

Migrating Check Point Firewall to Cisco Secure Firewall Threat Defense with the Cisco Secure Firewall Migration Tool

First Published: 2022-11-17

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)

© 2022– 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 18

Platform Requirements for the Secure Firewall Migration Tool 18

Requirements and Prerequisites for Threat Defense Devices 19

Check Point Configuration Support 19

Guidelines and Limitations 22

Supported Platforms for Migration 25

Supported Target Management Center for Migration 26

Supported Software Versions for Migration 28

CHAPTER 2 **Check Point to Threat Defense Migration Workflow** 29

End-to-End Procedure 29

Prerequisites for Migration 31

Download the Secure Firewall Migration Tool from Cisco.com 31

Export the Check Point Configuration Files 32

Export the Check Point Configuration Files for r77 32

Run the Migration 35

Launch the Secure Firewall Migration Tool 35

Using the Demo Mode in the Secure Firewall Migration Tool 38

Export the Check Point Configuration Files for r80-r82 38

Pre-Stage the Check Point (r80-r82) Devices for Configuration Extraction Using Live Connect 38

Procedure to Export the Check Point Configuration Files for r80-r82 46

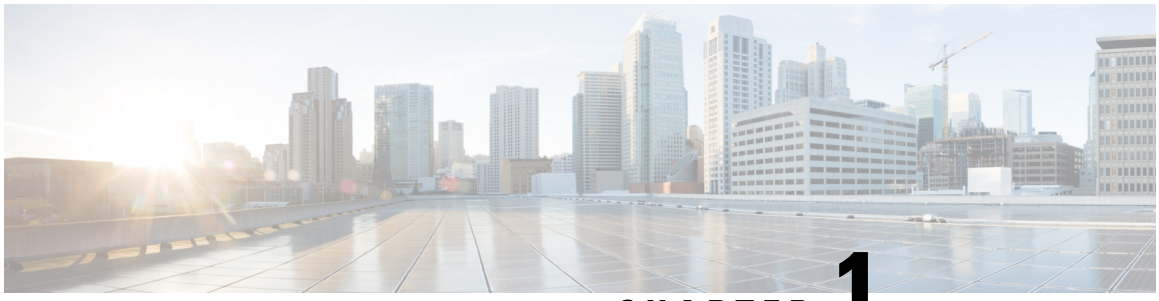
Extract Another Configuration File 49

Upload the Check Point Configuration File 50

Specify Destination Parameters for the Secure Firewall Migration Tool 50
Review the Pre-Migration Report 53
Map Check Point Firewall Configurations with Firewall Threat Defense Interfaces 54
Map Check Point Interfaces to Security Zones and Interface Groups 55
Optimize, Review and Validate the Configuration 57
Push the Migrated Configuration to Firewall Management Center 62
Review the Post-Migration Report for Check Point and Complete the Migration 63
Uninstall the Secure Firewall Migration Tool 64
Sample Migration: Check Point to Threat Defense 2100 64
Pre-Maintenance Window Tasks 64
Maintenance Window Tasks 66

CHAPTER 3 **Cisco Success Network-Telemetry Data** 67
Cisco Success Network - Telemetry Data 67

CHAPTER 4 **Troubleshooting Migration Issues** 77
Troubleshooting for the Secure Firewall Migration Tool 77
Logs and Other Files Used for Troubleshooting 78
Troubleshooting Check Point File Upload Failures 78
Troubleshooting Example for Check Point: Cannot Find Member of Object Group (For r75–r77.30 Only) 79
Troubleshooting Example for Check Point (r80-r82) for Live Connect 79



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 18
- Platform Requirements for the Secure Firewall Migration Tool, on page 18
- Requirements and Prerequisites for Threat Defense Devices, on page 19
- Check Point Configuration Support, on page 19
- Guidelines and Limitations, on page 22
- Supported Platforms for Migration, on page 25
- Supported Target Management Center for Migration, on page 26
- Supported Software Versions for Migration, on page 28

