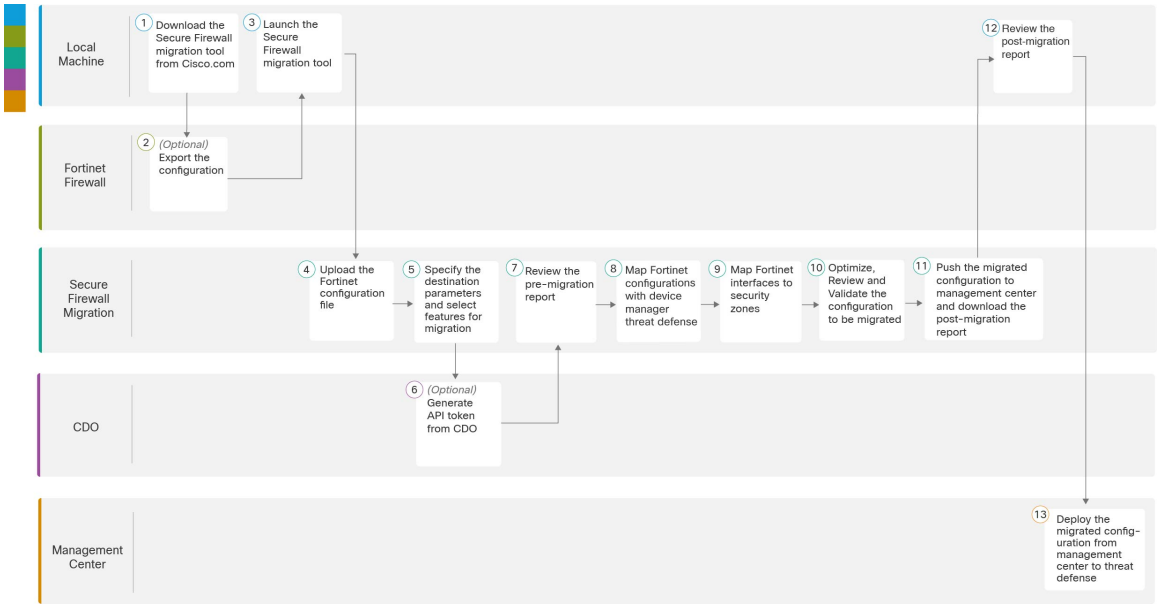


CHAPTER 2

Fortinet Firewall to Threat Defense Migration Workflow

End-to-End Procedure

The following flowchart illustrates the workflow for migrating a Fortinet firewall to threat defense using the Secure Firewall migration tool.



	Workspace	Steps
1	Fortnet Frewall	Export the configuration to the local system, see Download the Secure Firewall Migration Tool from Cisco.com.
2	Fortinet Firewall	Export the Configuration File: To export the configuration from Fortinet firewall, see Export the Configuration from Fortinet Firewall.
3	Local Machine	Launch the Secure Firewall migration tool on your local machine, see Launch the Secure Firewall Migration Tool.
4	Secure Firewall Migration Tool	Upload the Fortinet config file exported from Fortinet firewall, see Upload the Fortinet Configuration File.
5	Secure Firewall Migration Tool	During this step, you can specify the destination parameters for the migration. For detailed steps, see Specify Destination Parameters for the Secure Firewall Migration Tool. .
6	CDO	(Optional) This step is optional and only required if you have selected cloud-delivered Firewall Management Center as destination management center. For detailed steps, see Specify Destination Parameters for the Secure Firewall Migration Tool.
7	Secure Firewall Migration Tool	Navigate to where you downloaded the pre migration report and review the report. For detailed steps, see Review the Pre-Migration Report.
8	Secure Firewall Migration Tool	To ensure that the Fortinet configuration is migrated correctly, map the Fortinet interfaces to the appropriate threat defense interface objects, security zones and interface groups. For detailed steps, see Map Fortinet Firewall Configurations with Threat Defense Interfaces
9	Secure Firewall Migration Tool	Map the Fortinet interfaces to the appropriate security zones, see Map Fortinet Interfaces to Security Zones Interface Groups for detailed steps.
10	Secure Firewall Migration Tool	Optimize and review the configuration carefully and validate that it is correct and matches how you want to configure the threat defense device. For detailed steps, see Optimize, Review and Validate the Configuration.
11	Secure Firewall Migration Tool	This step in the migration process sends the migrated configuration to management center and allows you to download the post-migration report. For detailed steps, see Push the Migrated Configuration to Management Center.
12	Local Machine	Navigate to where you downloaded the post migration report and review the report. For detailed steps, see Review the Post-Migration Report and Complete the Migration.
13	Management Center	Deploy the migrated configuration from the management center to threat defense. For detailed steps, see Review the Post-Migration Report and Complete the Migration.

Prerequisites for Migration

Before you migrate your Fortinet configuration, execute the following activities:

Download the Secure Firewall Migration Tool from Cisco.com

Before you begin

You must have a Windows 10 64-bit or macOS version 10.13 or higher machine with an internet connectivity to Cisco.com.

Step 1 On your computer, create a folder for the Secure Firewall migration tool.

We recommend that you do not store any other files in this folder. When you launch the Secure Firewall migration tool, it places the logs, resources, and all other files in this folder.

Note Whenever you download the latest version of the Secure Firewall migration tool, ensure, you create a new folder and not use the existing folder.

Step 2 Browse to https://software.cisco.com/download/home/286306503/type and click **Firewall Migration Tool**.

The above link takes you to the Secure Firewall migration tool under Firewall NGFW Virtual. You can also download the Secure Firewall migration tool from the threat defense device download areas.

Step 3 Download the most recent version of the Secure Firewall migration tool into the folder that you created.

Download the appropriate executable of the Secure Firewall migration tool for Windows or macOS machines.

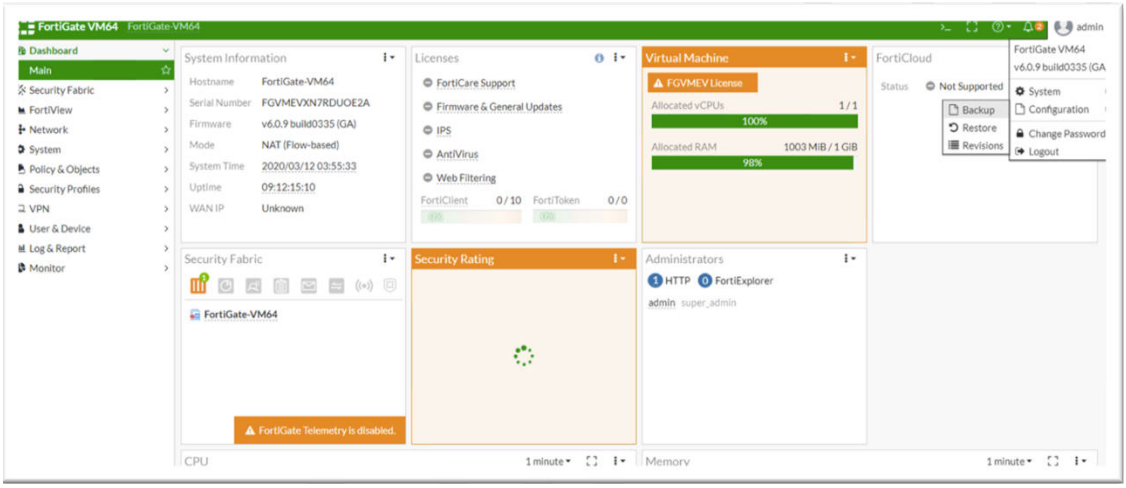
Export the Configuration from Fortinet Firewall

You can export Fortinet firewall configurations in the following ways:

Export Fortinet Firewall Configuration from Fortinet Firewall GUI

Follow these steps to extract the configuration from the Fortinet firewall GUI:

Step 1 From the FortiGate VM64 GUI, choose **Admin** > **Configuration** > **Backup** .



Step 2 Direct the backup to your local PC or to a USB disk.

Note If VDOMs are enabled, indicate whether the scope of the backup is for the entire FortiGate configuration (Global) or only for a specific VDOM configuration (VDOM).

Step 3 Select the VDOM name from the **VDOM** list if the back up is a VDOM configuration.

Note The Secure Firewall migration tool requires an unencrypted file to proceed with the backup process.

Step 4 Select **Ok**.

The web browser prompts you for a location to save the configuration file.

The configuration file has a **.conf** extension.

What to do next

Upload the Fortinet Configuration File

Export Fortinet Firewall Configuration from FortiManager

You can extract the relevant device configuration from FortiManager.

Step 1 Login to FortiManager.

Step 2 Locate the correct Fortigate device for which you must run the backup.

Step 3 Under **Configuration and Installation Status**, choose the icon next to **Total Revision** to get the latest revision.

Step 4 Click **Download** to download the config file.

The downloaded file is a file type with .conf extension.

