

Migrating Microsoft Azure Native Firewall to Cisco Secure Firewall Threat Defense with the Cisco Secure Firewall Migration Tool

First Published: 2025-06-18

Last Modified: 2026-07-10

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025– Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Getting Started with the Secure Firewall Migration Tool** 1

About the Secure Firewall Migration Tool 1

What's New in the Secure Firewall Migration Tool 3

Licensing for the Secure Firewall Migration Tool 15

Platform Requirements for the Secure Firewall Migration Tool 16

Requirements and Prerequisites for Threat Defense Devices 16

Guidelines and Limitations 16

Supported Target Management Center for Migration 18

Supported Software Versions for Migration 19

CHAPTER 2 **Microsoft Azure Native Firewall to Threat Defense Migration Workflow** 21

End-to-End Procedure 21

Prerequisites for Migration 22

Download the Secure Firewall Migration Tool from Cisco.com 23

Export the Configuration from Microsoft Azure Native Firewall 23

Export Policy Configuration from Azure Firewall GUI 23

Export IP Group Configuration 24

Run the Migration 24

Launch the Secure Firewall Migration Tool 24

Using the Demo Mode in the Secure Firewall Migration Tool 26

Upload the Microsoft Azure Configuration File 27

Specify Destination Parameters for the Secure Firewall Migration Tool 28

Review the Pre-Migration Report 30

Optimize, Review and Validate the Configuration 31

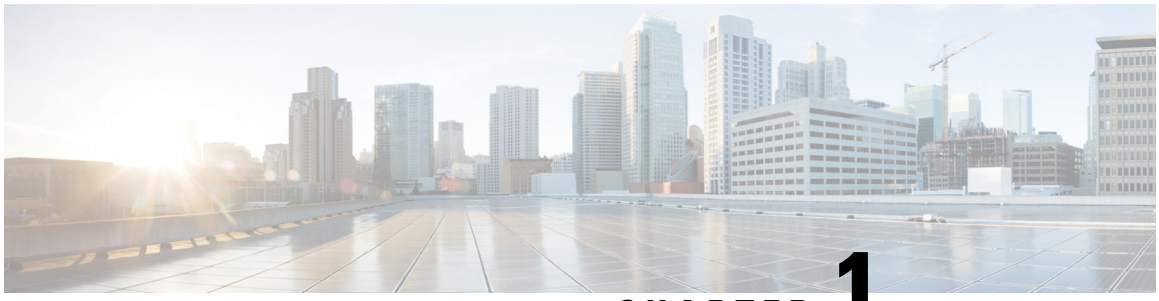
Push the Migrated Configuration to Firewall Management Center 35

Review the Post-Migration Report and Complete the Migration 36

Parse Summary 38
Migration Failures 38
Uninstall the Secure Firewall Migration Tool 39
Sample Migration: Azure to Threat Defense 2100 39
Pre-Maintenance Window Tasks 39
Maintenance Window Tasks 40

CHAPTER 3 Cisco Success Network-Telemetry Data 41
Cisco Success Network - Telemetry Data 41

CHAPTER 4 Troubleshooting Migration Issues 43
Troubleshooting for the Secure Firewall Migration Tool 43
Logs and Other Files Used for Troubleshooting 44



CHAPTER 1

Getting Started with the Secure Firewall Migration Tool

- About the Secure Firewall Migration Tool, on page 1
- What's New in the Secure Firewall Migration Tool, on page 3
- Licensing for the Secure Firewall Migration Tool, on page 15
- Platform Requirements for the Secure Firewall Migration Tool, on page 16
- Requirements and Prerequisites for Threat Defense Devices, on page 16
- Guidelines and Limitations, on page 16
- Supported Target Management Center for Migration, on page 18
- Supported Software Versions for Migration, on page 19

About the Secure Firewall Migration Tool

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

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

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

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

- A summary of the supported Microsoft Azure configuration elements that can be successfully migrated.
- Azure configuration lines with errors
- Azure configuration items that are ignored for migration

Note If there are parsing errors, you can rectify the issues, reupload a new configuration, connect to the destination device, and proceed to review and validate your configuration. You can then migrate the configuration to the destination device.

Console

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

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

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

Logs

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

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

Resources

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

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

Unparsed File

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

You can find the unparsed file in the following location:

<migration_tool_folder>\resources

Search in the Secure Firewall Migration Tool

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

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

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

Ports

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

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

Notifications Center

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

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

Cisco Success Network

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

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

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

What's New in the Secure Firewall Migration Tool

Version	Supported Features
10.0.2	This patch release contains bug fixes.

Version	Supported Features
10.0.1	You can now migrate DHCP and DNS configurations using the Secure Firewall Migration Tool. Supported migration: Check Point Firewall to Firewall Threat Defense
	This release introduces comprehensive migration support for Secure Firewall 6100 series devices.
	The migration tool now features an enhanced Application Mapping screen. This improvement simplifies the migration of application configurations to Firewall Threat Defense. Supported migration: Check Point Firewall to Firewall Threat Defense
	Added support for migrating firewall configuration from Check Point Small and Medium Business (SMB) devices to Cisco Secure Firewall Threat Defense.
	The Firewall Migration Tool does not display attribute counts on the **Parsed Summary** page during the pre-parsing phase. This change improves clarity and streamlines the migration process. Supported migration: All
	You can now migrate configurations from Cisco Adaptive Security Appliance (ASA) 55XX-X Series devices running Firewall Threat Defense to Firewall Threat Defense devices, such as Cisco Firewall 1000, 2000, 3000, 4000, 6000, and 9000 Series devices.
10.0	This release introduces comprehensive migration support for CSF200 series devices. Supported migration: All
	Migration support for Firewall Management Center and Firewall Threat Defense 10.0 designed to facilitate smooth transitions to this release. Supported migration: All
	This release introduces significant enhancements to telemetry capabilities, improving data collection for analysis and troubleshooting. Supported migration: All
	This release delivers significant enhancements to parsing performance, making the system more responsive and efficient. Supported migration: Check Point Firewall to Firewall Threat Defense, Palo Alto Networks Firewall to Firewall Threat Defense and ASA Firewall to Firewall Threat Defense.
	The Dual Network Address Translation (NAT) feature is enhanced to improve the user experience. See: Check Point Configuration Support Supported migration: Check Point Firewall to Firewall Threat Defense