About the Secure Firewall Migration Tool

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

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

- 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

If there are parsing errors, you can rectify the issues, reupload a new configuration, connect to the destination device, map the Check Point interfaces to Firewall Threat Defense interfaces, map security zones and interface groups, 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
10.0.2	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: • Secure Firewall Migration Tool 4.0.2 introduces the inbuilt configuration extractor tool, which is now displayed on the **Extract Config Information** page. This eases configuration extraction and eliminates the task of downloading the extractor tool. Note that the FMT-CP-Config-Extractor tool is no longer available as a stand-alone application to download. See Export Device Configuration using Configuration Extractor for more information. • 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?**.

Version	Supported Features
4.0.1	The Secure Firewall migration tool 4.0.1 includes the following new features and enhancements: • You can now migrate Check Point R81 configuration to Secure Firewall Threat Defense. • You can now choose to add a **Virtual System ID** when connecting to the Check Point Security Gateway, for exporting configuration from a multi-domain Virtual System Extension (VSX) deployment. • You can extract configuration from a Check Point VSX version R77 by executing a few commands manually. See Export Device Configuration Using FMT-CP-Config-Extractor_v4.0-7965 Tool in the *Migrating Check Point Firewall to Threat Defense with the Migration Tool* guide for detailed information.
3.0.1	• For ASA with FirePOWER Services, Check Point, Palo Alto Networks, and Fortinet, Secure Firewall 3100 series is only supported as a destination device.
3.0	The Secure Firewall migration tool 3.0 provides support to migrate to Cloud-delivered Firewall Management Center from Check Point if the destination management center is 7.2 or later.
2.5.2	The Secure Firewall migration tool 2.5.2 provides support to identify and segregate ACLs that can be optimized (disabled or deleted) from the firewall rule base without impacting the network functionality from Check Point Firewalls. The ACL Optimization supports the following ACL types: • Redundant ACL—When two ACLs have the same set of configurations and rules, then removing the non-base ACL will not impact the network. • Shadow ACL—The first ACL completely shadows the configurations of the second ACL. **Note** Optimization is available for the Check Point only for ACP rule action. The Secure Firewall migration tool 2.5.2 supports Border Gateway Protocol (BGP) and Dynamic-Route Objects migration if the destination Firewall Management Center is 7.1 or later.

Version	Supported Features

2.2	• Provides support for r80 Check Point OS versions
	• Provides support for Live Connect to extract configurations from Check Point (r80) devices.
	• You can migrate the following supported Check Point configuration elements to Firewall Threat Defense for r80:
	  • Interfaces
	  • Static Routes
	  • Objects
	  • Network Address Translation
	  • Access Control Policies
	  • Global Policy—When you select this option, the source, and destination zones of the ACL policy are migrated as **Any** because there is no route-lookup.
	  • Zone-Based Policy—When you select this option, source, and destination zones are derived based on the predicative route-lookup through routing mechanism for the source and destination network objects or groups.
	Note
	Route-lookup is limited to Static routes and Dynamic routes (excluding PBR and NAT) only, and depending on the nature of the source and destination Network Object-Groups, this operation may result in rule explosion.
	Note
	IPv6 route-lookup for zone-based policy is unsupported.

Version	Supported Features

2.0	• The new optimization functionality in the Secure Firewall migration tool allows you to fetch the migration results quickly using the Search filters.
	• The Secure Firewall migration tool allows you to migrate the following supported Check Point configuration elements to Firewall Threat Defense:
	  • Interfaces
	  • Static Routes
	  • Objects
	  • Access Control Policy
	  • Global Policy—When you select this option, the source, and destination zones for the ACL policy are migrated as **Any**.
	  • Zone-Based Policy—When you select this option, source, and destination zones are derived based on the predicative route-lookup through routing mechanism for the source and destination network objects or groups.
	  Note
	  Route-lookup is limited to Static routes and Dynamic routes (excluding PBR and NAT) only, and depending on the nature of the source and destination Network Object-Groups, this operation may result in rule explosion.
	  • Network Address Translation
	• Provides support for Check Point OS versions—r75, r76, r77, r77.10, r77.20, and r77.30.