What to do next

Upload the Fortinet Configuration File

Run the Migration

Launch the Secure Firewall Migration Tool

This task is applicable only if you are using the desktop version of the Secure Firewall migration tool. If you are using the cloud version of the migration tool hosted on CDO, skip to Upload the Fortinet Configuration File.

Note When you launch the Secure Firewall migration tool a console opens in a separate window. As you go through the migration, the console displays the progress of the current step in the Secure Firewall migration tool. If you do not see the console on your screen, it is most likely to be behind the Secure Firewall migration tool.

Before you begin

- Download the Secure Firewall Migration Tool from Cisco.com
- Review and verify the requirements in the Supported Target Management Center for Migration, on page 15 section.
- Ensure that your computer has a recent version of the Google Chrome browser to run the Secure Firewall migration tool. For information on how to set Google Chrome as your default browser, see Set Chrome as your default web browser.
- If you are planning to migrate a large configuration file, configure sleep settings so the system doesn't go to sleep during a migration push.

Step 1 On your computer, navigate to the folder where you downloaded the Secure Firewall migration tool.

Step 2 Do one of the following:

- On your Windows machine, double-click the Secure Firewall migration tool executable to launch it in a Google Chrome browser.

  If prompted, click **Yes** to allow the Secure Firewall migration tool to make changes to your system.

  The Secure Firewall migration tool creates and stores all related files in the folder where it resides, including the log and resources folders.

- On your Mac move, the Secure Firewall migration tool `*.command` file to the desired folder, launch the Terminal application, browse to the folder where the Secure Firewall migration tool is installed and run the following commands:

```
# chmod 750 Firewall_Migration_Tool-version_number.command
# ./Firewall_Migration_Tool-version_number.command
```

The Secure Firewall migration tool creates and stores all related files in the folder where it resides, including the log and resources folders.

Tip When you try to open the Secure Firewall migration tool, you get a warning dialog because the Secure Firewall migration tool is not registered with Apple by an identified developer. For information on opening an application from an unidentified developer, see Open an app from an unidentified developer.

Note Use MAC terminal zip method.

Step 3 On the **End User License Agreement** page, click **I agree to share data with Cisco Success Network** if you want to share telemetry information with Cisco, else click **I'll do later**.

When you agree to send statistics to Cisco Success Network, you are prompted to log in using your Cisco.com account. Local credentials are used to log in to the Secure Firewall migration tool if you choose not to send statistics to Cisco Success Network.

Step 4 On the Secure Firewall migration tool's login page, do one of the following:

- To share statistics with Cisco Success Network, click the **Login with CCO** link to log in to your Cisco.com account using your single sign-on credentials. If you do not have a Cisco.com account, create it on the Cisco.com login page.

  Proceed to step 8, if you have used your Cisco.com account to log in.

- If you have deployed your firewall in an air-gapped network that does not have internet access, contact Cisco TAC to receive a build that works with administrator credentials. Note that this build does not send usage statistics to Cisco, and TAC can provide you the credentials.

Step 5 On the **Reset Password** page, enter the old password, your new password, and confirm the new password.

The new password must have 8 characters or more and must include upper and lowercase letters, numbers, and special characters.

Step 6 Click **Reset**.

Step 7 Log in with the new password.

Note If you have forgotten the password, delete all the existing data from the <*migration_tool_folder*> and reinstall the Secure Firewall migration tool.

Step 8 Review the pre-migration checklist and make sure you have completed all the items listed.

If you have not completed one or more of the items in the checklist, do not continue until you have done so.

Step 9 Click **New Migration**.

Step 10 On the **Software Update Check** screen, if you are not sure you are running the most recent version of the Secure Firewall migration tool, click the link to verify the version on Cisco.com.

Step 11 Click **Proceed**.

What to do next

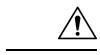
You can proceed to the following step:

- If you must extract information from a Fortinet firewall using the Secure Firewall migration tool, proceed to Export the Configuration from Fortinet Firewall.

Using the Demo Mode in the Secure Firewall Migration Tool

When you launch the Secure Firewall Migration tool and are on the **Select Source Configuration** page, you can choose to start performing a migration using **Start Migration** or enter the **Demo Mode**.

The demo mode provides an opportunity to perform a demo migration using dummy devices and visualize how an actual migration flow would look like. The migration tool triggers the demo mode based on the selection you make in the **Source Firewall Vendor** drop-down; you can also upload a configuration file or connect to a live device and continue with the migration. You can proceed performing the demo migration by selecting demo source and target devices such as demo FMC and demo FTD devices.



Caution Choosing **Demo Mode** erases existing migration workflows, if any. If you use the demo mode while you have an active migration in **Resume Migration**, your active migration is lost and needs to be restarted from first, after you use the demo mode.

You can also download and verify the pre-migration report, map interfaces, map security zones, map interface groups, and perform all other actions like you would in an actual migration workflow. However, you can only perform a demo migration up to validation of the configurations. You cannot push the configurations to the demo target devices you selected because this is only a demo mode. You can verify the validation status and the summary and click **Exit Demo Mode** to go the **Select Source Configuration** page again to start your actual migration.

Note The demo mode lets you leverage the whole feature set of the Secure Firewall Migration Tool, except pushing of configurations, and do a trial run of the end-to-end migration procedure before performing your actual migration.

Upload the Fortinet Configuration File

Before you begin

Export the configuration file as `.conf` or `.txt` from the source Fortinet device.

Note Do not upload a hand-coded or manually altered configuration file. Text editors add blank lines and other issues to the file that can cause the migration to fail.

Step 1 The Secure Firewall migration tool uploads the configuration file. For large configuration files, this step takes a longer time. The console provides a line by line log view of the progress, including the Fortinet configuration line that is being parsed. If you do not see the console, you can find it in a separate window behind the Secure Firewall migration tool. The **Context Selection** section identifies if the uploaded configuration corresponds to the multi-context Fortinet.

Step 2 Review the **Context Selection** section and select the Fortinet VDOM that you want to migrate.

Step 3 Click **Start Parsing**.

The **Parsed Summary** section displays the parsing status.

Step 4 Review the summary of the elements in the uploaded configuration file that the Secure Firewall migration tool detected and parsed.

Step 5 Click **Next** to select the target parameters.

What to do next

Specify Destination Parameters for the Secure Firewall Migration Tool, on page 26

Specify Destination Parameters for the Secure Firewall Migration Tool

Before you begin

If you are using the cloud version of the migration tool hosted on CDO, skip to Step 3.

- Obtain the IP address for the management center for On-Prem Firewall Management Center.
- From Secure Firewall Migration Tool 3.0 onwards, you can select between On-Prem Firewall Management Center or Cloud-delivered Firewall Management Center.
- For Cloud-delivered Firewall Management Center, region and API token have to be provided. For more information, see Supported Target Management Center for Migration.
- (Optional) If you want to migrate device-specific configurations like interfaces and routes, add the target threat defense to the management center. See Adding Devices to the Firewall Management Center
- If it requires you to apply IPS or file policy to ACL in the **Review and Validate** page, we highly recommend you create a policy on the management center before migration. Use the same policy, as the Secure Firewall migration tool fetches the policy from the connected management center. Creating a new policy and assigning it to multiple access control lists may degrade the performance and may also result in a push failure.

Step 1 On the **Select Target** screen, in the **Firewall Management** section, do the following: you can choose to migrate to an On-Prem Firewall Management Center or Cloud-delivered Firewall Management Center:

- For migrating to an On-Prem Firewall Management Center, do the following:

a) Click the **On-Prem FMC** radio button.
b) Enter the IP address or Fully-Qualified Domain Name (FQDN) for the management center.
c) In the **Domain** drop-down list, select the domain to which you are migrating.

   If you want to migrate to a threat defense device, you can only migrate to the threat defense devices available in the selected domain.

d) Click **Connect** and proceed to **Step 2**.

- For migrating to a Cloud-delivered Firewall Management Center, do the following:

a) Click the **Cloud-delivered FMC** radio button.
b) Choose the region and paste the CDO API token. For generating the API token. from CDO, follow the below steps:

   1. Log in to CDO portal.

2. Navigate to **Settings** > **General Settings** and copy the API Token.

c) Click **Connect** and proceed to **Step 2**.

Step 2 In the **Firewall Management Center Login** dialog box, enter the username and password of the dedicated account for the Secure Firewall migration tool, and click **Login**.

The Secure Firewall migration tool logs in to the management center and retrieves a list of threat defense devices that are managed by that management center. You can view the progress of this step in the console.

Step 3 Click **Proceed**.

Step 4 In the **Choose Threat Defense** section, do one of the following:

- Click the **Select Firewall Threat Defense Device** drop-down list and check the device where you want to migrate the Fortinet configuration.

  The devices in the selected management center domain are listed by **IP Address** and **Name**.