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

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

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

Version	Supported Features
7.0.1	

Version	Supported Features
	This release includes the following new features and enhancements: • You can now migrate configurations from your Cisco firewalls such as ASA and FDM-managed devices and third-party firewalls to Cisco Secure Firewall 1200 Series devices. See: Cisco Secure Firewall 1200 Series • You can now update the preshared keys for more than one site-to-site VPN tunnel configuration at once. Export the site-to-site VPN table in the **Optimize, Review and Validate Configuration** page to an Excel sheet, specify the preshared keys in the respective cells, and upload the sheet back. The migration tool reads the preshared keys from the Excel and updates the table. See: Optimize, Review, and Validate the Configuration Supported migrations: All • You can now choose to ignore migration-hindering, incorrect configurations and still continue the final push of a migration. Previously, the whole migration failed even if a single object's push failed because of errors. You also now have the control to abort the migration manually to fix the error and retry migration. See: Push the Migrated Configuration to Management Center Supported migrations: All • The Secure Firewall migration tool now detects existing site-to-site VPN configurations in the target threat defense device and prompts you to choose if you want them deleted, without having to log in to the management center. You could choose **No** and manually delete them from the management center to continue with the migration. See: Optimize, Review, and Validate the Configuration Supported migrations: All • If you have an existing hub and spoke topology configured on one of the threat defense devices managed by the target management center, you could choose to add your target threat defense device as one of the spokes to the existing topology right from the migration tool, without having to manually do it on the management center. See: Optimize, Review, and Validate the Configuration Supported migrations: Secure Firewall ASA • When migrating thrid-party firewalls, you can now select threat defense devices as target, which are part of a high availability pair. Previously, you could only choose standalone threat defense devices as target devices. Supported migrations: Palo Alto Networks, Check Point, and Fortinet firewall migrations • The Secure Firewall migration tool now provides a more enhanced, intuitive demo mode, with guided migration instructions at every step. In addition, you

Version	Supported Features
	can also see versions of target threat defense devices to choose and test based on your requirements. Supported migrations: All
7.0	This release includes the following new features and enhancements: **Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense Migration** • You can now configure a threat defense high availability (HA) pair on the target management center and migrate configurations from a Secure Firewall ASA HA pair to the management center. Choose **Proceed with HA Pair Configuration** on the **Select Target** page and choose an active and a standby device. When selecting the active threat defense device, ensure you have an identical device on the management center for the HA pair configuration to be successful. See Specify Destination Parameters for the Secure Firewall Migration Tool in the *Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool* book for more information. • You can now configure a site-to-site hub and spoke VPN topology using threat defense devices when migrating site-to-site VPN configurations from an ASA device. Click **Add Hub & Spoke Topology** under **Site-to-Site VPN Tunnels** on the **Optimize, Review and Validate Configuration** page. See Optimize, Review, and Validate the Configuration in the *Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool* book for more information. **Fortinet Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate IPv6 and multiple interface and interface zones in SSL VPN and central SNAT configurations from a Fortinet firewall to your threat defense device. See Fortinet Configuration Support in *Migrating Fortinet Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool* book for more information.

Version	Supported Features
6.0.1	This release includes the following new features and enhancements: **Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense Migration** • You can now optimize network and port objects when you migrate configurations from Secure Firewall ASA to threat defense. Review these objects in their respective tabs in the **Optimize, Review and Validate Configuration** page and click **Optimize Objects and Groups** to optimize your list of objects before migrating them to the target management center. The migration tool identifies objects and groups that have the same value and prompts you to choose which to retain. See Optimize, Review, and Validate the Configuration for more information. **FDM-managed Device to Cisco Secure Firewall Threat Defense Migration** • You can now migrate DHCP, DDNS, and SNMPv3 configurations from your FDM-managed device to a threat defense device. Ensure you check the **DHCP** checkbox and **Server**, **Relay**, and **DDNS** checkboxes on the **Select Features** page. See Optimize, Review, and Validate the Configuration for more information. **Fortinet Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate URL objects in addition to other object types from a Fortinet firewall to your threat defense device. Review the **URL Objects** tab in the **Objects** window in **Optimize, Review and Validate Configuration** page during migration. See Optimize, Review, and Validate the Configuration for more information. **Palo Alto Networks Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate URL objects in addition to other object types from a Palo Alto Networks firewall to your threat defense device. Ensure you review the **URL Objects** tab in the **Objects** window in **Optimize, Review and Validate Configuration** page during migration. See Optimize, Review, and Validate the Configuration for more information. **Check Point Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate port objects, FQDN objects, and object groups from a Check Point Firewall to your threat defense device. Review the **Objects** window in **Optimize, Review and Validate Configuration** page during migration. See Optimize, Review, and Validate the Configuration for more information.

