

Migrating Check Point Firewall to Cisco Multicloud Defense Using the Secure Firewall Migration Tool

First Published: 2025-06-18

Last Modified: 2025-12-11

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 This Guide 1

About the Secure Firewall Migration Tool 1

What's New in the Secure Firewall Migration Tool 4

Licensing for the Secure Firewall Migration Tool 15

Platform Requirements for the Secure Firewall Migration Tool 16

Requirements and Prerequisites for Migration to Cisco Multicloud Defense 16

Check Point Firewall Configuration Support for Multicloud Defense 16

Supported Software Versions for Migration 17

Related Documentation 17

CHAPTER 2 **Check Point to Multicloud Defense Migration Workflow** 19

Workflow for Check Point to MultiCloud Defense Migration 19

Prerequisites for Migration 20

Download the Secure Firewall Migration Tool from Cisco.com 20

Run the Migration 21

Launch the Secure Firewall Migration Tool 21

Using the Demo Mode in the Secure Firewall Migration Tool 23

Export the Check Point Configuration Files for r80 24

Pre-Stage the Check Point (r80) Devices for Configuration Extraction Using Live Connect 24

Procedure to Export the Check Point Configuration Files for r80 32

Extract Another Configuration File 35

Specify Destination Parameters for Multicloud Defense 36

Review the Pre-Migration Report 38

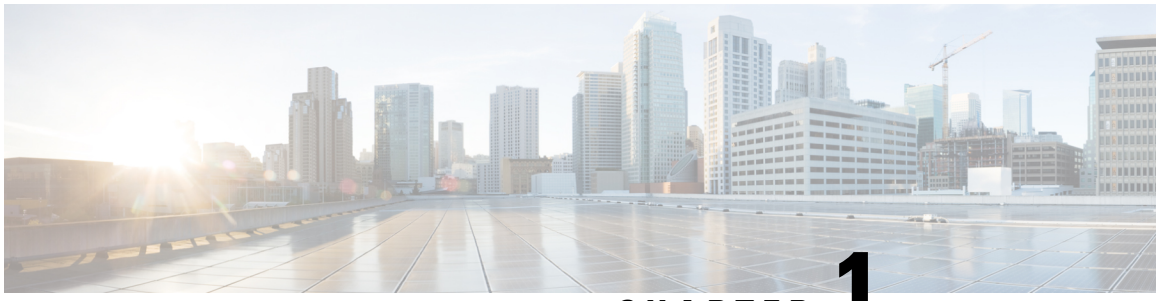
Optimize, Review, and Validate the Configuration to be Migrated 39

Push the Configuration to Multicloud Defense 41

Review the Post-Migration Report and Complete the Migration 42

CHAPTER 3 **Cisco Success Network-Telemetry Data 45**

Cisco Success Network - Telemetry Data 45



CHAPTER 1

Getting Started with the Secure Firewall Migration Tool

- About This Guide, on page 1
- About the Secure Firewall Migration Tool, on page 1
- What's New in the Secure Firewall Migration Tool, on page 4
- Licensing for the Secure Firewall Migration Tool, on page 15
- Platform Requirements for the Secure Firewall Migration Tool, on page 16
- Requirements and Prerequisites for Migration to Cisco Multicloud Defense, on page 16
- Check Point Firewall Configuration Support for Multicloud Defense, on page 16
- Supported Software Versions for Migration, on page 17
- Related Documentation, on page 17

About This Guide

This guide contains information on how you can download the Secure Firewall Migration Tool and complete the migration. In addition, it provides you troubleshooting tips to help you resolve migration issues that you may encounter.

About the Secure Firewall Migration Tool

The Secure Firewall Migration Tool converts supported Check Point configurations to Multicloud Defense. The Secure Firewall Migration Tool allows you to automatically migrate the supported Check Point features and policies to Multicloud Defense.

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

The Secure Firewall Migration Tool gathers Check Point information, parses it, and finally pushes it to the Multicloud Defense. During the parsing phase, the Secure Firewall Migration Tool generates a **Pre-Migration Report** that identifies the following:

- Check Point configuration XML or JSON lines with errors

- Check Point lists the Check Point XML or JSON lines that the Secure Firewall Migration Tool cannot recognize. Report the XML or JSON configuration lines under error section in the **Pre-Migration Report** and the console logs; this blocks 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**, Check Point 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 Check Point 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	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
7.7.10.4	This patch release contains bug fixes.

Version	Supported Features
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. However, the CDO tenant and Multicloud Defense must have the required licenses.

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 Migration to Cisco Multicloud Defense

For migrating configurations from Check Point to Multicloud Defense, ensure you have met the following requirements and prerequisites:

- You have a CDO tenant with Multicloud Defense enabled on it.
- You have purchased the required operating licenses for Multicloud Defense.

Note You can migrate configurations to Multicloud Defense even during the 90-day free trial because the trial experience offers full functionality of a paid subscription.

- You have the base URL of Multicloud Defense and the CDO tenant name handy.
- You have created an API key and also copied the **API Key ID** and **API Key Secret** that Multicloud Defense generates when you create the API key. See Create an API Key in Multicloud Defense for more information.