  Note At minimum, the native threat defense device you choose must have the same number of physical or port channel interfaces as the Fortinet configuration that you are migrating. At minimum, the container instance of the threat defense device must have the same number of physical or port channel interfaces and subinterfaces. You must configure the device with the same firewall mode as the Fortinet configuration. However, these interfaces do not have to have the same names on both devices.

  Note Only when the supported target threat defense platform is Firewall 1010 with management center version 6.5 or later.6.5, FDM 5505 migration support is applicable for shared policies and not for device specific policies. When you proceed without threat defense, the Secure Firewall migration tool will not push any configurations or the policies to the threat defense. Thus, interfaces and routes, and site-to-site VPN which are threat defense device-specific configurations will not be migrated. However, all the other supported configurations (shared policies and objects) such as NAT, ACLs, and port objects will be migrated. Remote Access VPN is a shared policy and can be migrated even without threat defense.

  Fortinet firewall migration to management center or threat defense 6.7 or later with the Remote deployment enabled is supported by the Secure Firewall migration tool. However, migration of Interface and Routes must be migrated manually.

- Click **Proceed without FTD** to migrate the configuration to the management center.

  When you proceed without threat defense, the Secure Firewall migration tool will not push any configurations or the policies to threat defense. Thus, interfaces and routes, and site-to-site VPN which are threat defense device-specific configurations will not be migrated and need to be manually configured on management center. However, all the other supported configurations (shared policies and objects) such as NAT, ACLs, and port objects will be migrated. Remote Access VPN is a shared policy and can be migrated even without threat defense.

Step 5 Click **Proceed**.

Depending on the destination that you are migrating to, the Secure Firewall migration tool allows you to select the features that you want to migrate.

Step 6 Click the **Select Features** section to review and select the features that you want to migrate to the destination.

- If you are migrating to a destination threat defense device, the Secure Firewall migration tool automatically selects the features available for migration from the Fortinet configuration in the **Device Configuration** and **Shared Configuration** sections. You can further modify the default selection, according to your requirements.

- If you are migrating to a management center, the Secure Firewall migration tool automatically selects the features available for migration from the Fortinet configuration in the **Device Configuration**, **Shared Configuration**, and **Optimization** sections. You can further modify the default selection, according to your requirements.
- If you are migrating a configuration from a Fortinet firewall, and if you have VPN configured in your Fortinet firewall, ensure that you do the following on the **Select Features** pane:
  - The migration tool displays your site-to-site VPN features under **Device Configuration**. Select **Policy Based (Crypto Map)** or **Route Based (VTI)**, depending on your requirement.
  - The migration tool displays your remote-access VPN features under **Shared Configuration**.
  - Select **SSL VPN** or both **IPsec VPN** and **SSL VPN**.

    Note You cannot select only **IPsec VPN** because pre-shared key-based (PSK-based) or certificate-based authentication is not supported in management center for remote access VPN configurations.

  If your Fortinet firewall configuration has site-to-site and remote access VPN configured, they are selected by default in the **Select Features** pane. Use the checkboxes to unselect them, if required.
- The Secure Firewall migration tool supports Destination Security Zones that enable mapping of destination zones for the ACL during migration.

  Based on the nature of source and destination network object or groups and service object or groups, this operation may result in ACL rule explosion when migrating from Fortinet to management center.
- (Optional) In the **Optimization** section, select **Migrate only referenced objects** to migrate only those objects that are referenced in an access control policy and a NAT policy.

  Note When you select this option, unreferenced objects in the Fortinet configuration will not be migrated. This optimizes migration time and cleans out unused objects from the configuration.

Step 7 Click **Proceed**.

Step 8 In the **Rule Conversion/ Process Config** section, click **Start Conversion** to initiate the conversion.

Step 9 Review the summary of the elements that the Secure Firewall migration tool converted.

To check whether your configuration file is successfully uploaded and parsed, download and verify the **Pre-Migration Report** before you continue with the migration.

Step 10 Click **Download Report** and save the **Pre-Migration Report**.

A copy of the **Pre-Migration Report** is also saved in the `Resources` folder in the same location as the Secure Firewall migration tool.

Review the Pre-Migration Report

If you have missed to download the Pre-Migration Reports during migration, use the following link to download:

Pre-Migration Report Download Endpoint—http://localhost:8888/api/downloads/pre_migration_summary_html_format

Note You can download the reports only when the Secure Firewall migration tool is running.

Step 1 Navigate to where you downloaded the **Pre-Migration Report**.

A copy of the **Pre-Migration Report** is also saved in the `Resources` folder in the same location as the Secure Firewall migration tool.

Step 2 Open the **Pre-Migration Report** and carefully review its contents to identify any issues that can cause the migration to fail.

The **Pre-Migration Report** includes the following information:

- A summary of the supported Fortinet configuration elements that can be successfully migrated to threat defense and specific Fortinet features selected for migration.
- **Configuration Lines with Errors**—Details of Fortinet configuration elements that cannot be successfully migrated because the Secure Firewall migration tool could not parse them. Correct these errors on the Fortinet configuration, export a new configuration file, and then upload the new configuration file to the Secure Firewall migration tool before proceeding.
- **Partially Supported Configuration**—Details of Fortinet configuration elements that can be only partially migrated. These configuration elements include rules and objects with advanced options where the rule or the object can be migrated without the advanced options. Review these lines, verify whether the advanced options are supported in management center, and if so, plan to configure those options manually after you complete the migration with the Secure Firewall migration tool.
- **Unsupported Configuration**—Details of Fortinet configuration elements that cannot be migrated because the Secure Firewall migration tool does not support migration of those features. Review these lines, verify whether each feature is supported in management center, and if so, plan to configure the features manually after you complete the migration with the Secure Firewall migration tool.
- **Ignored Configuration**—Details of Fortinet configuration elements that are ignored because they are not supported by the management center or the Secure Firewall migration tool. The Secure Firewall migration tool does not parse these lines. Review these lines, verify whether each feature is supported in management center, and if so, plan to configure the features manually.

For more information about supported features in management center and threat defense, see Management Center Configuration Guide.

Step 3 If the **Pre-Migration Report** recommends corrective actions, complete those corrections on the Fortinet interface, export the Fortinet configuration file again and upload the updated configuration file before proceeding.

Step 4 After your Fortinet configuration file is successfully uploaded and parsed, return to the Secure Firewall migration tool, and click **Next** to continue the migration.

What to do next

Map Fortinet Firewall Configurations with Threat Defense Interfaces

Map Fortinet Firewall Configurations with Threat Defense Interfaces

The threat defense device must have an equal or greater number of physical and port channel interfaces than those used by Fortinet configuration. These interfaces do not have to have the same names on both devices. You can choose how you want to map the interfaces.

On the **Map FTD Interface** screen, the Secure Firewall migration tool retrieves a list of interfaces on the threat defense device. By default, the Secure Firewall migration tool maps the interfaces in Fortinet and the threat defense device according to their interface identities.

The mapping of Fortinet interface to the threat defense interface differs based on the threat defense device type:

- If the target threat defense is of native type:
  - The threat defense must have equal or a greater number of used Fortinet interfaces or port channel (PC) data interfaces (excluding management-only and subinterfaces in the Fortinet configuration). If the number is less, add the required type of interface on the target threat defense.
  - Subinterfaces are created by the secure Firewall migration tool based on physical interface or port channel mapping.
- If the target threat defense is of container type:
  - The threat defense must have equal or a greater number of used Fortinet interfaces, physical subinterfaces, port channel, or port channel subinterfaces (excluding management-only in Fortinet configuration). If the number is less, add the required type of interface on the target threat defense. For example, if the number of physical interfaces and physical subinterface on the target threat defense is 100 less than that of Fortinet then you can create the additional physical or physical subinterfaces on the target threat defense.
  - Subinterfaces are not created by the Secure Firewall migration tool. Only interface mapping is allowed between physical interfaces, port channel, or subinterfaces.

Before you begin

Make sure you have connected to the management center and chosen the destination as threat defense. For more information, see Specify Destination Parameters for the Secure Firewall Migration Tool, on page 26.

Note This step is not applicable if you are migrating to a management center without a threat defense device.

Step 1 If you want to change an interface mapping, click the drop-down list in the **FTD Interface Name** and choose the interface that you want to map to that Fortinet interface.

You cannot change the mapping of the management interfaces. If a threat defense interface has already been assigned to an Fortinet interface, you cannot choose that interface from the drop-down list. All assigned interfaces are greyed out and unavailable.

You do not need to map subinterfaces. The Secure Firewall migration tool maps subinterfaces on the threat defense device for all subinterfaces in the Fortinet configuration.

Step 2 When you have mapped each Fortinet interface to a threat defense interface, click **Next**.

What to do next

Map the Fortinet interfaces to the appropriate threat defense interface objects, security zones, and interface groups. For more information, see Map Fortinet Interfaces to Security Zones Interface Groups.