Version	Supported Features
6.0	

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

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

Version	Supported Features
5.0	• Secure Firewall migration tool now supports migration of multiple security contexts from Secure Firewall ASA to threat defense devices. You can choose to migrate configurations from one of your contexts or merge the configurations from all your routed firewall mode contexts and migrate them. Support for merging configurations from multiple transparent firewall mode contexts will be available soon. See Select the ASA Primary Security Context for more information. • The migration tool now leverages the virtual routing and forwarding (VRF) funtionality to replicate the segregated traffic flow observed in a multi-context ASA environment, which will be part of the new merged configuration. You can check the number of contexts the migration tool has detected in a new **Contexts** tile and the same after parsing, in a new **VRF** tile in the **Parsed Summary** page. In addition, the migration tool displays the interfaces to which these VRFs are mapped, in the **Map Interfaces to Security Zones and Interface Groups** page. • You can now try the whole migration workflow using the new demo mode in Secure Firewall migration tool and visualize how your actual migration looks like. See Using the Demo Mode in Firewall Migration Tool for more information. • With new enhancements and bug fixes in place, Secure Firewall migration tool now provides an improved, faster migration experience for migrating Palo Alto Networks firewall to threat defense.
4.0.3	The Secure Firewall migration tool 4.0.3 includes bug fixes and the following new enhancements: • The migration tool now offers an enhanced **Application Mapping** screen for migrating PAN configurations to threat defense. See Map Configurations with Applications in *Migrating Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Migration Tool* guide for more information.
4.0.2	The Secure Firewall migration tool 4.0.2 includes the following new features and enhancements: • The migration tool now has an always-on telemetry; however, you can now choose to send limited or extensive telemetry data. Limited telemetry data inludes few data points, whereas extensive telemetry data sends a more detailed list of telemetry data. You can change this setting from **Settings** > **Send Telemetry Data to Cisco?**.

Licensing for the Secure Firewall Migration Tool

The Secure Firewall migration tool application is free and does not require license.

Platform Requirements for the Secure Firewall Migration Tool

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

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

Requirements and Prerequisites for Threat Defense Devices

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

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

- The target threat defense device must be registered with the management center.
- The target threat defense device can be in a high availability configuration.
- The threat defense device can be a standalone device or a container instance. It must **not** be part of a cluster.
    - If the target threat defense device is a container instance, at minimum it must have an equal number of used physical interfaces, physical subinterfaces, port channel interfaces, and port channel subinterfaces (excluding 'management-only') as that of the Azure; if not you must add the required type of interface on the target threat defense device.

Note

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

Guidelines and Limitations

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

The Secure Firewall Migration Tool does not migrate unsupported objects, NAT rules, and routes.

Azure Configuration Limitations

Migration of the source Azure configuration has the following limitations:

- You must manually migrate the interface and route configuration to Firewall Threat Defense

Azure Migration Guidelines

The source configuration file should be in zip format and contain these files:

- template.json file exported from Azure portal
- IPGroup.txt file comprising of IP Group data exported using PowerShell

Supported Azure Configurations

The Secure Firewall Migration Tool can fully migrate the following:

- Access Control Lists
- Network objects
- Service objects
- Network object groups
- Destination NAT (D-NAT)
- FQDN
- IP groups
- URLs



Note To migrate the above configurations in Firewall Threat Defense; the Firewall Management Center and version must be 6.6 or later. For Service Object configuration migration, the version must be 6.4 or later.

Guidelines and Limitations for Threat Defense Devices

When you migrate your Azure configuration to Firewall Threat Defense, if there are device-specific configurations in the devices, such as routes, interfaces, and so on, during push migration, the Secure Firewall Migration Tool cleans the device automatically and overwrites from the Azure configuration.



Note To prevent loss of device (target) configuration data, we recommend that you manually clean the device before 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 19.
- The cloud-delivered or on-prem Firewall Management Center software version that is supported for Azure migration is 6.6 and later.
- You have obtained and installed smart licenses for Firewall Threat Defense that include all features that you plan to migrate from the Azure interface, as described in the following:
  - The Getting Started section of Cisco Smart Accounts on Cisco.com.
  - Register the Firewall Management Center with the Cisco Smart Software Manager.
  - Licensing the Firewall System
  - You have enabled Firewall Management Center for REST API.

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



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

Cloud-Delivered Firewall Management Center

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

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

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

Security Cloud Control Regions

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

Table 1: Security Cloud Control Regions and URL

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

Supported Software Versions for Migration

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

Supported Secure Firewall Migration Tool Versions

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

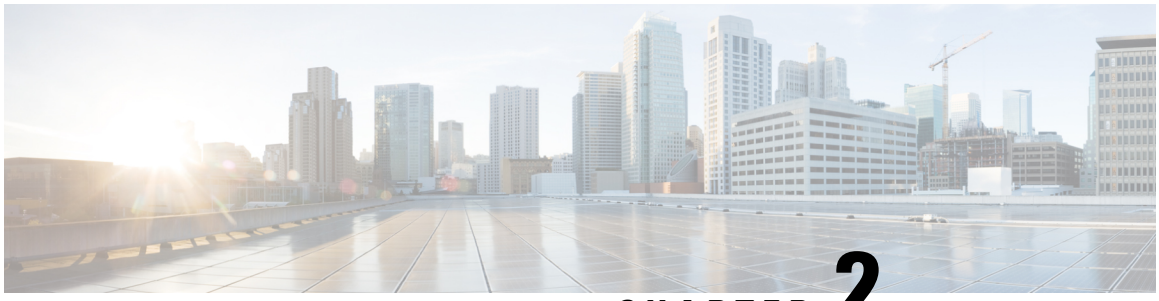
Supported Management Center Versions for source Microsoft Azure Firewall Configuration

For Azure firewall, the Secure Firewall Migration Tool supports migration to a Management Center device managed by a Management Center that is running Version 6.6 or later.