Check Point Firewall Configuration Support for Multicloud Defense

Supported Configurations

The Secure Firewall Migration Tool supports the following Check Point configurations during migrations to Multicloud Defense:

- Access control lists
- Network objects

- Port objects
- FQDN objects

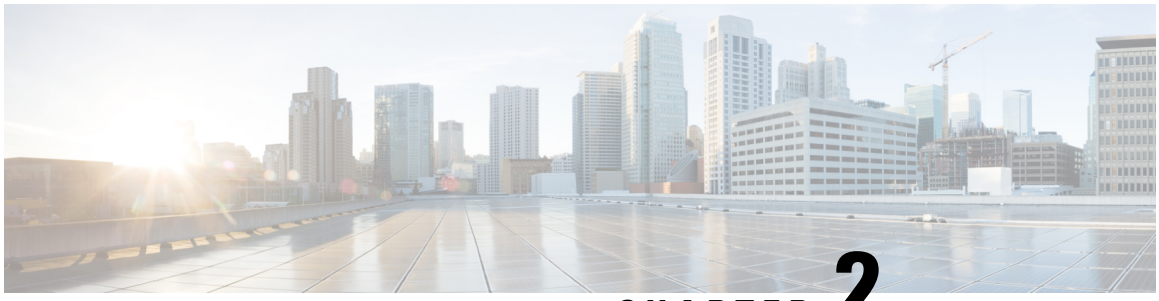
Supported Software Versions for Migration

The Secure Firewall migration tool supports migration of Check Point (r80-r81) versions to Multicloud Defense.

Related Documentation

This section summarizes the various Multicloud Defense-related user guides:

- Cisco Multicloud Defense User Guide
- Multicloud Defense Release Notes
- Multicloud Defense Naming Conventions
- Recommended Versions of Multicloud Defense Components
- Multicloud Defense in Cisco Security Provisioning and Administration



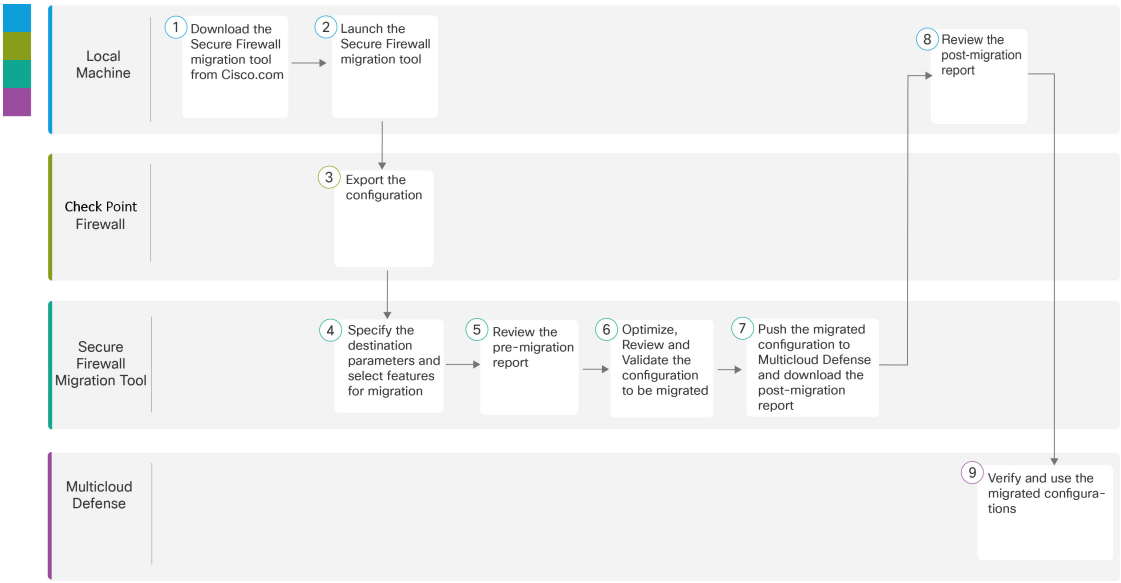
CHAPTER 2

Check Point to Multicloud Defense Migration Workflow

- Workflow for Check Point to MultiCloud Defense Migration, on page 19
- Prerequisites for Migration, on page 20
- Run the Migration, on page 21

Workflow for Check Point to MultiCloud Defense Migration

The following flowchart illustrates the workflow for migrating a Check Point firewall to Multicloud defense using the Secure Firewall Migration Tool.



	Workspace	Steps
1	Local machine	Download the latest version of the Secure Firewall Migration Tool from Cisco.com. For detailed steps, see Download the Secure Firewall Migration Tool from Cisco.com.

	Workspace	Steps
2	Local Machine	In the local machine, initiate the Secure Firewall Migration tool by double-clicking in the application file that you downloaded from Cisco.com.
3	Check Point Firewall	Export the configuration file. To export the configuration from the Check Point firewall, see Export the Check Point Configuration Files for r80, on page 24.
4	Secure Firewall Migration Tool	During this step, you can specify the destination parameters for Multicloud Defense. For detailed steps, see Specify Destination Parameters for Multicloud Defense, on page 36.
5	Secure Firewall Migration Tool	Navigate to the location where you downloaded the premigration report and review the report. For detailed steps, see Review the Pre-Migration Report, on page 38.
6	Secure Firewall Migration Tool	Optimize and review the configuration carefully and validate that it is correct. For detailed steps, see Optimize, Review, and Validate the Configuration to be Migrated, on page 39.
7	Secure Firewall Migration Tool	This step in the migration process sends the migrated configuration to Multicloud Defense and allows you to download the postmigration report. For detailed steps, see Push the Configuration to Multicloud Defense, on page 41.
8	Local Machine	Navigate to the location where you downloaded the postmigration report and review the report. For detailed steps, see Review the Post-Migration Report and Complete the Migration, on page 42.
9	Multicloud Defense	Verify the migrated configurations and use them as required in configuring gateways.

Prerequisites for Migration

Before you migrate your configuration, execute the following activities.

Download the Secure Firewall Migration Tool from Cisco.com

Before you begin

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

If you want to use the cloud version of the Secure Firewall migration tool hosted on CDO, 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 CDO user and want to use the migration tool hosted on it, log in to your CDO tenant and on the left pane, navigate to **Administration** > **Migration** > **Firewall Migration Tool** to create your migration instance.