Map Fortinet Interfaces to Security Zones Interface Groups

To ensure that the Fortinet configuration is migrated correctly, map the Fortinet interfaces to the appropriate threat defense interface objects, security zones and interface groups. In an Fortinet configuration, access control policies and NAT policies use interface names (nameif). In management center, those policies use interface objects. In addition, management center policies group interface objects into the following:

- Security zones—An interface can belong to only one security zone.

The Secure Firewall migration tool allows one-to-one mapping of interfaces with security zones; when a security zone is mapped to an interface, it is not available for mapping to other interfaces although the management center allows it. For more information about security zones in management center, see Security Zones and Interface Groups in *Cisco Secure Firewall Management Center Device Configuration Guide*.

Step 1 To map interfaces to security zones and interface groups that exist in management center, or that is available in configuration files as Security Zone type objects and is available in the drop-down list, do the following:

a) In the **Security Zones** column, choose the security zone for the interface.
b) In the **Interface Groups** column, choose the interface group for the interface.

Step 2 To map interfaces to security zones that exist in management center, in the **Security Zones** column, choose the security zone for that interface.

Step 3 You can manually map or auto-create the security zones.

To map the security zones manually, perform the following:

a) Click **Add SZ**.
b) In the **Add SZ** dialog box, click **Add** to add a new security zone.
c) Enter the security zone name in the **Security Zone** column. The maximum characters allowed is 48.
d) Click **Close**.

To map the security zones through auto-creation, perform the following:

a) Click **Auto-Create**.
b) In the **Auto-Create** dialog box, check **Zone Mapping**.
c) Click **Auto-Create**.

Once you click **Auto-Create**, the source firewall zones are mapped automatically. If the same name zones already exist on management center, then the zone will be re-used. The mapping page will display "(A)" against the re-used zone. For example, **inside** "(A)".

Step 4 When you have mapped all interfaces to the appropriate security zones, click **Next**.

Optimize, Review and Validate the Configuration

Before you push the migrated Fortinet configuration to management center, optimize and review the configuration carefully and validate that it is correct and matches how you want to configure the threat defense device. A flashing tab indicates that you must take the next course of action.

Note If you close the Secure Firewall migration tool at the **Optimize, Review and Validate Configuration** screen, it saves your progress and allows you to resume the migration later. If you close the Secure Firewall migration tool before this screen, your progress is not saved. If there is a failure after parsing, relaunching the Secure Firewall migration tool resumes from the **Interface Mapping** screen.

Here, the Secure Firewall migration tool fetches the Intrusion Prevention System (IPS) policies and file policies, which are already present on the management center and allows you to associate those to the access control rules you are migrating.

A file policy is a set of configurations that the system uses to perform Advanced Malware Protection for networks and file control, as part of your overall access control configuration. This association ensures that before the system passes a file in traffic that matches the conditions of the access control rule, it first inspects the file.

Similarly, you can use an IPS policy as the system's last line of defense before traffic is allowed to proceed to its destination. Intrusion policies govern how the system inspects traffic for security violations and, in inline deployments, can block or alter malicious traffic. Whenever the system uses an intrusion policy to evaluate traffic, it uses an associated variable set. Most variables in a set represent values commonly used in intrusion rules to identify source and destination IP addresses and ports. You can also use variables in intrusion policies to represent IP addresses in rule suppression and dynamic rule states.

To search for specific configuration items on a tab, enter the item name in the field at the top of the column. The table rows are filtered to display only items that match the search term.

Note By default, the Inline Grouping option is enabled.

If you close the Secure Firewall migration tool at the **Optimize, Review and Validate Configuration** screen, it saves your progress and allows you to resume the migration later. If you close the before this screen, your progress is not saved. If there is a failure after parsing, relaunching the Secure Firewall migration tool resumes from the **Interface Mapping** screen.

Secure Firewall Migration Tool ACL Optimization Overview

The Secure Firewall migration tool provides support to identify and segregate ACLs that can be optimized (disabled or deleted) from the firewall rule base without impacting the network functionality.

The ACL optimization supports the following ACL types:

- Redundant ACL—When two ACLs have the same set of configurations and rules, then removing the non-base ACL will not impact the network. For example, if any two rule allows FTP and IP traffic on the same network with no rules that are defined for denying access, the first rule can be deleted.
- Shadow ACL—The first ACL completely shadows the configurations of the second ACL. If two rules have similar traffic, the second rule is not applied to any traffic as it appears later in the access list. If the two rules specify different actions for traffic, you can either move the shadowed rule or edit any one of

the rules to implement the required policy. For example, the base rule may deny the IP traffic, and the shadowed rule may allow FTP traffic for a given source or destination.

The Secure Firewall migration tool uses the following parameters while comparing rules for ACL optimization:

Note Optimization is available for the Fortinet only for ACP rule action.

- The disabled ACLs are not considered during the optimization process.
- The source ACLs are expanded into the corresponding ACEs (inline values), and then compared for the following parameters:
  - Source and Destination Zones
  - Source and Destination Network
  - Source and Destination Port

Click **Download Report** to review the ACL name and the correponding redundant and shadowed ACLs tabulated in an Excel file. Use the **Detailed ACL Information** sheet to view more ACL information. The **Applications** column lists the applications associated with the ACL in your Fortinet firewall.

Step 1 On the **Optimize, Review and Validate Configuration** screen, click **Access Control Rules** and do the following:

a) For each entry in the table, review the mappings and verify that they are correct.

A migrated access policy rule uses the ACL name as prefix and appends the ACL policy ID to it to make it easier to map back to the Fortinet configuration file. For example, if a Fortinet ACL is named "inside_access", then the first rule (or ACE) line in the ACL will be named as "inside_access_#1". If a rule must be expanded because of TCP/UDP combinations, an extended service object, or some other reason, the Secure Firewall migration tool adds a numbered suffix to the name. For example, if the allow rule is expanded into two rules for migration, they are named "inside_access _#1-1" and " inside_access_#1-2".

For any rule that includes an unsupported object, the Secure Firewall migration tool appends an "_UNSUPPORTED" suffix to the name.

b) If you do not want to migrate one or more access control list policies, choose the rows by checking the box against the policy, choose **Actions** > **Do not migrate** and then click **Save**.

All rules that you choose not to migrate are grayed out in the table.

c) If you want to apply a management center file policy to one or more access control policies, check the box for the appropriate rows, choose **Actions** > **File Policy**.

In the **File Policy** dialog, select the appropriate file policy and apply it to the selected access control policies and click **Save**.

d) If you want to apply a management center IPS policy to one or more access control policies, check the box for the appropriate rows, choose **Actions** > **IPS Policy**.

In the **IPS Policy** dialog, select the appropriate IPS policy and its corresponding variable set and apply it to the selected access control policies and click **Save**.

e) If you want to change the logging options for an access control rule which has logging enabled, check the box for the appropriate row and choose **Actions** > **Log**.

In the **Log** dialog, you can enable logging events either at the beginning or end of a connection or both. If you enable logging, you must opt to send the connection events either to the **Event Viewer** or to the **Syslog** or both. When you opt to send connection events to a syslog server, you can choose the syslog policies that are already configured on the management center from the **Syslog** drop-down menu.

f) If you want to change the actions for the migrated access control rules in the Access Control table, check the box for the appropriate row and choose **Actions** > **Rule Action**.

Tip The IPS and file policies that are attached to an access control rule are automatically removed for all rule actions except for the **Allow** option.

You can filter the ACE counts in the ascending, descending, equal, greater than, and lesser than filtering order sequence.

To clear the existing filter criteria, and to load a new search, click **Clear Filter**.

Note The order that you sort the ACL based on ACE is for viewing only. The ACLs are pushed based on the chronological order in which they occur.

Step 2 Click the following tabs and review the configuration items:

- **Access Control**
- **Objects (Network Objects, Port Objects, VPN Objects, URL Objects)**
- **NAT**
- **Interfaces**
- **Routes**
- **Site-to-Site VPN Tunnels**
- **Remote Access VPN**

Note For site-to-site and remote access VPN configurations, VPN filter configurations and extended access list objects pertaining to them are migrated and can be reviewed under the respective tabs.

If you do not want to migrate one or more NAT rules or route interfaces, check the box for the appropriate rows, choose **Actions** > **Do not migrate**, and then click **Save**.

All rules that you choose not to migrate are grayed out in the table.

Step 3 (Optional) While reviewing your configuration, you can rename one or more network or port objects in the **Network Objects** or the **Port Objects** tab by selecting the object and choosing **Actions** > **Rename**.

Access rules and NAT policies that reference the renamed objects are also updated with new object names.

Step 4 You can view routes from the **Routes** area and select the routes that you do not want to migrate, by selecting an entry and choosing **Actions** > **Do not migrate**.

Step 5 In the **Site-to-Site VPN Tunnels** section, the VPN tunnels from the source firewall configurations are listed. Review the VPN tunnel data such as **Source Interface**, **VPN Type**, and **IKEv1** and **IKEv2** configurations for each row and ensure that you provide the preshared key values for all the rows.