Licensing for the Secure Firewall Migration Tool

The Secure Firewall migration tool application is free and does not require license. However, the Firewall Management Center must have the required licenses for the related Firewall Threat Defense features to successfully register Firewall Threat Defense devices and deploy policies to it.

Platform Requirements for the Secure Firewall Migration Tool

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

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

- (macOS) Has Energy Saver settings configured so that the computer and the hard disk do not go to sleep during a large migration push

Requirements and Prerequisites for 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 Check Point 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.
  - The target native Firewall Threat Defense device must have at least an equal number of used physical data or port channel interfaces or subinterfaces (excluding 'management-only') as that of the Check Point; if not you must add the required type of interface on the target Firewall Threat Defense device. Subinterfaces are created by the Secure Firewall migration tool that are based on physical or port channel mapping.
  - 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 Check Point; 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.

Check Point Configuration Support

Supported Check Point Configurations

- Interfaces (Physical, VLAN, and Bond interfaces)
- Network objects and groups: Secure Firewall migration tool supports migrating all the Check Point network objects to the threat defense
- Service objects
- Network Address Translation

- Manual NAT rule containing Network Objects with Dual Type IP Address
- IPv6 conversion support (Interface, Static Routes, and Objects) and except zone-based ACLs with IPv6
- Access rules that are applied globally and support to convert Global ACLs to Zone-based ACLs
- Static routes, except for the routes configured with scope as local, and with logical interfaces as the egress interface for a static route without the next-hop IP address
- ACL with an additional logging type
- ACE with negate parameters
- Policy-based site-to-site VPN for Check Point r80-r82 and later versions: IPv4 and preshared key (PSK)-based authentication. We recommend that you use the **Live Connect** option to migrate VPN configurations.
- Identity-based ACL policies
- User-based access control policy rules

Note For the ACEs configured in Check Point that have corresponding NAT rules in Check Point, the Secure Firewall migration tool does not map the real IP addresses against the translated IP addresses in the corresponding migrated ACE rules. Secure Firewall migration tool does not map the IP addresses because of the lack of reference information for the ACE rule against the NAT rule. So, during the validation of the migrated ACE and NAT configuration on the Firewall Management Center, you must validate and manually make changes to the ACE rules corresponding to the threat defense packet flow.

Note Though the Secure Firewall migration tool does not migrate service objects (configured with a source and destination, and a port combination with the same type of object that is called in an object group), referenced ACL rules are migrated with full functionality.

For more information on Unsupported Check Point Configuration, see Unsupported Check Point Configuration.

Partially Supported Check Point Configurations

The Secure Firewall migration tool partially supports the following Check Point configurations for migration. Some of these configurations include rules with advanced options that can be migrated without those options. If the Firewall Management Center supports those advanced options, you can configure them manually after the migration is complete.

- Static routes with rank and ping parameters are partially migrated.
- Bond interface with mode, XOR, active backup, round-robin types are partially migrated to LACP type in Firewall Management Center by the Secure Firewall migration tool.
- Alias interface configurations part of parent interfaces like physical or bond Interface, alias interface configuration in ignored and parent interface attributes are migrated as is.
- Network object group of type exclusion is supported through an ACL to keep the meaning intact.
- ACL with Add logging type and ACL with Time range.

Unsupported Check Point Configurations

The Secure Firewall migration tool does not support the following Check Point configurations. If these configurations are supported in the Firewall Management Center, you can configure them manually after the migration is complete.