Run the Migration

Launch the Secure Firewall Migration Tool

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

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 must extract information from a Check Point (r80) using the Secure Firewall migration tool, proceed to Export the Check Point Configuration Files for r80.

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, demo FTD devices, or Multicloud Defense.

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.

Export the Check Point Configuration Files for r80

Note Export of Check Point r80 configuration is supported only with the Live Connect feature on the Secure Firewall migration tool.

To configure on the Check Point device the credentials required for migration and to export the Check Point configuration files, perform the following:

- Pre-stage the Check Point (r80) Devices for Configuration Extraction using Live Connect
- Procedure to export the Check Point Configuration Files for r80

Pre-Stage the Check Point (r80) Devices for Configuration Extraction Using Live Connect

Note Ensure that your Check Point management center command line (CLI) is in CLISH mode. If it is in Expert mode, exit Expert mode and switch to CLISH mode before proceeding with the configuration export via Live Connect.

You can configure the credentials on the Check Point (r80) devices before migration using any one of the following steps:

- Distributed Check Point Deployment—When you have an independent Check Point Security Gateway and a Check Point Security Manager.
- Standalone Check Point Deployment—When you have a Check Point Security Gateway and a Check Point Security Manager as one single device.
- Multi-Domain Check Point Deployment—When you have a Check Point Security Gateway and a Check Point Security Manager with a multi-domain deployment setup.

Export from Distributed Check Point Deployment

You must configure the credentials on the Check Point (r80) devices before using Live Connect on the Secure Firewall migration tool to extract the Check Point configuration.

The procedure for pre-staging credentials on a distributed Check Point deployment includes the following steps:

Procedure

Step 1 Create the following on the Gaia Console Check Point Security Gateway:

a) In the web browser, open the Check Point Gaia Console application through an HTTPS session to connect to the Check Point Security Gateway.

b) Navigate to the **User Management** tab and choose **Users** > **Add**.

c) In the **Add User** window, create a new username and password with the following details:

- From the **Shell** drop-down, choose */etc/cli.sh*.
- From the **Available Roles**, choose *adminRole*.
- Retain the default values for the remaining fields.
- Click **Ok**.

d) SSH into your Check Point Security Gateway and create a new password using the command:

set expert-password <password>

Note

- If you already have the expert password configured on the Check Point device, reuse that.
- You will need these credentials on **Connect to Check Point Security Gateway** page as shown in step 3.

Once you have configured the expert password, the pre-staging of credentials for Check Point r80 Gateway is complete.

For more information, see Figure 3.

Step 2 Create the username and password on the Check Point Security Manager for r80:

a) On the SmartConsole application, perform these steps:

1. Log in to Check Point Security Manager.
2. Navigate to **Manage and Settings** > **Permissions and Administrators** > **Administrators**.
3. Click ***** to create a new username and password, and perform these steps:
   - Choose **Authentication Method** as **Check Point Password**.
   - Click **Set New Password** to set up a new password.

     Note
     Ensure that you do not select the **User Must Change Password on the Next Login** check box.

   - Choose **Permission Profile** as **Super User**.
   - Choose **Expiration** as **Never**.
4. Click **Publish** to save the configuration changes on the Check Point SmartConsole application.

b) On the Gaia Console for Check Point Security Manager, perform these steps:

Note
Ensure that the username and password that you now create is the same as that created in the SmartConsole application in Step 2a.

1. In the web browser, open the Gaia Console application through an HTTPS session to connect to the Check Point Security Manager.
2. Navigate to the **User Management** tab, and choose **Users** > **Add**.
3. Create a username and password that are the same as the username and password created in Step 2a (3) of the SmartConsole application.
   - From the **Shell** drop-down, choose */bin/bash*.
   - From the **Available Roles** drop-down, choose *adminRole*.
   - Retain the default values for the remaining fields.
   - Click **Ok**.
4. SSH into the Check Point Security Manager and create an expert password using the command:

   set expert-password <password>

   Note
   - If you have already configured the expert password, you can use that password.
   - The username and password that are created in Step 2b (3) and Step 2a (3) must be the same.

Pre-staging of credentials on Check Point in a distributed deployment for Check Point Security Manager is complete.

You will need these credentials on **Connect to Check Point Security Manager** page as shown in Step 4.

If you are using a custom API port on the Check Point Smart Manager, see Custom API Port for Check Point r80.

What to do next

Export the Check Point Configuration Files for r80

Export from Standalone Check Point Deployment

You must configure the credentials on the Check Point (r80) devices before using Live Connect on the Secure Firewall migration tool to extract the Check Point configuration.

The procedure for pre-staging credentials on standalone Check Point deployment includes the following steps:

Procedure

Step 1 In the web browser, open the Gaia Console application through an HTTPS session to connect to the standalone Check Point Device that manages both Check Point Security Gateway and Check Point Security Manager.

Step 2 Navigate to the **User Management** tab and choose **Users** > **Add**.

a) In the **Add User** window, create a new username and password with the following details:

- From the **Shell** drop-down, choose */etc/cli.sh*.
- From the **Available Roles** drop-down, choose *adminRole*.
- Retain the default values for the remaining fields.
- Click **Ok**.

You will need these credentials on **Connect to Check Point Security Gateway** page as shown in step 3.

For more information, see Figure 3.

b) In the **Add User** window, create another username and password with the following details:

- From the **Shell** drop-down, choose */bin/bash*.
- From the **Available Roles** drop-down, choose *adminRole*.
- Retain the default values for the remaining fields.
- Click **Ok**.