Step 6 In the **Remote Access VPN** section, all objects corresponding to remote access VPN are migrated from Fortinet to the management center, and are displayed:

- **Policy Assignment**: Review and validate your connection profiles, their VPN protocols, targeted devices, and the names of the VPN interfaces. To rename a connection profile, select the corresponding entry and choose **Actions** > **Rename**.
- **IKEV2**: Review and validate your IKEv2 protocol configurations, if any, and the source interfaces mapped with them.
- **Anyconnect Packages**: Retreive the AnyConnect packages and AnyConnect profiles should be retrieved from the source Fortinet device for migration.

  As part of the premigration activity, upload all the AnyConnect packages to the management center. You can upload AnyConnect profiles either directly to the management center or from the Secure Firewall migration tool.

  Select pre-existing AnyConnect, Hostscan, or external browser packages retrieved from the management center. You must select atleast one AnyConnect package. You must also select the Hostscan, dap.xml, data.xml, or external browser, if they are available in the source configuration. AnyConnect profiles are optional.

  Ensure that the correct Dap.xml file is retrieved from the source firewall. Validations are performed on the dap.xml file that are available in the configuration file. You must select all the files that are required for validation and upload them. Failure to update marks as incomplete and the Secure Firewall migration tool does not proceed with validation.
- **Address Pool**—Review all the IPv4 and IPv6 pools that are displayed here.
- **Group-Policy**—Select or remove the user profile, management profile, and client module profile from this area, which displays group policies with client profiles, management profiles, client modules, and group policies without profiles. If a profile was added in the AnyConnect file area, it is displayed as preselected. You can select or remove the user profile, management profile, and client module profile.
- **Connection Profile**—Review all connection profiles/tunnel groups that are displayed here.
- **Trustpoints**—Trustpoint or PKI object migration from the Fortinet firewall to the management center is part of the premigration activity and is required for successful migration of remote access VPN. Map the trustpoint for Global SSL, IKEv2, and interfaces in the **Remote Access Interface** section to proceed with the migration.

  If a Security Assertion Markup Language (SAML) object exists, the trustpoint for the SAML IDP and SP can be mapped in the SAML section. SP certificate upload is optional. Trustpoints can be overridden for a specific tunnel group. If the overriden SAML trustpoint configuration is available in the source Fortinet firewall, it can be selected under **Override SAML**.

Step 7 (Optional) To download the details for each configuration item in the grid, click **Download**.

Step 8 After you have completed your review, click **Validate**. Note that the mandatory fields that need your attention keeps flickering until you enter values in them. The **Validate** button gets enabled only after all the mandatory fields are filled.

During validation, the Secure Firewall migration tool connects to management center, reviews the existing objects, and compares those objects to the list of objects to be migrated. If an object already exists in management center, the Secure Firewall migration tool does the following:

- If the object has the same name and configuration, the Secure Firewall migration tool reuses the existing object and does not create a new object in management center.
- If the object has the same name but a different configuration, the Secure Firewall migration tool reports an object conflict.

You can view the validation progress in the console.

Step 9 When the validation is complete, if the **Validation Status** dialog box shows one or more object conflicts, do the following:

a) Click **Resolve Conflicts**.

The Secure Firewall migration tool displays a warning icon on either or both of the **Network Objects** or **Port Objects** tab, depending upon where the object conflicts were reported.

b) Click the tab and review the objects.
c) Check the entry for each object that has a conflict and choose **Actions** > **Resolve Conflicts**.
d) In the **Resolve Conflicts** window, complete the recommended action.

For example, you might be prompted to add a suffix to the object name to avoid a conflict with the existing management center object. You can accept the default suffix or replace it with one of your own.

e) Click **Resolve**.
f) When you have resolved all object conflicts on a tab, click **Save**.
g) Click **Validate** to revalidate the configuration and confirm that you have resolved all object conflicts.

Step 10 When the validation is complete and the **Validation Status** dialog box displays the message **Successfully Validated**, continue with Push the Migrated Configuration to Management Center, on page 36.

Push the Migrated Configuration to Management Center

You cannot push the migrated Fortinet configuration to management center if you have not successfully validated the configuration and resolved all object conflicts.

This step in the migration process sends the migrated configuration to management center. It does not deploy the configuration to the threat defense device. However, any existing configuration on the threat defense is erased during this step.

Note Do not make any configuration changes or deploy to any device while the Secure Firewall migration tool is sending the migrated configuration to management center.

Step 1 In the **Validation Status** dialog box, review the validation summary.

Step 2 Click **Push Configuration** to send the migrated Fortinet configuration to management center.

The Secure Firewall migration tool displays a summary of the progress of the migration. You can view detailed, line-by-line progress of which the components that are being pushed to management center in the console.

Step 3 After the migration is complete, click **Download Report** to download and save the post-migration report.

Copy of the **Post-Migration Report** is also saved in the `Resources` folder in the same location as the Secure Firewall migration tool.

Step 4 If your migration failed, review the post-migration report, log file, and unparsed file carefully to understand what caused the failure.

You can also contact the support team for troubleshooting.

Migration Failure Support

If the migration is unsuccessful, contact Support.

a. On the **Complete Migration** screen, click the **Support** button.

The Help support page appears.

b. Check the **Support Bundle** check box and then select the configuration files to download.

Note The Log and dB files are selected for download by default.

c. Click **Download**.

The support bundle file is downloaded as a .zip to your local path. Extract the Zip folder to view the log files, DB, and the Configuration files.

d. Click **Email us** to email the failure details for the technical team.

You can also attach the downloaded support files to your email.

e. Click **Visit TAC page** to create a TAC case in the Cisco support page.

Note You can open a TAC case at any time during the migration from the support page.

Review the Post-Migration Report and Complete the Migration

The Post-migration report provides details on ACL count under various categories, ACL optimization, and the overall view of optimization performed on the configuration file. For more information, see Optimize, Review and Validate the Configuration, on page 32

Review and verify the objects:

- **Category**
  - Total ACL rules (Source Configuration)
  - Total ACL rules considered for Optimization. For example, Redundant, Shadow, and so on.
- ACL Count for optimization gives the total number of ACL rules counted before and after Optimization.

If you have missed to download the Post-Migration Reports during migration, use the following link to download:

Post-Migration Report Download Endpoint—http://localhost:8888/api/downloads/post_migration_summary_html_format

Note You can download the reports only when the Secure Firewall migration tool is running.

Step 1 Navigate to where you downloaded the **Post-Migration Report**.

Step 2 Open the post-migration report and carefully review its contents to understand how your Fortinet configuration was migrated:

- **Migration Summary**—A summary of the configuration that was successfully migrated from Fortinet to threat defense, including information about the Fortinet interface, management center hostname and domain, target threat defense device (if applicable), and the successfully migrated configuration elements.
- **Selective Policy Migration**—Details of the specific Fortinet feature selected for migration are available within three categories - Device Configuration Features, Shared Configuration Features, and Optimization.
- **Fortinet Interface to Threat Defense Interface Mapping**—Details of the successfully migrated interfaces and how you mapped the interfaces on the Fortinet configuration to the interfaces on the threat defense device. Confirm that these mappings match your expectations.

  Note This section is not applicable for migrations without a destination threat defense device or if **Interfaces** are **not** selected for migration.

- **Source Interface Names to Threat Defense Security Zones**—Details of the successfully migrated Fortinet logical interfaces and name and how you mapped them to security zones in threat defense. Confirm that these mappings match your expectations.

  Note This section is not applicable if **Access Control Lists** and **NAT** are **not** selected for migration.

- **Object Conflict Handling**—Details of the Fortinet objects that were identified as having conflicts with existing objects in management center. If the objects have the same name and configuration, the Secure Firewall migration tool reused the management center object. If the objects have the same name but a different configuration, you renamed those objects. Review these objects carefully and verify that the conflicts were appropriately resolved.
- **Access Control Rules, NAT, and Routes You Chose Not to Migrate**—Details of the rules that you choose not to migrate with the Secure Firewall migration tool. Review these rules that were disabled by the Secure Firewall migration tool and were not migrated. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.
- **Partially Migrated Configuration**—Details of the Fortinet rules that were only partially migrated, including rules with advanced options where the rule could be migrated without the advanced options. Review these lines, verify whether the advanced options are supported in management center, and if so, configure these options manually.
- **Unsupported Configuration**—Details of Fortinet configuration elements that were not migrated because the Secure Firewall migration tool does not support migration of those features. Review these lines, verify whether each feature is supported in threat defense. If so, configure those features manually in management center.
- **Expanded Access Control Policy Rules**—Details of Fortinet access control policy rules that were expanded from a single Fortinet Point rule into multiple threat defense rules during migration.
- **Actions Taken on Access Control Rules**
  - **Access Rules You Chose Not to Migrate**—Details of the Fortinet access control rules that you choose not to migrate with the Secure Firewall migration tool. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.
  - **Access Rules with Rule Action Change**—Details of all Access Control Policy Rules that had ‘Rule Action’ changed using the Secure Firewall migration tool. The Rule Action values are - Allow, Trust, Monitor, Block, Block with reset. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.
  - **Access Control Rules that have IPS Policy and Variable Set Applied**—Details of all Fortinet access control policy rules that have IPS Policy applied. Review these rules carefully and determine whether the feature is supported in threat defense.