Supported Firewall Threat Defense Versions

The Secure Firewall Migration Tool recommends migration to a device that is running Version 6.6 or later and Version 7.0 or later for virtual..

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



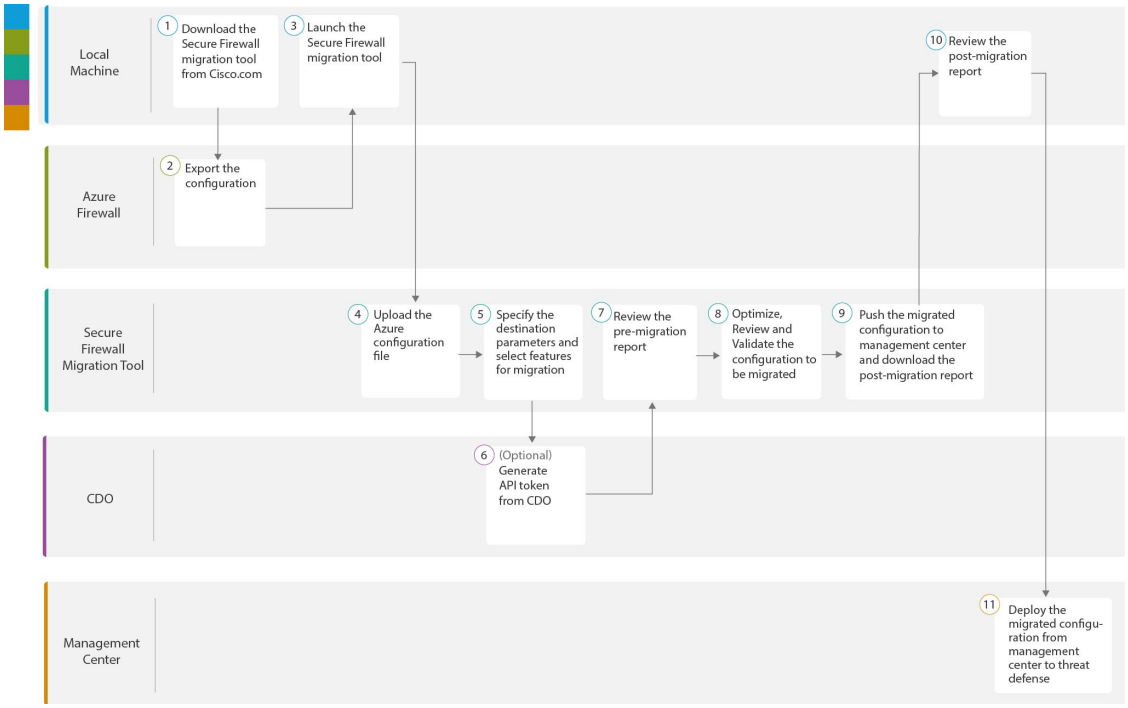
CHAPTER 2

Microsoft Azure Native Firewall to Threat Defense Migration Workflow

- End-to-End Procedure, on page 21
- Prerequisites for Migration, on page 22
- Run the Migration, on page 24
- Uninstall the Secure Firewall Migration Tool, on page 39
- Sample Migration: Azure to Threat Defense 2100 , on page 39

End-to-End Procedure

The following flowchart illustrates the workflow for migrating a Microsoft Azure Native firewall to threat defense using the Secure Firewall Migration Tool.



	Workspace	Steps
1	Local Machine	Download the latest version of Secure Firewall Migration Tool from Cisco.com. For detailed steps, see Download the Secure Firewall Migration Tool from Cisco.com.
2	Azure Firewall	Export the configuration file: For details about exporting the configuration from Azure firewall, see Export the Configuration from Microsoft Azure Native Firewall, on page 23.
3	Local Machine	Launch the Secure Firewall Migration Tool in your local machine. For details, see Launch the Secure Firewall Migration Tool.
4	Secure Firewall Migration Tool	Upload the Azure configuration file exported from Azure firewall. For details, see Upload the Microsoft Azure Configuration File, on page 27.
5	Secure Firewall Migration Tool	Specify the destination parameters for the migration. For detailed steps, see Specify Destination Parameters for the Secure Firewall Migration Tool.
6	Security Cloud Control	(Optional) This step is required if you have selected Cloud-Delivered Firewall Management Center as the destination Management Center. For detailed steps, see Specify Destination Parameters for the Secure Firewall Migration Tool, step 1.
7	Secure Firewall Migration Tool	Navigate to where you downloaded the premigration report and review the report. For detailed steps, see Review the Pre-Migration Report.
8	Secure Firewall Migration Tool	Optimize and review the configuration carefully and validate that it is correct and matches how you want to configure the device. For detailed steps, see Optimize, Review and Validate the Configuration to be Migrated.
9	Secure Firewall Migration Tool	Sends the migrated configuration to Management Center and download the postmigration report. For detailed steps, see Push the Migrated Configuration to Management Center.
10	Local Machine	Navigate to where you downloaded the postmigration report and review the report. For detailed steps, see Review the Post-Migration Report and Complete the Migration.
11	Management Center	Deploy the migrated configuration from the Management Center to the . For detailed steps, see Review the Post-Migration Report and Complete the Migration.

Prerequisites for Migration

Before you migrate your Microsoft Azure configuration, perform 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.

If you want to use the cloud version of the Secure Firewall migration tool hosted on Security Cloud Control, skip to step 4.

Procedure

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 Firewall Threat Defense device download areas.