Step 3 Create the following on the SmartConsole application for r80 on the Check Point device:

Note
Ensure that the username and password that you will now create are the same as those created in the Check Point Gaia Console in the preceding step.

a) Log in to SmartConsole application of the Check Point device.
b) Navigate to **Manage and Settings** > **Permissions and Administrators** > **Administrators**.
c) Click ***** to create a new username and password with the following details:

- Choose the **Authentication Method** as **Check Point Password**.
- Click **Set New Password** to set up a new password.

  Note
  Ensure that you do not select the **User Must Change Password on the Next Login** check box.

- Choose the **Permission Profile** as **Super User**.
- Choose the **Expiration** as **Never.**

The username and password that you created in Step b of Step 2 and Step c of Step 3 must be the same.

You will need these credentials on **Connect to Check Point Security Manager** page as shown in Step 4.

d) Click **Publish** to save the configuration changes on the Check Point SmartConsole application.

Step 4 SSH into the Check Point device and create an expert password using the command:

set expert-password <password>

Note

- If you already have the expert password configured on the Check Point device, reuse that.
- The username and password that were created in Step b of Step 2 and Step c of Step 3 must be the same.

Pre-staging of credentials on Check Point devices in a Standalone deployment is complete.

If you are using a custom API port on the Check Point Smart Manager, see Custom API Port for Check Point r80.

What to do next

Export the Check Point Configuration Files for r80

Export from Multi-Domain Check Point Deployment

You must configure the credentials on the Check Point (r80) devices using Live Connect on the Secure Firewall migration tool to extract the Check Point configuration.

The procedure for pre-staging credentials on a multi-domain Check Point deployment includes the following steps:

Procedure

Step 1 Create the following on the Gaia Console Check Point Security Gateway:

a) In the web browser, open the Gaia Console application through an HTTPS session to connect to the Check Point Security Gateway.

b) Navigate to the **User Management** tab, and choose **Users** > **Add**.

c) In the **Add User** window, create a new username and password with the following details:

- From the **Shell** drop-down, choose */etc/cli.sh*.
- From the **Available Roles** drop-down, choose *adminRole*.
- Retain the default values for the remaining fields.
- Click **Ok**.

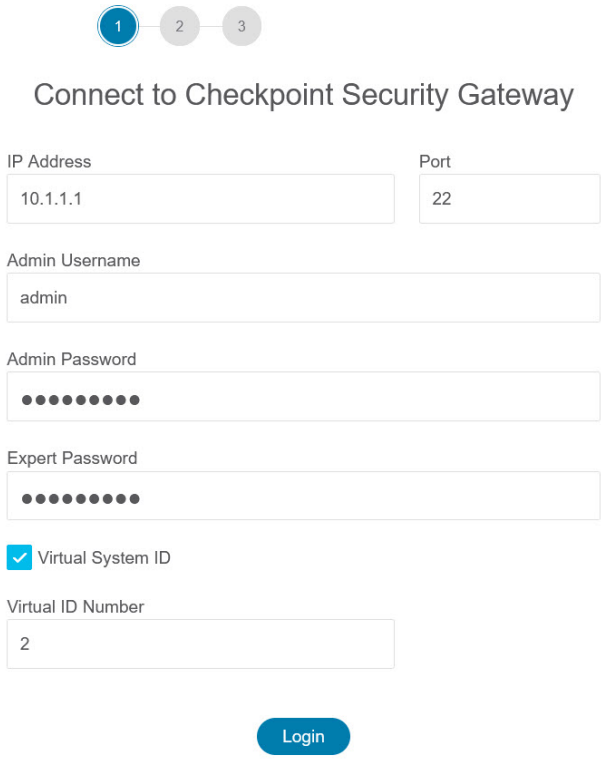
d) SSH into your Check Point Security Gateway and create a new password using the command:

set expert-password <password>

Pre-staging of credentials on the Check Point Security Gateway for a multi-domain deployment is complete.

e) (Optional) When exporting configuration from a Virtual System Extension (VSX) device, check the **Virtual System ID** checkbox to be able to enter the virtual system ID.

Figure 1: Connect to Check Point Security Gateway - Multi-Domain Deployment



Step 2 Create the username and password on the Check Point Security Manager:

a) On the SmartConsole (mds) application, perform these steps:

1. Log in to Check Point Security Manager.
2. Navigate to **Manage and Settings** > **Permissions and Administrators** > **Administrators**.
3. Click ***** to create a new username and password with the following details:
   - Choose the **Authentication Method** as **Check Point Password**.
   - Click **Set New Password** to set up a new password.

     Note
     Ensure that you do not select the **User Must Change Password on the Next Login** check box.

   - Choose the **Permission Profile** as **Multi-domain Super User**.
   - Choose the **Expiration** as **Never**.
4. Click **Publish** to save the configuration changes on the Check Point SmartConsole application.

   If you are using a custom API port on the Check Point Smart Manager, see Custom API Port for Check Point r80.

b) On the Gaia Console for Check Point Security Manager, perform these steps:

Note

Ensure that the username and password that you will now create is the same as that created in the SmartConsole application Step 2a (3).