- **Access Control Rules that have File Policy Applied**—Details of all Fortinet access control policy rules that have File Policy applied. Review these rules carefully and determine whether the feature is supported in threat defense.
- **Access Control Rules that have Rule 'Log' Setting Change**—Details of the Fortinet access control rules that had 'Log setting' changed using the Secure Firewall migration tool. The Log Setting values are - False, Event Viewer, Syslog. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.

Note An unsupported rule that was not migrated causes issues with unwanted traffic getting through your firewall. We recommend that you configure a rule in management center to ensure that this traffic is blocked by threat defense.

Note If it requires you to apply IPS or file policy to ACL in the **Review and Validate** page, you are highly recommended to create a policy on the management center before migration. Use the same policy, as the Secure Firewall migration tool fetches the policy from the connected management center. Creating a new policy and assigning it to multiple policies may degrade the performance and may also result in a push failure.

For more information about supported features in management center and threat defense, see Management Center Configuration Guide, Version 6.2.3.

Step 3 Open the **Pre-Migration Report** and make a note of any Fortinet configuration items that you must migrate manually on the threat defense device.

Step 4 In management center, do the following:

a) Review the migrated configuration for the threat defense device to confirm that all expected rules and other configuration items, including the following, were migrated:

- Access control lists (ACL)
- Network Address Translation rules
- Port and network objects
- Routes
- Interfaces

b) Configure all partially supported, unsupported, ignored, and disabled configuration items and rules that were not migrated.

For information on how to configure these items and rules, see the Management Center Configuration Guide. The following are examples of configuration items that require manual configuration:

- Platform settings, including SSH and HTTPS access, as described in Platform Settings for Threat Defense
- Syslog settings, as described in Configure Syslog
- Dynamic routing, as described in Routing Overview for Threat Defense
- Service policies, as described in FlexConfig Policies
- VPN configuration, as described in Threat Defense VPN
- Connection log settings, as described in Connection Logging

Step 5 After you have completed your review, deploy the migrated configuration from management center to the threat defense device.

Verify that the data is reflected correctly in the **Post-Migration Report** for unsupported and partially supported rules.

The Secure Firewall migration tool assigns the policies to the threat defense device. Verify that the changes are reflected in the running configuration. To help you to identify the policies that are migrated, the description of those policies includes the hostname of the Fortinet configuration.

Uninstall the Secure Firewall Migration Tool

All components are stored in the same folder as the Secure Firewall migration tool.

Step 1 Navigate to the folder where you placed the Secure Firewall migration tool.

Step 2 If you want to save the logs, cut or copy and paste the `log` folder to a different location.

Step 3 If you want to save the pre-migration reports and the post-migration reports, cut or copy and paste the `resources` folder to a different location.

Step 4 Delete the folder where you placed the Secure Firewall migration tool.

Tip The log file is associated with the console window. If the console window for the Secure Firewall migration tool is open, the log file and the folder cannot be deleted.

Sample Migration: Fortinet to Threat Defense 2100

Note Create a test plan that you can run on the target device after you complete the migration.

- Pre-Maintenance Window Tasks
- Maintenance Window Tasks

Pre-Maintenance Window Tasks

Before you begin

Make sure you have installed and deployed a management center. For more information, see the appropriate Management Center Hardware Installation Guide and the appropriate Management Center Getting Started Guide.

Step 1 Save a copy of the Global or per–VDOM configuration from the source Fortinet that you want to migrate.

Step 2 Deploy the Firepower 2100 series device in your network, connect the interfaces and power on the appliance.

For more information, see Cisco Threat Defense for the 2100 Series Using Management Center Quick Start Guide.

Step 3 Register the Firepower 2100 series device to be managed by the management center.

For more information, see Add Devices to the Management Center.

Step 4 (Optional) If your source Fortinet configuration has aggregate interfaces, create port channels (EtherChannels) on the target Firepower 2100 series device.

For more information, see Configure EtherChannels and Redundant Interfaces.

Step 5 Download and run the most recent version of the Secure Firewall migration tool from https://software.cisco.com/download/home/286306503/type.

For more information, see Download the Secure Firewall Migration Tool from Cisco.com, on page 21.

Step 6 When you launch the Secure Firewall migration tool, and specify destination parameters, make sure that you select the Firepower 2100 series device that you registered to the management center.

For more information, see Specify Destination Parameters for the Secure Firewall Migration Tool, on page 26.

Step 7 Map the Fortinet interfaces with the threat defense interfaces.

Note The Secure Firewall migration tool allows you to map an Fortinet interface type to the threat defense interface type.

For example, you can map an aggregate interfaces in Fortinet to a physical interface in threat defense.

For more information, see Map Fortinet Firewall Configurations with Threat Defense Interfaces.

Step 8 While mapping logical interfaces to security zones, click **Auto-Create** to allow the Secure Firewall migration tool to create new security zones. To use existing security zones, manually map the Fortinet logical interfaces to the security zones.

For more information, see Map Fortinet Interfaces to Security Zones Interface Groups.

Step 9 Follow the instructions of this guide to sequentially review and validate the configuration to be migrated, and then push the configuration to the management center.

Step 10 Review the Post Migration report, manually setup and deploy other configurations to the threat defense and complete the migration.

For more information, see .

Step 11 Test the Firepower 2100 series device using the test plan that you would have created while planning for migration.

Maintenance Window Tasks

Before you begin

Make sure you have completed all the tasks that must be performed before the maintenance window. See Pre-Maintenance Window Tasks, on page 40.

Step 1 Clear the Address Resolution Protocol (ARP) cache on the surrounding switching infrastructure.

Step 2 Perform basic ping tests from surrounding switching infrastructure to the Firepower 2100 series device interface IP addresses, to make sure that they are accessible.

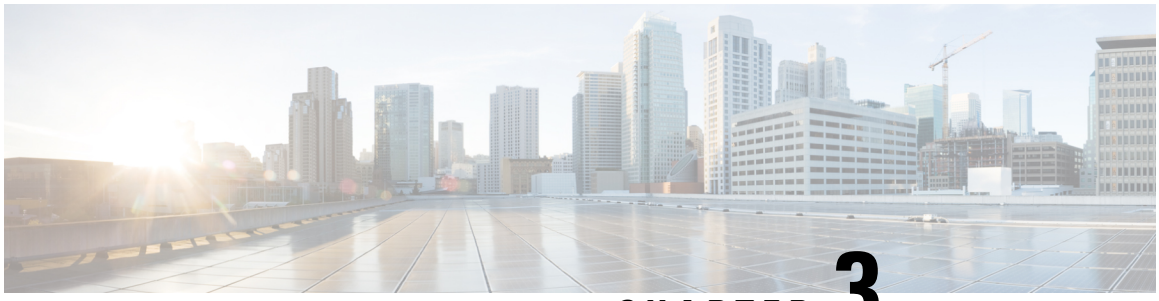
Step 3 Perform basic ping tests from devices which require layer 3 routing to Firepower 2100 series device interface IP addresses.

Step 4 If you are assigning a new IP address to the Firepower 2100 series device and not reusing the IP address assigned to the perform the following steps:

a. Update any static routes which refer to the IP address, so that they now point to the Firepower 2100 series device IP address.

b. If you are using routing protocols, ensure that neighbors see the Firepower 2100 series device IP address as the next hop for expected destinations.

Step 5 Run a comprehensive test plan and monitor logs within the managing management center for your Firepower 2100 device.



CHAPTER 3

Cisco Success Network-Telemetry Data

Cisco Success Network - Telemetry Data

Cisco Success Network is an always-on usage information and metrics collection feature in the Secure Firewall migration tool, which collects and trasmits usage statistics through a secure cloud connection between the migration tool and the Cisco cloud. These statistics help us provide additional support on unused features and also improve our products. When you initiate a migration process in the Secure Firewall migration tool, the corresponding telemetry data file is generated and stored in a fixed location.

When you push the migrated Fortinet configuration to management center, the push service reads the telemetry data file from the location and deletes it after the data is successfully uploaded to the cloud.

The migration tool provides two options to choose from, for streaming telemetry data—**Limited** and **Extensive**.