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

Ensure that you download the appropriate executable of the Secure Firewall migration tool for Windows or macOS machines.

Step 4 If you are a Security Cloud Control user and want to use the migration tool hosted on it, log in to your Security Cloud Control tenant and on the left pane, navigate to **Administration** > **Migration** > **Firewall Migration Tool** to create your migration instance.

Export the Configuration from Microsoft Azure Native Firewall

Perform these tasks to export the Microsoft Azure configuration:

- Export Policy Configuration from Azure Firewall GUI, on page 23
- Export IP Group Configuration, on page 24

Export Policy Configuration from Azure Firewall GUI

Perform this procedure to export policy configuration from the Microsoft Azure firewall GUI.

Procedure

Step 1 From the Microsoft Azure firewall GUI, choose **Policy**.

Step 2 Select **Export Template** in the **Automation** section.

Step 3 Click the download button to download the configuration.

The policy configuration is downloaded in zipped format. Extract the template.json file.

What to do next

Export IP Group Configuration, on page 24

Export IP Group Configuration

Perform this procedure to extract the IP address group configuration from Microsoft Azure PowerShell.

Procedure

Step 1 Open PowerShell and run this command:

```
Get-AzIpGroup -ResourceGroupName "your_ResourceGrp_name"| Select Name,IPAddresses
```

Note
Replace `your_ResourceGrp_name` with resource group name.

Step 2 Copy the output in text file and save it as IPGroup.txt.

What to do next

Upload the Microsoft Azure Configuration File, on page 27

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 Security Cloud Control, skip to Upload the Microsoft Azure Configuration File, on page 27 .

Note When you launch the desktop version of 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
- 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.

Procedure

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.

  Note
  Ensure you disable any popup blockers in your browser because they might hinder login popus from appearing.

  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 premigration 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, verify the version on Cisco.com.

Step 11 Click **Proceed**.

What to do next

You can proceed to the following step:

- If you have exported FDM-managed device configuration to your computer, proceed to Upload the Microsoft Azure Configuration File, on page 27.

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, 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 Microsoft Azure Configuration File

Perform this procedure to upload the Microsoft Azure configuration file to the Firewall Migration Tool.

Before you begin

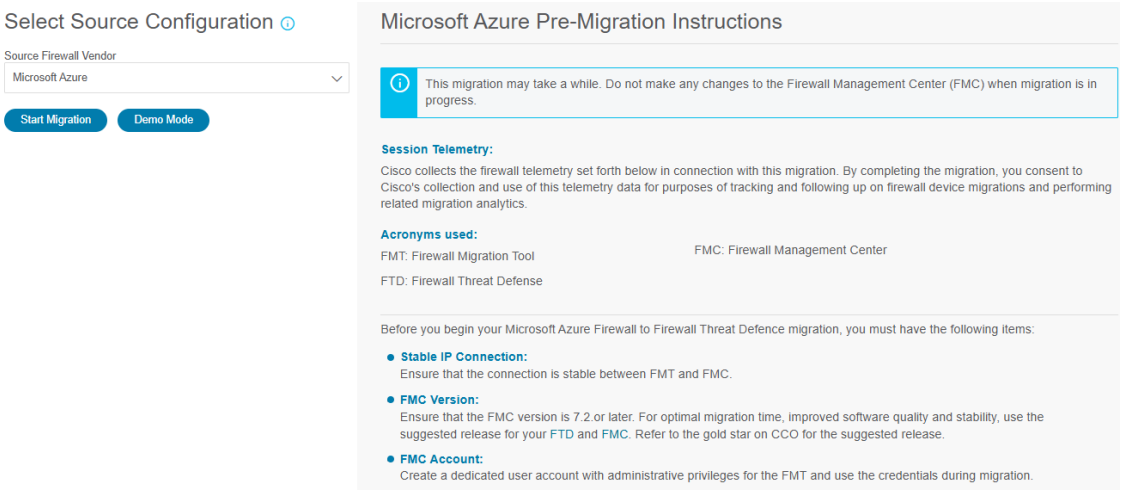
- Export the policy and IP group configuration file from the source Azure device. For more information, see Export the Configuration from Microsoft Azure Native Firewall, on page 23.
- Create a zip file that includes the IPGroup.txt and template.json files, which were extracted.

Note If IPGroup is not configured in the Azure environment, use only the template.json file for migration.

Procedure

Step 1 Launch the Secure Firewall Migration Tool.

Step 2 In the **Select Source Configuration** window, from the **Select Source** drop-down list, choose **Microsoft Azure** and click **Start Migration**.



Step 3 In the **Extract Config Information** window, click **Upload** and select the zip file from your local machine.

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.

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 Security Cloud Control, skip to Step 3.

- Obtain the IP address for the Firewall 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) to the Firewall Management Center. See Adding Devices to the Firewall Management Center

Procedure

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) 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 Security Cloud Control API token. For generating the API token. from Security Cloud Control, follow the below steps:
   1. Log in to Security Cloud Control.
   2. From the top-right corner, navigate to **Preferences** > **General Preferences** and copy the API Token from **My Tokens** section.
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 Firewall Management Center and retrieves a list of Firewall Threat Defense devices that are managed by that Firewall Management Center. You can view the progress of this step in the console.

Step 3 On the **Select Target** screen, in the **Choose Threat Defense** section, you can either select a Firewall Threat Defense device that you want to migrate to, or if you do not have a Firewall Threat Defense device, you can migrate the shared policies (Access Control Lists, NAT, and Objects) of the Azure configuration to the Firewall Management Center.

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

- Click the **Select FTD Device** drop-down list and check the device where you want to migrate the Azure configuration.