1. In the web browser, open the Gaia Console application through an HTTPS session to connect to the Check Point Security Manager.
2. Navigate to the **User Management** tab, and choose **Users** > **Add**.
3. Create a username and password that is the same as that created in Step 2a (3) of the SmartConsole application.
   - From the **Shell** drop-down, choose */bin/bash*.
   - From the **Available Roles** drop-down, choose *adminRole*.
   - Retain the default values for the remaining fields.
   - Click **Ok**.
4. SSH into your Check Point Security Manager and create a new password using the command:

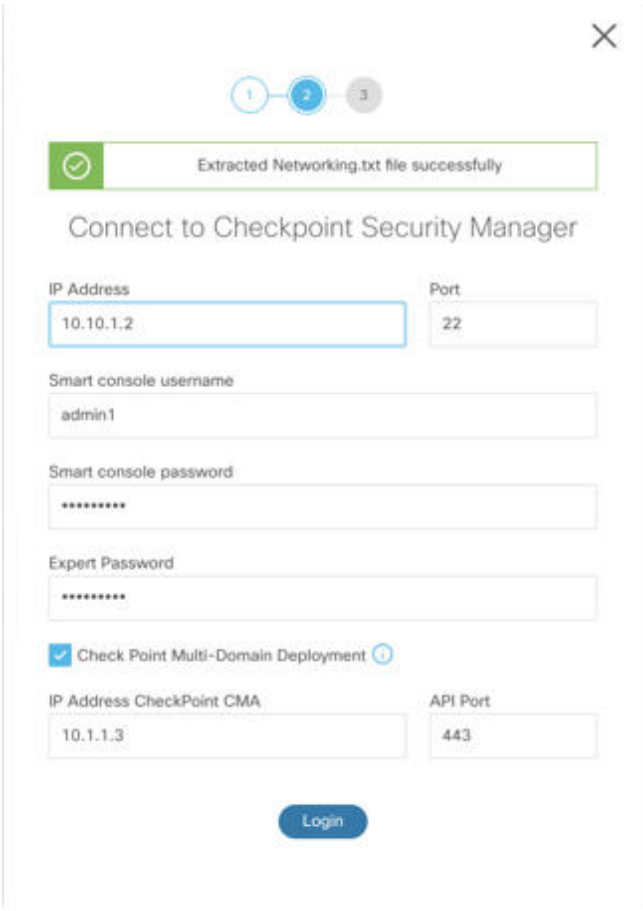
   set expert-password <password>

   Note
   - If you already have the expert password configured on the Check Point device, reuse that.
   - The username and password that are created in Step 2a (3) and Step 2b (3) must be the same.

Pre-staging of credentials on Check Point Security Manager in a Multi-Domain deployment is complete.

You will need the credentials to connect to Live Connect as in Figure 2.

Figure 2: Connect to Check Point Security Manager - Multi-Domain Deployment



Note

- If you are using a custom API port on the Check Point Smart Manager, see Custom API Port for Check Point r80.
- Extraction of Global Policy Package for Multi-Domain Deployment is not possible. Hence, the Objects, ACE rules, and NAT rules configured as part of configuration under Check Point CMA are only exported and migrated.

What to do next

Export the Check Point Configuration Files for r80

Use a Custom API Port for Check Point (r80) Security Manager

Note If you are using a custom API port on the Check Point Smart Manager, perform these steps:

- Check the **Check Point Multi-Domain Deployment** check box on the **Check Point Security Manager** page of Live Connect.
- Add the IP Address of Check Point CMA and API port details if using the multi-domain deployment.
- Retain the IP Address of the Check Point Security Manager if it is a general deployment and enter the details of the Custom API Port.

Procedure to Export the Check Point Configuration Files for r80

Before you begin

It is mandatory to pre-stage the Check Point devices. For detailed information on configuring the credentials on the Check Point (r80) devices before migration, see Pre-stage the Check Point (r80) Devices for Configuration Extraction Using Live Connect.

Note

- We recommend that you use Live Connect to extract the Check Point (r80) configurations.
- Using a Check Point (r80) configuration, that is not exported using Live Connect in the Secure Firewall migration tool, results in the configuration getting migrated as unsupported, getting partially migrated, or resulting in a failed migration.

  If the information in the configuration export is incomplete, certain configurations are not migrated and are marked as **unsupported**.

To export the Check Point configuration files for r80, perform the following:

Procedure

Step 1 Select Check Point (r80) from the **Select Source Config** page.

Step 2 Click **Connect**.

Note
Live connect is available for Check Point (r80) only.

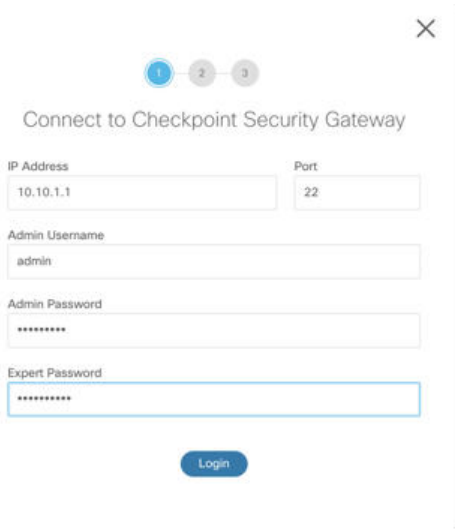
Step 3 Connect to Check Point Security Gateway. Perform the following:

a) Enter the following in the Check Point r80 Security Gateway:

- IP Address
- SSH Port
- Admin Username

- Admin Password
- Expert Password

Figure 3: Connect to Check Point Security Gateway



b) Click **Login**.

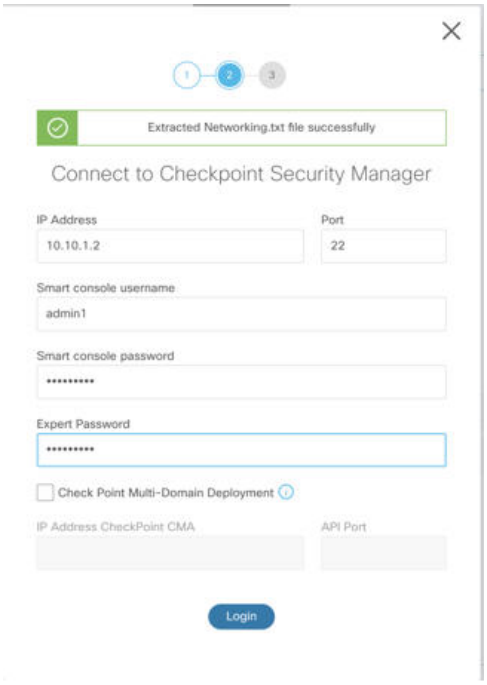
The Secure Firewall migration tool generates the *networking.txt* file that has device-specific configurations such as interface and route configurations. Store the *networking.txt* file in a local directory for the current session of the Secure Firewall migration tool.