With **Cisco Success Network** set to **Limited**, the following telemetry data points are collected:

Table 2: Limited Telemetry

Data Point	Description	Example Value
Time	The time and date when the telemetry data is collected	2023-04-25 10:39:19
Source Type	The source device type	ASA
Device Model Number	Model number of ASA	ASA5585-SSP-10, 5969 MB RAM, CPU Xeon 5500 series 2000 MHz, 1 CPU (4 cores)
Source Version	Version of ASA	9.2 (1)
Target Management Version	The target version of management center	6.5 or later
Target Management Type	The type of target management device, namely, management center	Management Center
Target Device Version	The version of target device	75

Data Point	Description	Example Value
Target Device Model	The model of target device	Cisco Secure Firewall Threat Defense for VMware
Migration Tool Version	The version of the migration tool	1.1.0.1912
Migration Status	The status of the migration of ASA configuration to management center	SUCCESS

The following tables provide information on the telemetry data points, their descriptions, and sample values, when **Cisco Success Network** is set to **Extensive**:

Table 3: Extensive Telemetry

Data Point	Description	Example Value
Operating System	Operating system that runs the Secure Firewall migration tool. It could be Windows7/Windows10 64-bit/macOS High Sierra	Windows 7
Browser	Browser used to launch the Secure Firewall migration tool. It could be Mozilla/5.0 or Chrome/68.0.3440.106 or Safari/537.36	Mozilla/5.0

Table 4: Source Fortinet Information

Data Point	Description	Example Value
Time	The time and date when the telemetry data is collected	2023-04-25 10:39:19
Source Type	The source device type	Fortinet
Source Device Serial Number	Serial number of Fortinet	Serial number of device if exists.
Source Device Model Number	Model number of Fortinet	FGT80E
Source Device Version	Version of Fortinet	6.0.6
Source Config Counts	The total number of lines in the source configuration	504
Firewall Mode	The firewall mode configured on Fortinet - routed or transparent	ROUTED
Context Mode	The context mode of Fortinet. This can be single or multi-context.	SINGLE
Fortinet Config Statistics:		
ACL Counts	The number of ACLs which are attached to access group	46
Access Rules Counts	The total number of access rules	46

Data Point	Description	Example Value
NAT Rule Counts	The total number of NAT rules	17
Network Object Counts	The number of network objects configured in Fortinet	34
Network Object Group Counts	The number of network object groups in Fortinet	6
Port Object Counts	The number of port objects	85
Port Object Group Counts	The number of port object groups	37
Unsupported Access Rules Count	The total number of unsupported access rules	3
Unsupported NAT Rule Count	The total number of unsupported NAT access rules	0
FQDN Based Access Rule Counts	The number of FQDN -based access rules	7
Time range Based Access Rule Counts	The number of time range based access rules	1
SGT Based Access Rule Counts	The number of SGT-based access rules	0
Summary of Config lines that Tool is not able to parse		
Unparsed Config Count	The number of config lines that are unrecognized by the parser	68
Total Unparsed Access Rule Counts	The total number of unparsed access rules	3
More Fortinet config details...		
Is RA VPN Configured	Whether RA VPN is configured on Fortinet	false
Is S2S VPN Configured	Whether Site-to-Site VPN is configured on Fortinet	false
Is BGP Configured	Whether BGP is configured on Fortinet	false
Is OSPF Configured	Whether OSPF is configured on Fortinet	false
Local Users Counts	The number of local users configured	0

Table 5: Target Management Device (Management Center) Information

Data Point	Description	Example Value
Target Management Version	The target version of management center	6.2.3.3 (build 76)
Target Management Type	The type of target management device, namely, management center	Management Center
Target Device Version	The version of target device	75

Data Point	Description	Example Value
Target Device Model	The model of target device	Cisco Secure Firewall Threat Defense for VMware
Migration Tool Version	The version of the migration too1	1.1.0.1912

Table 6: Migration Summary

Data Point	Description	Example Value
Access Control Policy		
Name	The name of access control policy	Doesn't Exist
Access Rule Counts	The total number of migrated ACL rules	0
Partially Migrated ACL Rule Counts	The total number of partially migrated ACL rules	3
Expanded ACP Rule Counts	The number of expanded ACP rules	0
NAT Policy		
Name	The name of NAT policy	Doesn't Exist
NAT Rule Counts	The total number of migrated NAT rules	0
Partially Migrated NAT Rule Counts	The total number of partially migrated NAT rules	0
More migration details...		
Interface Counts	The number of updated interfaces	0
Sub Interface Counts	The number of updated subinterfaces	0
Static Routes Counts	The number of static routes	0
Objects Counts	The number of objects created	34
Object Group Counts	The number of object groups created	6
Security Zone Counts	The number of security zones created	3
Network Object Reused Counts	The number of objects reused	21
Network Object Rename Counts	The number of objects that are renamed	1
Port Object Reused Counts	The number of port objects that are reused	0
Port Object Rename Counts	The number of port objects that are renamed	0

Table 7: Secure Firewall Migration Tool Performance Data

Data Point	Description	Example Value
Conversion Time	The time taken to parse Fortinet configuration lines (in minutes)	14
Migration Time	The total time taken for end-to-end migration (in minutes)	592
Config Push Time	The time taken to push the final configuration (in minutes)	7
Migration Status	The status of the migration of Fortinet configuration to management center	SUCCESS
Error Message	The error message as displayed by the Secure Firewall migration tool	null
Error Description	The description about the stage when the error has occurred and the possible root cause	null

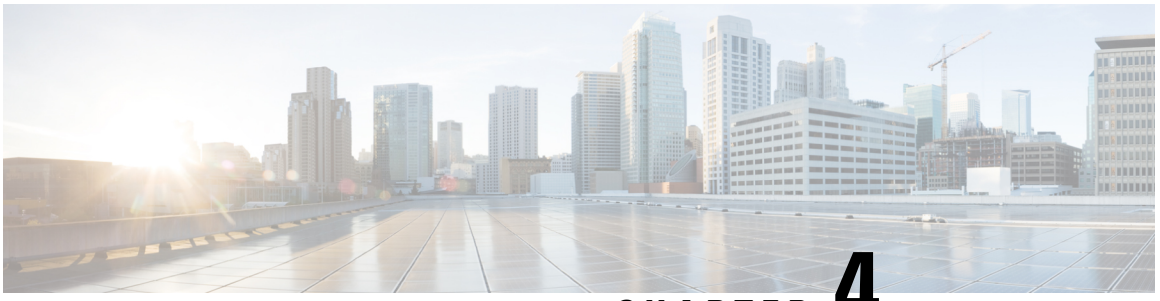
Telemetry Fortinet Example File

The following is an example of a telemetry data file on the migration of Fortinet configuration to threat defense :


```
{
    "metadata": {
        "contentType": "application/json",
        "topic": "migrationtool.telemetry"
    },
    "payload": {
        "fortinet_config_stats": {
            "Ipv6_access_rule_counts": 3,
            "Ipv6_bgp_count": 0,
            "Ipv6_nat_rule_count": 3,
            "Ipv6_network_counts": 3,
            "Ipv6_static_route_counts": 6,
            "access_rules_counts": 62,
            "acl_counts": 62,
            "fqdn_based_access_rule_counts": 2,
            "nat_rule_counts": 27,
            "network_object_counts": 59,
            "network_object_group_counts": 11,
            "no_of_fqdn_based_objects": 9,
            "port_object_counts": 166,
            "port_object_group_counts": 37,
            "timerange_based_access_rule_counts": 0,
            "total_unparsed_access_rule_counts": 0,
            "tunneling_protocol_based_access_rule_counts": 0,
            "unparsed_config_count": 0,
            "unsupported_access_rules_count": 0,
            "unsupported_nat_rule_count": 0
        },
        "context_mode": "SINGLE",
        "error_description": null,
        "error_message": null,
        "firewall_mode": "ROUTED",
        "log_info_acl_count": 0,
        "migration_status": "SUCCESS",
        "migration_summary": {
            "access_control_policy": [
                [
```

```
                {
                    "access_rule_counts": 62,
                    "apply_file_policy_rule_counts": 0,
                    "apply_ips_policy_rule_counts": 0,
                    "apply_log_rule_counts": 0,
                    "do_not_migrate_rule_counts": 0,
                    "enable_hit_count": false,
                    "expanded_acp_rule_counts": 1,
                    "name": "FTD-Mig-ACP-1602513965",
                    "partially_migrated_acl_rule_counts": 0,
                    "time_based_acl_count": 0,
                    "total_acl_element_counts": 69,
                    "update_rule_action_counts": 0
                }
            ]
        ],
        "interface_counts": 20,
        "interface_group_counts": 0,
        "interface_group_manually_created_counts": 0,
        "ip_sla_monitor_count": 0,
        "nat_Policy": [
            [
                {
                    "NAT_rule_counts": 27,
                    "do_not_migrate_rule_counts": 0,
                    "name": "FTD-Mig-1602513959",
                    "partially_migrated_nat_rule_counts": 0
                }
            ]
        ],
        "network_object_rename_counts": 0,
        "network_object_reused_counts": 37,
        "object_group_counts": 2,
        "objects_counts": 35,
        "port_object_rename_counts": 0,
        "port_object_reused_counts": 10,
        "prefilter_control_policy": [
            [
                {
                    "do_not_migrate_rule_counts": 0,
                    "name": null,
                    "partially_migrated_acl_rule_counts": 0,
                    "prefilter_rule_counts": 0
                }
            ]
        ],
        "security_zone_counts": 19,
        "security_zone_manually_created_counts": 0,
        "static_routes_counts": 9,
        "sub_interface_counts": 20,
        "time_out": false
    },
    "migration_tool_version": "2.3",
    "mtu_info": {
        "interface_name": null,
        "mtu_value": null
    },
    "rule_change_acl_count": 0,
    "selective_policy": {
        "acl": true,
        "acl_policy": true,
        "application": false,
        "csm": true,
        "interface": true,
```

```
                "interface_groups": true,
                "migrate_tunneled_routes": false,
                "nat": true,
                "network_object": true,
                "policy_assignment": true,
                "populate_sz": false,
                "port_object": true,
                "routes": true,
                "security_zones": true,
                "unreferenced": true
            },
            "source_config_counts": 0,
            "source_device_model_number": "FGT80E",
            "source_device_serial_number": null,
            "source_device_version": "6.0.6",
            "source_type": "FORTINET",
            "system_information": {
                "browser": "Chrome/85.0.4183.121",
                "operating_system": "Windows NT 10.0; Win64; x64"
            },
            "target_device_model": "Cisco Firepower 9000 Series SM-24 Threat Defense",
            "target_device_version": "76",
            "target_management_type": "6.6.0 (build 56)",
            "target_management_version": "6.6.0 (build 56)",
            "template_version": "1.1",
            "time": "2020-10-12 20:16:15",
            "tool_analytics_data": {
                "objectsplit_100_count": 0
            },
            "tool_performance": {
                "config_push_time": 533,
                "conversion_time": 3,
                "migration_time": 1108
            }
        },
        "version": "1.0"
}
```