- Alias, Bridge, 6IN4 tunnel, loopback, and PPPoE interfaces
- Network objects and groups:
  - UTM-1 Edge gateway
  - Check Point host
  - Gateway cluster
  - Externally Managed Gateways or Hosts
  - Open Security Extension (OSE) device
  - Logical servers
  - Dynamic objects
  - VoIP domains
  - Zone
  - CP security gateway
  - CP management server
  - Network Object group of the exclusion type
- Service objects:
  - RPC
  - DCE-RPC
  - Compound TCP
  - GTP
  - Other Check Point Specific service objects
- ACL policies with:
  - Unsupported ACE action types (Client Auth, Session Auth, User Auth, and other custom authentication types) are migrated with the Allow action type, but in a disabled state
  - Zone-based policy with IPv6 route-lookup
  - Global Multi-Domain System rules cannot be migrated



Note The configurations from the Global Multi-domain system in Check Point multi-domain deployment cannot be exported. Hence the configurations pertaining to specific CMAs can only be exported and migrated.

- Objects with an Unsupported ICMP type and code
- Tunneling protocol-based access control policy rules
- Implied ACL rules
- Remote Access VPN
- Zones for ACE when zone-based ACE is selected and has the range object with value more than 100 is migrated and are marked as **Any** with no-lookup that is appended to the ACE name and appropriate comment
- Zone for ACE with IPv6 address when zone-based ACE selected is marked as **Any** and the ACE unsupported with an appropriate comment.

Unsupported NAT Rules

The Secure Firewall migration tool does not provide support for the following NAT rules:

- Auto NAT rules that hide behind the gateway
- Manual NAT rule using Check Point Security Gateway.
- Manual NAT rules containing an object-group of which the inherited object has IPv6 configuration
- Manual NAT rule with a service group
- IPv6 NAT rules

Unsupported Static Routes

- Static routes when no egress interface is found in **netstat -rnv**
- Static routes that have the logical gateway as exit interface
- Static routes of ECMP types
- Static routes that have the local scope attribute as exit interface

Guidelines and Limitations

During conversion, the Secure Firewall migration tool creates a one-to-one mapping for all supported objects and rules, whether they are used in a rule or policy. However, 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).

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

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

Check Point Configuration Limitations

Migration of the source Check Point configuration has the following limitations:

- The system configuration is not migrated.
- Live Connect of Firewall is supported only for Check Point (r80-r82) and later versions.
- All the Security Policies that are explicit (available in `Security_Policy.xml` for r77.30 and earlier versions and under Security Policy File for r80-r82 and later versions) are migrated to the ACP on the management center. The rules on a Check Point Smart dashboard are not migrated because implied rules are not part of the exported configuration.



Note

- For Check Point (r80-r82) and later versions, if there is a separate Application Layer Policy attached to the L4 Security Later Policy, the Secure Firewall migration tool migrates them as **unsupported**. Also, in such cases, there will be two files with ACE configurations: one for the security layer and the other for the application layer. The Secure Firewall migration tool migrates based on the priority information available in the access layer, in the *index.json* of the configuration zip file.
- For Check Point versions r80-r82 and later, which have the Multi-Domain Deployment setup, and, which have a Global Policy along with Customer-Managed Add-on (CMA) specific policy, the order in which the Secure Firewall migration tool migrates the Check Point configuration will be slightly different from the order in the source configuration. Also, in such cases, there will be two files with ACE configurations: one for the Global Policy, and the other for the CMA policy. ACEs configured under the Domain Layer will be migrated as **unsupported**.
- The definition of the order of ACE rules, configured for a CMA that has Action as the Domain Layer in the multi-domain system, is incomplete in the extracted configuration. So, if you have a Global policy attached to a specific CMA policy in the source configuration, validate the rule number index in the extracted configuration to ensure that it is in the correct order.

- Some of the Check Point configurations, such as Dynamic Routing and VPN to threat defense cannot be migrated using the Secure Firewall migration tooll. Migrate these configurations manually.
- Check Point bridge, tunnel, and alias interfaces to management center cannot be migrated.
- Nested service object-groups or port group are not supported on the management center. As part of conversion, the Secure Firewall migration tool expands the content of the referenced nested object-group or port group.
- The Secure Firewall migration tool splits the service objects or groups with source and destination ports that are configured within the same object. References to such access control rules are converted into management center rules with the exact same meaning.