Step 4 Connect to Check Point Security Manager. Perform the following:

a) Enter the following in the Check Point r80 Security Manager:

- IP Address
- SSH Port
- Smart Console Username
- Smart Console Password
- Expert Password

Figure 4: Connect to Check Point Security Manager



b) Click **Login**.

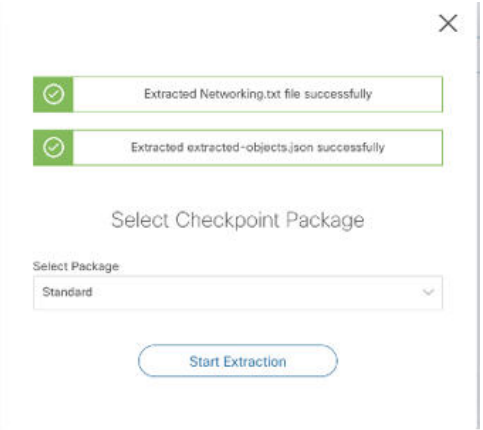
The Secure Firewall migration tool generates the *Extracted-objects.json* file that captures the complete network and service object configuration available in the Check Point Security Manager.

Store the *Extracted-objects.json* in a local directory for the current session of the Secure Firewall migration tool.

Note
If you have connected the Secure Firewall migration tool to the Check Point Security Manager, the list of policy packages available in the Check Point Security Manager is displayed.

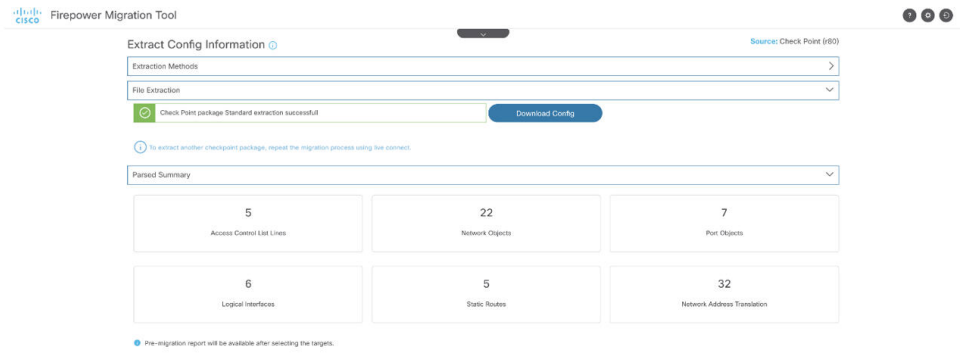
Step 5 Select the Check Point Policy Package that you want to migrate from the **Select Check Point Package** list, and click **Start Extraction**.

Figure 5: Extracting the Check Point Policy Package



Step 6 Download the configuration and proceed with the migration.

Figure 6: Extraction of the Check Point Configuration Complete for Distributed and Standalone Deployment



Step 7 Click **Next** to proceed with Migration of Check Point (r80) configuration.

Extract Another Configuration File

To extract another configuration file, perform the following steps:

- Click **Back to source selection** to extract a new configuration for a different policy package or to connect to a different Check Point (r80) firewall.
- Download the current configuration if you must migrate the extracted Check Point (r80) configuration later.

Note The current configuration file is downloaded to a default download location set by the browser.

You can use Assembly Line Approach to extract r80 configuration:

- Perform Live Connect to extract the Check Point (r80) configuration file for each package of firewall or for different firewalls.
- Create a repository for multiple configurations.
- Use the **Start Migration later** option using manual upload to proceed with the migration later.

Specify Destination Parameters for Multicloud Defense

Before you begin

- Ensure that you have a CDO tenant with Multicloud Defense enabled on it.
- Ensure that you have purchased the required operating licenses for Multicloud Defense.

Note You can migrate configurations to Multicloud Defense even during the 90-day free trial because the trial experience offers full functionality of a paid subscription.

- Ensure that you have obtained the base URL of Multicloud Defense and the CDO tenant name.
- Ensure that you have created an API key and also copied the **API Key ID** and **API Key Secret** that Multicloud Defense generates when you create the API key. See Create an API Key in Multicloud Defense for more information.