CHAPTER 4

Troubleshooting Migration Issues

Troubleshooting for the Secure Firewall Migration Tool

A migration typically fails during the Fortinet configuration file upload or during the push of the migrated configuration to management center.

Some of the common scenarios where the migration process fails are:

- Unknown or invalid characters in the Fortinet configuration file
- Incomplete or missing elements in the Fortinet configuration file
- Loss of network connectivity or latency

Secure Firewall Migration Tool Support Bundle

The Secure Firewall migration tool provides the option to download a support bundle to extract valuable troubleshooting information like log files, DB, and configuration files. Perform the following:

1. On the **Complete Migration** screen, click the **Support** button.

   The Help support page appears.

2. Check the **Support Bundle** check box and then select the configuration files to download.

Note The Log and dB files are selected for download by default.

3. Click **Download**.

   The support bundle file is downloaded as a .zip to your local path. Extract the Zip folder to view the log files, DB, and the Configuration files.

4. Click **Email us** to email the failure details for the technical team.

   You can also attach the downloaded support files to your email.

5. Click **Visit TAC page** to create a TAC case in the Cisco support page.

Note You can open a TAC case at any time during the migration from the support page.

Logs and Other Files Used for Troubleshooting

You can find information that is useful for identifying and troubleshooting issues in the following files.

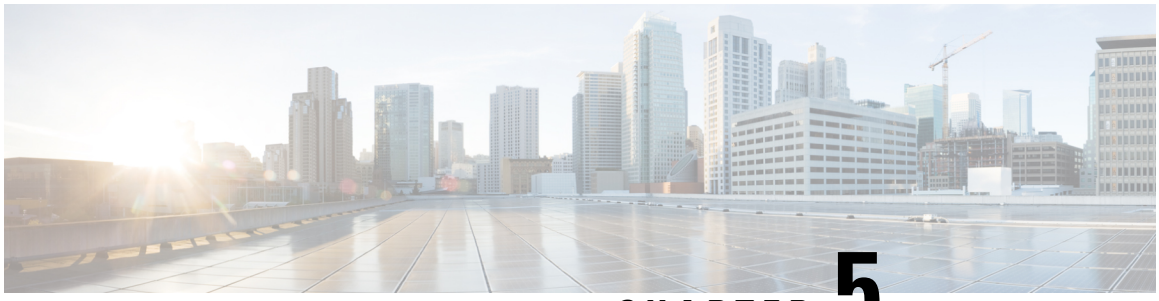
File	Location
Log file	*<migration_tool_folder>*\logs
Pre-migration report	*<migration_tool_folder>*\resources
Post-migration report	*<migration_tool_folder>*\resources
unparsed file	*<migration_tool_folder>*\resources

Troubleshooting Fortinet File Upload Failures

If your Fortinet configuration file fails to upload, the reason is that the Secure Firewall migration tool could not parse one or more lines in the file.

You can find information about the errors that caused the upload and parsing failure in the following locations:

- Error message displayed by the Secure Firewall migration tool—Provides a high-level summary of what caused the failure.
- Pre-Migration Report—Review the Configuration Lines with Errors section to see which lines in the Fortinet configuration file caused the failure.
- Log file—Search on the word "error" to view the reason for the failure.
- Unparsed file—Look at the end of the file to identify the last ignored line of the Fortinet configuration file that was successfully parsed.



CHAPTER 5

Secure Firewall Migration Tool FAQs

Secure Firewall Migration Tool Frequently Asked Questions

Q. What are the new features supported on the Secure Firewall migration tool for Release 3.0.1?

A. The Secure Firewall migration tool 3.0.1 now provides support for Secure Firewall 3100 series only as a destination device for migrations from Fortinet.

Q. What are the new features supported on the Secure Firewall migration tool for Release 3.0?

A. The following features are supported with release 3.0:

- Migration to Cloud-delivered Firewall Management Center.

Q. What are the new features supported on the Secure Firewall migration tool for Release 2.5.2?

A. ACL Optimization for Fortinet.

Q. What are the source and target platforms for Secure Firewall migration tool 2.3 to migrate policies?

A. The Secure Firewall migration tool can now migrate policies from the supported Fortinet firewall platform to the threat defense platform. For more information, see Supported Platforms for Migration.

Q. What are the new features supported on the Secure Firewall migration tool 2.3?

A. The Secure Firewall migration tool 2.3 can migrate policies from the supported Fortinet platform to the threat defense platform.

Q. What are the supported source devices and code version?

A. You can use the Secure Firewall migration tool to migrate the configuration from Single or Multi VDOM Fortinet firewall running FortiOS 5.0 and later. For more information on the list of devices, see Supported Platforms for Migration.

Q. Does Fortinet firewall support interface groups?

A. No. Fortinet firewall does not support interface groups for conversion to the threat defense.

Q. What are the features the Secure Firewall migration tool supports for migration?

A. The Secure Firewall migration tool supports migration of L3/L4 Fortinet configuration to the threat defense and can migrate the following Fortinet configurations:

- Network objects and groups (except for a few of the unsupported object types)

- Service objects, except for those service objects configured for a source and destination
- 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
- NAT rules
- NAT using VIP and IP pool (Central NAT is not supported)
- Static routes and ECMP routes which are not migrated
- Physical interfaces
- Subinterfaces
- Port channels
- Zones
- Time-based objects

Q. NAT uses FQDN, which is not supported by the management center. What should I do?
A. Use of FQDN-address-object in NAT fields is not supported on Secure Firewall migration tool and management center. To replicate the same configuration as the source, you must manually, configure, post-migration, the whole set of IP addresses that are mapped with FQDN.

Q. What should I do when the source firewall has more interfaces than the target?
A. If the source firewall has more interfaces than the target, create subinterfaces on the threat defense before initiating the migration.

Q. Will the Secure Firewall migration tool migrate aggregate interfaces (port channels)?
A. The Secure Firewall migration tool does not migrate aggregate interfaces (port channels). You must configure the port channel interface on the management center before initiating the migration.

Q. What should I do with the Ignored Configuration files?
A. The Ignored configuration files contain lines that are specific to Fortinet only and are irrelevant to the management center. Hence, they are ignored. You must review the ignored configuration carefully. Any

irrelevant details that reflect in the ignored section should be configured manually on the management center.

Q. I get error in the Pre-Migration Report. Can I ignore the interfaces and continue?
A. If you choose to proceed without interfaces, then the routes will also not get migrated.

Q. What are the common causes for Parse Failure?
A. Parse failure occurs if the interfaces have multiple IP addresses or IP addresses assigned with subnets, for example /32 or /128. To proceed, you must correct the IP address and retry the migration.

Q. How can I export a Fortinet configuration?
A. You can export the Fortinet configuration by extracting it from the Fortigate device or from the FortiManager if the device is managed by FortiManager. For more information, see Export the Configuration from Fortinet Firewall.

Q. Is there any dependency on the management center to use the new features introduced in the Secure Firewall migration tool?
A. Yes. The Time-based Objects feature is supported with the target management center 6.6 and later.