Check Point Migration Guidelines

The migration of the Check Point log option follows the best practices for threat defense. The log option for a rule is enabled or disabled based on the source Check Point configuration. For rules with **drop** or **reject** action, the Secure Firewall migration tool configures logging at the beginning of the connection. If the action is **permit**, the Secure Firewall migration tool configures logging at the end of the connection.

Object Migration Guidelines

Service objects, which are called port objects in the threat defense have different configuration guidelines for objects. For example, one or more service objects can have the same name in Check Point with one object name in lowercase and the other object name in uppercase. But, each object must have a unique name, regardless of the case as in the threat defense. The Secure Firewall migration tool analyzes all Check Point objects and handles their migration to threat defense in one of the following ways:

- Each Check Point object has a unique name and configuration. The Secure Firewall migration tool migrates the objects successfully without changes.
- The name of a Check Point service object includes one or more special characters that are not supported by management center. The Secure Firewall migration tool renames the special characters in the object name with a "_" character to meet the management center object naming criteria.
- A Check Point service object has the same name and configuration as an existing object in management center. The Secure Firewall migration tool reuses the management center object for the threat defense configuration and does not migrate the Check Point object.
- A Check Point service object has the same name but a different configuration than an existing object in the management center. The Secure Firewall migration tool reports object conflict and allows you to resolve the conflict by adding a unique suffix to the name of the Check Point Service object for migration purposes.
- Multiple Check Point service objects have the same name but in different cases. The Secure Firewall migration tool renames such objects to meet the threat defense object naming criteria.

Guidelines and Limitations for Firewall Threat Defense Devices

As you plan to migrate your Check Point configuration to Firewall Threat Defense, consider the following guidelines and limitations:

- If there are any existing device-specific configurations on the Firewall Threat Defense such as routes, interfaces, and so on, during the push migration, the Secure Firewall migration tool cleans the device automatically and overwrites from the Check Point configuration.



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

  During migration, the Secure Firewall migration tool resets the interface configuration. If you use these interfaces in policies, the Secure Firewall migration tool cannot reset them and hence the migration fails.

- The Secure Firewall migration tool can create subinterfaces on the native instance of the Firewall Threat Defense device based on the Check Point configuration. Manually create interfaces and port channel interfaces on the target Firewall Threat Defense device before starting migration. For example, if your Check Point configuration is assigned with the following interfaces and port channels, you must create them on the target Firewall Threat Defense device before the migration:
  - Five physical interfaces
  - Five port channels
  - Two management-only interfaces

Note For container instances of Firewall Threat Defense devices, subinterfaces are not created by the Secure Firewall migration tool, only interface mapping is allowed.

Supported Platforms for Migration

The following Check Point and Firewall Threat Defense platforms are supported for migration with the Secure Firewall migration tool. For more information about the supported Firewall Threat Defense platforms, see Cisco Secure Firewall Compatibility Guide.

Note The Secure Firewall migration tool supports migration of standalone mode or distributed Check Point configuration to a standalone Firewall Threat Defense device only.

Supported Target Firewall Threat Defense Platforms

You can use the Secure Firewall migration tool to migrate a source Check Point configuration to the following standalone or container instance of the Firewall Threat Defense platforms:

- Firepower 1000 Series
- Firepower 2100 Series
- Secure Firewall 220 Series
- Secure Firewall 3100 Series
- Secure Firewall 3200 Series
- Firepower 4100 Series
- Secure Firewall 4200 Series
- Secure Firewall 6100 Series
- Firepower 9300 Series that includes:
  - SM-24
  - SM-36
  - SM-40
  - SM-44
  - SM-48
  - SM-56
- Threat Defense on VMware, deployed using VMware ESXi, VMware vSphere Web Client, or vSphere standalone client

- Threat Defense Virtual on Microsoft Azure Cloud or AWS Cloud

Note

- For pre-requisites and pre-staging of Firewall Threat Defense Virtual in Azure, see Getting Started with Secure Firewall Threat Defense Virtual and Azure.
- For pre-requisites and pre-staging of Firewall Threat Defense Virtual in AWS Cloud, see Threat Defense Virtual Prerequisites.