Procedure

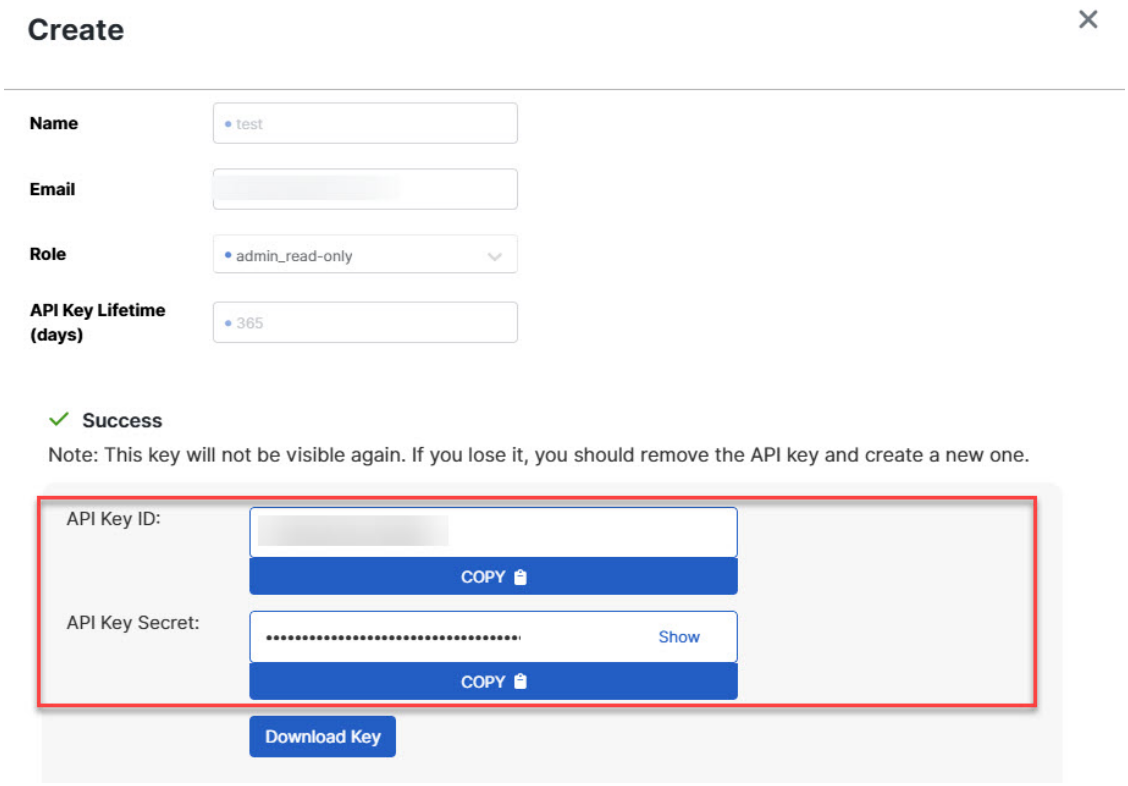
Step 1 On the **Select Target** window, choose **Multicloud Defense**.

Step 2 Specify the following parameters in the correponding fields to enable the connection between the migration tool and Multicloud Defense:

- **Enter Base URL**: This is the base URL that you see on your browser when you connect to your Multicloud Defense controller. For example, when you are in the controller dashboard, copy the link on your browser, excluding the **/dashboard** part. The URL looks like https://xxxx.mcd.apj.cdo.cisco.com
- **Enter Tenant Name**: The name of your CDO tenant. Copy it from the profile drop-down on the top-right corner when you are in the Multicloud Defense window or from **Administration** > **General Settings** if you are in the CDO window.
- **Enter API Key ID**: The **API Key ID** that Multicloud Defense controller generates when you create an API key by navigating to **System and Accounts** > **API Keys**. Specify a name for the key, your email address, the role you want the API key to have, and the API key lifetime to generate a key. The default key lifetime is set to 365 days.
- **Enter API Key Secret**: The **API Key Secret** that Multicloud Defense controller generates when you create an API key.

Note

Ensure you copy both the **API Key ID** and **API Key Secret** when they are displayed only at the time of creating the API key. If you missed to copy them, delete the API key that you created, generate a new one, and make sure you copy them this time.



Step 3 Click **Connect** and wait to receive the **Successfully gathered** message, which confirms that the connection attempt to Multicloud Defense is a success.

Step 4 The **Select Features** lets you select the configurations that you want to migrate to Multicloud Defense. **Access Control** and **Migrate Only Reference Objects** checkboxes are checked by default.

Note that other configurations from the source firewall such as interfaces and routes are not supported for this migration.

Step 5 Click **Proceed** and **Start Conversion**. Wait for the migration tool to parse the source configurations.

Step 6 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 7 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.

Step 8 Click **Next**.

Review the Pre-Migration Report

Note Configurations which are not parsed by the Secure Firewall Migration Tool are represented in the **Pre-Migration Report** with the exact XML (r75-r77.30) or json (r80) tags as in the source configuration files.

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 configuration elements that can be successfully migrated to Firewall Threat Defense or Multicloud Defense and specific features selected for migration.
- **Configuration Lines with Errors**—Details of configuration elements that cannot be successfully migrated because the Secure Firewall Migration Tool could not parse them. Correct these errors in the 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 configuration elements that are ignored because they are not supported by the Multicloud Defense 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 Multicloud Defense, and if not supported, plan to configure the features manually.

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

Step 4 After your 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 to be Migrated

Before you begin

The **Optimize, Review and Validate Configuration** page lets you review and validate the configuration parameters that you are about to migrate to the target Multicloud Defense. In this step, the migration tool validates the configurations against the existing configuration on Multicloud Defense and suggests changes that need to be performed for the migration to be successful, such as associating access control rules and renaming objects to avoid duplicates on the target Multicloud Defense.

After you validate, a flashing tab indicates that there is action you need to perform on the tab.

Procedure

Step 1 On the **Access Control** tab that lists all your access control list (ACL) entries, you can do the following:

- Click **Optimize ACL** to let the migration tool identify all the shadow and redundant ACLs and choose whether to migrate them as disabled ACLs or to exclude them from being migrated.

  Secure Firewall Migration Tool ACL Optimization Overview

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

  The ACL optimization supports the following ACL types:

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

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

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

  Click **Download Report** to review the ACL name and the correponding redundant and shadowed ACLs tabulated in an Excel file. Use the **Detailed ACL Information** sheet to view more ACL information.

  Click **Proceed** to start the optimization process.

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

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

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

- If you do not want to migrate or want to migrate a few ACLs as disabled, check the checkboxes against the row, click **Actions**, and choose the relevant option. Check the **Select all entries** checkbox to perform bulk changes.
- To edit an access control list policy, select the row by checking the check box for the policy, and choose **Actions** > **Edit**.

  All rules that are not applicable are grayed out in the table.