  Note
  This list includes both standalone threat defense devices and devices that are part of a high availability (HA) pair on the target Firewall Management Center.

  The devices in the selected Firewall Management Center domain are listed by **IP Address**, **Name**, **Device Model**, and **Mode** (routed or transparent).

- Click **Proceed without FTD** to migrate the configuration to the Firewall Management Center.

  When you proceed without Firewall Threat Defense, the Secure Firewall migration tool will not push any configurations or the policies to Firewall Threat Defense. Thus, interfaces and routes, and site-to-site VPN which are Firewall Threat Defense device-specific configurations will not be migrated and need to be manually configured on Firewall 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 Firewall Threat Defense device, the Secure Firewall migration tool automatically selects the features available for migration from the Azure 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 Firewall Management Center, the Secure Firewall migration tool automatically selects the features available for migration from theAzure configuration in the **Device Configuration**, **Shared**

Configuration, and **Optimization** sections. You can further modify the default selection, according to your requirements.

Note
The **Device Configuration** section is not applicable for Azure migration. The migration of Interface and Routes must be done manually.

- (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 Azure 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.

What to do next

Review the Pre-Migration Report, on page 30

Review the Pre-Migration Report

Note Review all contents of the Pre-Migration Report carefully. The Unsupported rules are not migrated completely, which might alter the original configuration, restrict traffic, or permit unwanted traffic. We recommend that you update the related rules and policies in Firewall Management Center to handle the traffic appropriately after the configuration is successfully migrated.

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.

Procedure

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

Note
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 issues, if any, that may cause the migration to fail.

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

- A summary of the supported Azure configuration elements that can be successfully migrated to Firewall Threat Defense and specific Azure features selected for migration.
- **Configuration Lines with Errors**—Details of Azure configuration elements that cannot be successfully migrated because the Secure Firewall Migration Tool could not parse them. Correct these errors in the Azure configuration, export a new configuration file, and then upload the new configuration file to the Secure Firewall Migration Tool before proceeding.
- **Ignored Configuration**—Details of Azure configuration elements that are ignored because they are not supported by the Firewall 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 Firewall Management Center, and if not supported, plan to configure the features manually.

For more information about the supported features in Firewall Management Center and Firewall Threat Defense, see the Cisco Secure Firewall Management Center Device Configuration Guide.

Step 3 (Optional) If the **Pre-Migration Report** recommends corrective actions, complete the corrections in the Azure interface, export the configuration file again, and upload the updated configuration file before proceeding.

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

Optimize, Review and Validate the Configuration

Before you push the migrated Azure configuration to Firewall Management Center, optimize and review the configuration carefully and validate that it is correct and matches how you want to configure the Firewall Threat Defense device. A flashing tab indicates that you must take the next course of action.

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.

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.
- Disable ACL—The ACL that has been explicitly turned off in the firewall's configuration. The rules exist in the configuration file, but the Secure Firewall Migration Tool ignores them when processing traffic.

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



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

- 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

Select the ACL and click download icon at the top-right of the **Optimize, Review and Validate Configuration** window to review the ACL name and the corresponding redundant, shadowed and disabled ACLs tabulated in an Excel file.

Object Optimization

The following objects are considered for object optimization during the migration process:

- Network Object
- Port Object
- URL Object

Procedure

Step 1 (Optional) On the **Optimize, Review and Validate Configuration** screen, click **Optimize ACL** in **Access Control** > **ACP** to run the optimization code, and perform the following:

a) Select rules and choose **Actions** > **Migrate as disabled** or **Do not migrate** and apply one of the actions.

Note
You can choose **Actions** > **Edit** to edit any rule.

b) Click **Save**.
The migration operation changes from **Do not migrate** to **disabled** or vice-versa.

You can perform bulk selection of rules, using the following options

- Migrate—To migrate with default state.
- Do not Migrate—To ignore the migration of ACLs.
- Migrate as disabled—To migrate ACLs with ***State*** field set to ***Disable***.
- Migrate as enabled—To migrate ACLs will with ***State*** field set to ***Enable***.

Step 2 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.
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) To edit an access control list policy, check the check box adjacent to the corresponding policy, and choose **Actions** > **Edit**.
d) In the **Edit Rule** dialog box, update the existing data or add new data.

To add an object to source or destination:

1. Check the check box adjacent to the object in the left pane.
2. Click the **Add Source** or **Add Destination** button under the **Selected Sources** or **Selected Destination and Applications** column to move the object to the respective location.

You can also delete the existing object from the source or destination by clicking the delete icon.

Note
Rules that are not applicable are grayed out in the table.

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 Firewall 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**.

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 3 Click the following tabs and review the configuration items:

- **Access Control**
- **Objects (Network Objects, Port Objects, URL Objects)**
- **NAT**

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

Step 5 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 Firewall Management Center, reviews the existing objects, and compares those objects to the list of objects to be migrated. If an object already exists in Firewall 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 Firewall 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 6 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 Firewall 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 7 The **Optimize Your Configuration** dialog box displays a check mark next to each optimized attribute and identifies attributes that need optimization. Click **Proceed** to start the optimization. You can skip optimization, but it is recommended to optimize the attributes before proceeding with migration.

Step 8 When the validation is complete and the **Validation Status** dialog box displays the message **Successfully Validated**, continue with Push the Migrated Configuration to Firewall Management Center, on page 35.

Push the Migrated Configuration to Firewall Management Center

You cannot push the migrated Azure configuration to Firewall 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 Firewall Management Center. It does not deploy the configuration to the Firewall Threat Defense device. However, any existing configuration on the Firewall 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 Firewall Management Center.