For each of these environments, once pre-staged as per the requirements, the Secure Firewall migration tool requires network connectivity to connect to the Firewall Management Center in Microsoft Azure or AWS Cloud, and then migrate the configuration to the Firewall Management Center in the Cloud.

Note The pre-requisites of pre-staging the Firewall Management Center or threat defense virtual is required to be completed before using the Secure Firewall migration tool, to have a successful migration.

Note The Secure Firewall migration tool requires network connectivity to any devices hosted in the cloud to either extract the source configuration (CP (r80-r82) Live Connect) or migrate the manually uploaded configuration to the Firewall Management Center in the cloud. Hence, as a pre-requisite, IP network connectivity is required to be pre-staged before using the Secure Firewall migration tool.

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 28.
- The Firewall Management Center software version that is supported for migration for Check Point is 6.2.3.3 and later.
- You have obtained and installed smart licenses for Firewall Threat Defense that include all features that you plan to migrate from the Check Point 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, Check Point 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 Check Point Versions

The Secure Firewall Migration Tool supports migration to Firewall Threat Defense that is running Check Point OS version r75-r77.30 and r80-r82.40. Select the appropriate Check Point version in the **Select Source** page.

The Secure Firewall Migration Tool supports migration from the Check Point Platform Gaia and Virtual System Extension (VSX) deployments.

Supported Firewall Management Center Versions for source Check Point Firewall Configuration

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

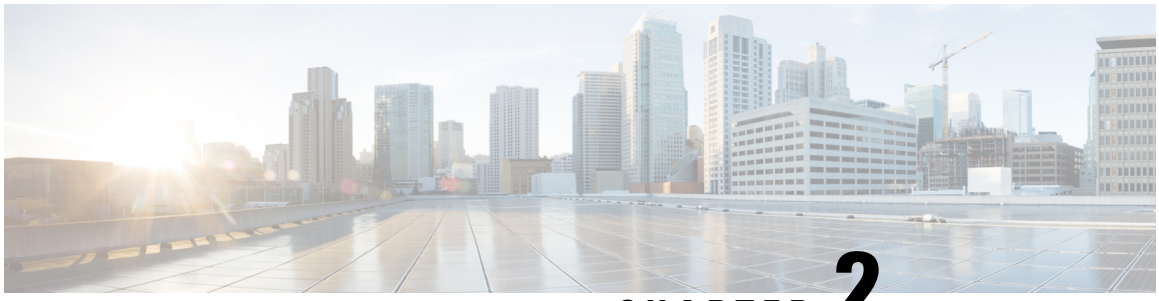


Note The migration to 6.7 Firewall Threat Defense device is currently not supported. Hence, migration may fail if the device is configured with data interface for Firewall Management Center access.

Supported Firewall Threat Defense Versions

The Secure Firewall Migration Tool recommends migration to a device that is running Firewall Threat Defense version 6.5 and later.