Step 2 On the **Objects** tab, you can do the following:

Choose the following tabs and review the mappings:

- Network Objects
- Port Objects
- FQDN Objects

If you want to rename an object, check the checkbox against the object row, click **Actions**, and choose **Rename**. Check the **Select all entries** checkbox to perform bulk changes.

Step 3 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 Multicloud Defense, reviews the existing objects, and compares those objects to the list of objects to be migrated. If an object already exists in Multicloud Defense, 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 Multicloud Defense.
- 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 4 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 Multicloud Defense 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 5 When the validation is complete and the **Validation Status** dialog box displays the message **Successfully Validated**, continue with pushing the configuration to Multicloud Defense.

Push the Configuration to Multicloud Defense

Before you begin

You cannot push the configuration to Multicloud Defense if you have not successfully validated the configuration and resolved all object conflicts.



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

Procedure

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

Step 2 Click **Push Configuration** to send the source firewall configuration to Multicloud Defense.

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 Multicloud Defense 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.

A 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 the configuration 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

Before you begin

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.

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 source configuration was migrated.

a. **Migration Summary**—A summary of the configuration that was successfully migrated from your source firewall to Multicloud Defense.

You can also view a comparison chart that illustrates the difference between the count of pre-migration and post-migration states.

b. **Object Conflict Handling**—Details of the objects that were identified as having conflicts with existing objects in Multicloud Defense. If the objects have the same name and configuration, the Secure Firewall migration tool reused the Multicloud Defense object. If the objects have the same name but a different configuration, you renamed those objects. Review these objects carefully and verify that the conflicts were appropriately resolved.

c. **Access Control Rules That You Chose Not to Migrate**—Details of the rules that you choose not to migrate with the Secure Firewall migration tool. Review these rules that were disabled by the Secure Firewall migration tool and were not migrated. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.

d. **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 Multicloud Defense, and if so, configure these options manually.

e. **Expanded Access Control Policy Rules**—Details of the source firewall access control policy rules that were expanded from a single point rule into multiple Multicloud Defense rules during migration.

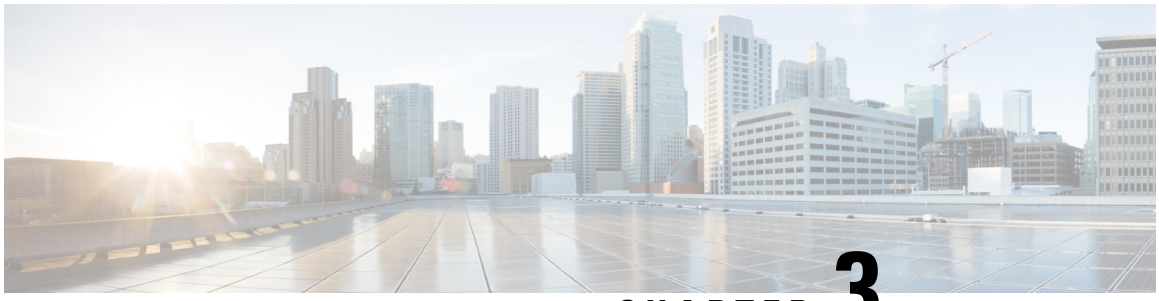
f. **Actions Taken on Access Control Rules**

- **Access Rules You Chose Not to Migrate**—Details of the access control rules that you choose not to migrate with the Secure Firewall migration tool. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually in Multicloud Defense.
- **Access Rules with Rule Action Change**—Details of all Access Control Policy Rules that had 'Rule Action' changed using the Secure Firewall migration tool. The Rule Action values are - Allow, Trust, Monitor, Block, Block with reset. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually in Multicloud Defense.

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 Multicloud Defense to ensure that this traffic is blocked.

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

Step 4 Verify and ensure that all the migrated configuration parameters are available on Multicloud Defense.



CHAPTER 3

Cisco Success Network-Telemetry Data

• Cisco Success Network - Telemetry Data, on page 45

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 or Multicloud Defense, 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 1: Limited Telemetry

Data Point	Description	Example Value
Time	The time and date when the telemetry data is collected	2025-04-11 14:17:24
Source Type	The source device type	Check Point
Source Device Version	The version of Check Point device	r81.20
Source Version	Version of Check Point	r81
Target Management Version	The target version of management center	6.23 or later
Target Management Type	The type of target management device, namely, management center	Management Center
Target Device Version	The version of target device	7.6

Data Point	Description	Example Value
Target Device Model	The model of target device	Cisco Secure Firewall 3105 Threat Defense
Migration Tool Version	The version of the migration tool	7.7-12208
Migration Status	The status of the migration of Check Point 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 2: 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 3: 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 4: Migration Summary

Data Point	Description	Example Value
Access Control Policy		
Name	The name of access control policy	Doesn't Exist
Partially Migrated ACL Rule Counts	The total number of partially migrated ACL rules	3
Expanded ACP Rule Counts	The number of expanded ACP rules	0
NAT Policy		
Name	The name of NAT policy	Doesn't Exist
NAT Rule Counts	The total number of migrated NAT rules	0

Data Point	Description	Example Value
Partially Migrated NAT Rule Counts	The total number of partially migrated NAT rules	0
More migration details...		
Interface Counts	The number of updated interfaces	0
Sub Interface Counts	The number of updated subinterfaces	0
Static Routes Counts	The number of static routes	0
Objects Counts	The number of objects created	34
Object Group Counts	The number of object groups created	6
Security Zone Counts	The number of security zones created	3
Network Object Reused Counts	The number of objects reused	21
Network Object Rename Counts	The number of objects that are renamed	1
Port Object Reused Counts	The number of port objects that are reused	0
Port Object Rename Counts	The number of port objects that are renamed	0

Table 5: 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