Procedure

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

Step 2 Click **Push Configuration** to send the migrated Azure configuration to Firewall Management Center.

Note
When the Secure Firewall Migration tool identifies duplicate object attributes, a dialog box appears and prompts you to correct the duplicate values. You can proceed with migration only after renaming the duplicate attributes.

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 Firewall Management Center in the console.

Note
If there are configurations with errors when a bulk configuration push is being done, the migration tool throws a warning, prompting you to abort the migration to fix the error manually or to continue the migration leaving out the incorrect configurations. You can choose to view the configurations that have errors and then select **Continue with migration** or **Abort**. If you abort the migration, you can download the troubleshooting bundle and share it with Cisco TAC for analysis.

If you continue the migration, the migration tool will treat the migration as a partial success migration. You can download the postmigration report to view the list of configurations that were not migrated because of the push error.

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 31

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.

Procedure

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 Azure configuration was migrated:

- **Migration Summary**—A summary of the configuration that was successfully migrated from Azure firewall to Firewall Threat Defense, including information about the source Azure device, target Firewall Threat Defense device, and the successfully migrated configuration elements.

  You can also view a comparison chart. This chart illustrates the difference between the count of firewall elements pushed during premigration and postmigration.

- **Selective Policy Migration**—Details of the specific Azure feature selected for migration are available within three categories - Device Configuration Features, Shared Configuration Features, and Optimization.

- **Object Conflict Handling**—Details of the Azure firewall objects identified as having conflicts with the existing objects in Firewall Management Center. If the objects have the same name but a different configuration, you can rename these objects. Review these objects carefully and verify that the conflicts are appropriately resolved.

- **Optimization**—Details of the Azure firewall objects and ACL optimization. If the objects have the same name and configuration, the Migration Tool reuses the management center object. Review these objects carefully and verify that the conflicts are appropriately resolved.
- **ACL Category Conflict Handling**—Details of the ACL Rule categories identified as having conflicts with naming limitation on management center. The category names are trimmed as it exceeded the supported limit on management center. Review these categories carefully.
- **Partially Migrated Configuration**—Details of the 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 Firewall Management Center, and if so, configure these options manually.
- **Action Taken on Converted Features**—Details of the features that you chose not to migration using the Migration Tool.
  - **Access Rules You Chose Not to Migrate**—Details of the Access Control rules that you chose not to migrate using the Migration Tool. Review these lines and verify that all the rules you chose are listed in this section. If necessary, you can configure these rules manually.
  - **NAT Rules You Chose Not to Migrate**—Details of the Network Address Translation (NAT) rules that you chose not to migrate using the Migration Tool. Review these lines and verify that all the rules you chose are listed in this section. If necessary, you can configure these rules manually.
  - **Access Rules with Rule Action Change**—Details of all the Access Control Policy rules that had 'Rule Action' changed using the Migration Tool. The Rule Action values are - Allow, Trust, Monitor, Block, Block with reset. Review these lines and verify that all the rules you chose are listed in this section. If necessary, you can configure these rules manually.
  - **Access Control Rules that have Rule 'Log' Setting Change**—Details of the 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 necessary, you can configure these rules manually.
- **Errors/Failure on Migrated Configuration**—Details on error causing the migration failure while pushing the migrated configuration elements. The error reported below could be related to the incorrect migrated configuration or else conflict on management center due to some existing configuration or unsupported feature. Review these errors and verify before proceeding or resuming the configuration push to the target management center.

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 Firewall Management Center to ensure that this traffic is blocked by Firewall Threat Defense.

Step 3 Open the **Pre-Migration Report** and make a note of any Azure configuration items that you must migrate manually on the Firewall Threat Defense device.

Step 4 After you have completed your review, deploy the migrated configuration from Firewall Management Center to the Firewall 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 Firewall 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 configuration.

Parse Summary

Parse summary displays the number of objects, interfaces, NAT, policy, and application. The summary has three components: Pre-parse Summary, Parse Summary and Pre-push Summary.

- **Pre-parse Summary**—Pre-parse summary is displayed after the configuration is uploaded. At this stage, the Secure Firewall migration tool displays the count of various components. Only custom applications or applications that are used in the group is displayed. If a configuration is multi-vsys, the interface count will be displayed for the complete *vsys*. Pre-parse summary does not show all the applications because, the application that is called directly in policy is not counted. So, application count is different than the Parse summary. Similar behavior is applicable on NAT. Few components of the Pre-parse summary may display zero count but that does not mean that these configurations have zero configurations elements.
- **Parse Summary**—Parse summary is displayed after you click start conversion. At this stage, the Secure Firewall migration tool has taken the action on the configuration and all the unsupported configuration is removed from the summary count. The unsupported policies are part of the count, as unsupported policies are migrated to the Firewall Management Center as disabled. Every component of the configuration is parsed. The count that is displayed at the Parse summary is the exact configuration count that is going to get migrated.
- **Pre-push Summary**—Pre-push summary is displayed before you are prompted to push the configuration to the Firewall Management Center. The Pre-parse summary count may be different from the parse summary as per the action taken by the Secure Firewall migration tool. Directly referenced IP in NAT will be pushed as objects. If applications are mapped to ports, service count increases and the application will go down. If application mapping is left blank, the application count reduces. If the static route has a duplicate entry, that will be removed and the count will decrease.

Migration Failures

The following are the parsing failures during migration:

- **Parse Failure**—Parse failure occurs after the configuration is uploaded to the Secure Firewall migration tool. Due to the misconfiguration of the interface. If multiple IPs are configured or a /32 or /128 IP is assigned to interface, that leads to a parsing failure.

  If an interface has multiple IP assigned or tunneled, loopback, or VLAN interface are part of routing, that leads to a push failure.

  Workaround—Download the **Pre-Migration Report** and refer to **Configuration lines with errors** section of the Migration Report. This section displays the details of the configuration that is causing the issue. You must rectify the issue and reupload the configuration to Secure Firewall migration tool.

  If push failure is caused by tunnel, loopback, or VLAN interface in the routes, you must delete such routes and retry the migration, as such interfaces are not supported on the Firewall Management Center.

- **Push Failure**—Push failure occurs when Secure Firewall migration tool has migrated the configuration and is being pushed to the Firewall Management Center. Push failures are captured in the **Post-Migration Report**.

  Workaround—Download the **Post-Migration Report** and refer to **Error Reporting** section of the Migration Report. This section displays the details of the configuration that causes the issue. You must rectify the issue on the **Review and Validation** page by choosing **do not migrate** option for the section that shows the failure or you can fix the issue in the source configuration and reupload the configuration to Secure Firewall migration tool.

Uninstall the Secure Firewall Migration Tool

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

Before you begin

This procedure is applicable to you only if you are using the desktop version of the Secure Firewall migration tool.

Procedure

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: Azure 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, on page 40

Pre-Maintenance Window Tasks

Before you begin

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

Procedure

Step 1 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 2 Register the Firepower 2100 series device to be managed by the Firewall Management Center.

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

Step 3 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 23.

Step 4 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 Firewall Management Center.

For more information, see Specify Destination Parameters for the Secure Firewall Migration Tool, on page 28.

Step 5 Follow the instructions of this guide to sequentially review and validate the configuration to be migrated, and then push the configuration to the Firewall Management Center.

Step 6 Review the Post Migration report, manually setup and deploy other configurations to the Firewall Threat Defense and complete the migration.

For more information, see Review the Post-Migration Report and Complete the Migration, on page 36.

Step 7 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 39.

Procedure

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.

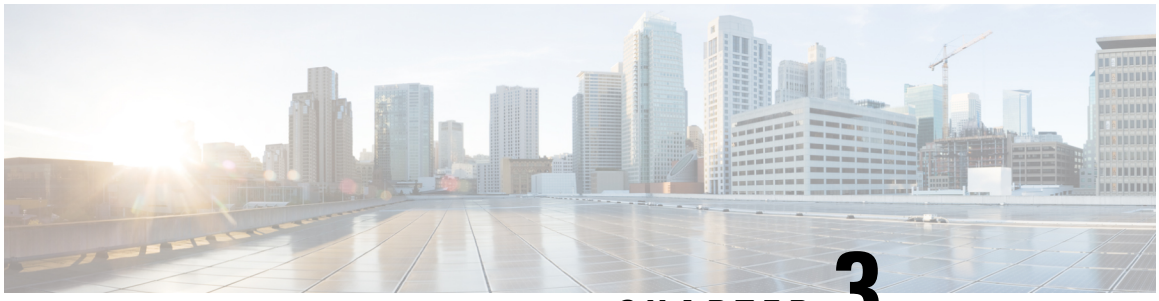
Step 3 Perform basic ping tests from devices which require layer 3 routing to Firepower 2100 series device interface IP addresses.

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 Firewall Management Center for your Firepower 2100 device.



CHAPTER 3

Cisco Success Network-Telemetry Data

• Cisco Success Network - Telemetry Data, on page 41

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 configuration to Firewall 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	Microsoft Azure
Target Management Version	The target version of management center	7.2 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
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

Data Point	Description	Example Value
Migration Status	The status of the migration of Azure 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

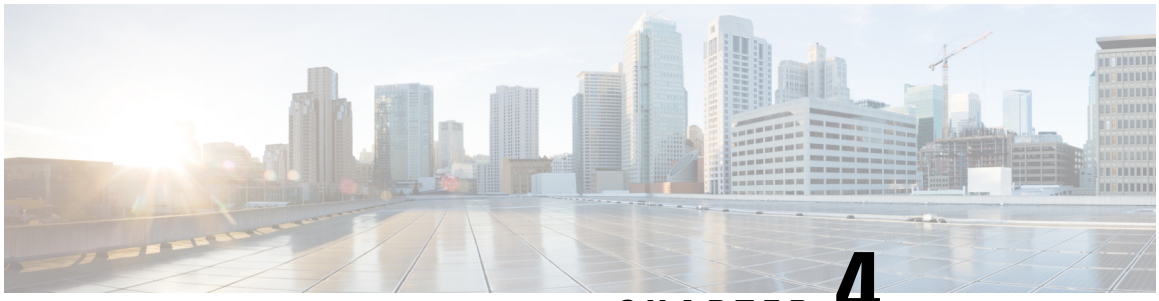
Table 4: Target Management Device (Firewall Management Center) Information

Data Point	Description	Example Value
Target Management Type	The type of target management device, namely, Firewall Management Center	Management Center
Target Device Version	The version of target device	75
Target Device Model	The model of target device	Cisco Secure Firewall Threat Defense for VMware

Table 5: Migration Summary

Table 6: Secure Firewall Migration Tool Performance Data

Data Point	Description	Example Value
Conversion Time	The time taken to parse 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 configuration to Firewall 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



CHAPTER 4

Troubleshooting Migration Issues

- Troubleshooting for the Secure Firewall Migration Tool, on page 43
- Logs and Other Files Used for Troubleshooting, on page 44

Troubleshooting for the Secure Firewall Migration Tool

A migration typically fails during the configuration file upload or during the push of the migrated configuration to Firewall Management Center.

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