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



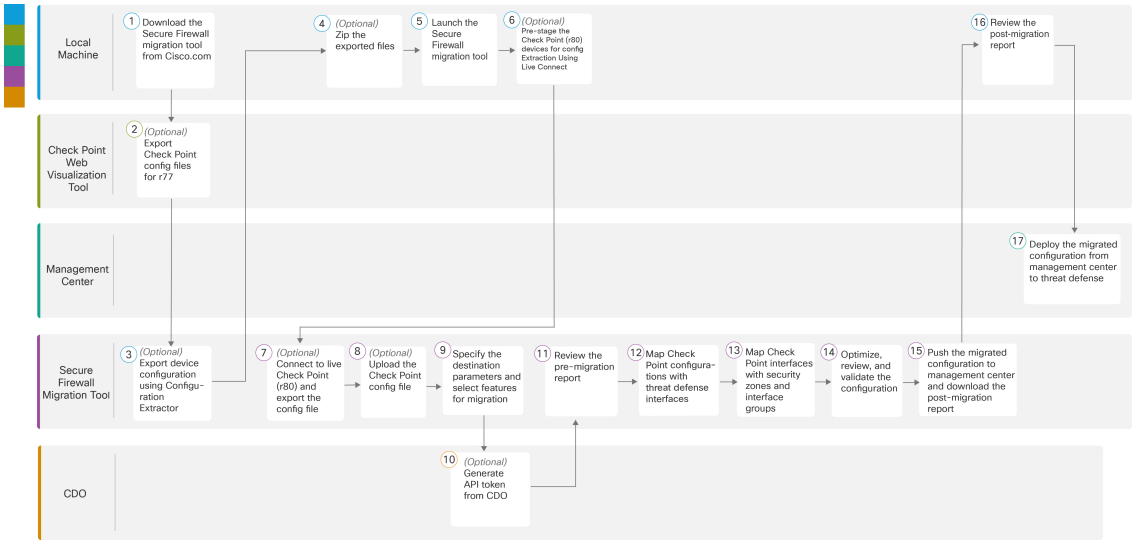
CHAPTER 2

Check Point to Threat Defense Migration Workflow

- End-to-End Procedure, on page 29
- Prerequisites for Migration, on page 31
- Run the Migration, on page 35
- Uninstall the Secure Firewall Migration Tool, on page 64
- Sample Migration: Check Point to Threat Defense 2100 , on page 64

End-to-End Procedure

The following flowchart illustrates the workflow for migrating a Check Point 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.

	Workspace	Steps
2	Check Point Web Visualization Tool	(Optional) Export the Check Point configuration file for r77: To export the Check Point configuration files for r77, see Export the Check Point Configuration Files for r77, on page 32. If you intend to export configuration files for r80-r82 using Secure Firewall migration tool live connect feature, skip to step 5.
3	Local Machine	Launch the Secure Firewall migration tool on your local machine and select **Check Point (r75–r77)** or **Check Point (r80-r82)** in the **Source Firewall Vendor** drop-down, based on your requirement. See Launch the Secure Firewall Migration Tool for more information.
4	Secure Firewall Migration Tool	(Optional) Export device configuration from Check Point (r75–r77): To export device configuration for r77 using **Configuration Extractor** through a secure gateway connection, see Export Device Configuration Using Configuration Extractor, on page 33.
5	Local Machine	(Optional) Zip the exported files: select all the exported configuration files for r77 and compress them to a zip file. For detailed steps, see Zip the exported files.
6	Local Machine	Pre-stage the Check Point (r80-r82) devices for config Extraction: You must configure the credentials on the Check Point (r80-r82) devices before using Live Connect on the Firewall. For pre-staging credentials on Check Point (r80-r82) devices, see Pre-stage the Check Point (r80-r82) devices for configuration Extraction. This step is only required if you are planning to migrate configuration files for r80-r82 devices. If you have planning to migrate configuration for r77 devices, skip to step 8.
7	Secure Firewall Migration Tool	(Optional) Connect to live Check Point (r80-r82) and export the config file: To export the Check Point configuration files for r80-r82 using live connect feature, see Procedure to Export the Check Point Configuration Files for r80-r82.
8	Secure Firewall Migration Tool	(Optional) Upload the Check Point config file: For detailed steps for uploading Check Point Configuration file, see Upload the Check Point Configuration File.
9	Secure Firewall Migration Tool	During this step, you can specify the destination parameters for the migration. For detailed steps, see Specify Destination Parameters for the Secure Firewall Migration Tool.
10	Security Cloud Control	(Optional) This step is optional and only required if you have selected cloud-delivered Firewall Management Center as destination management center. For detailed steps, see Specify Destination Parameters for the Secure Firewall migration tool, step 1.
11	Secure Firewall Migration Tool	Navigate to where you downloaded the pre-migration report and review the report. For detailed steps, see Review the Pre-Migration Report.

	Workspace	Steps
12	Secure Firewall Migration Tool	The Secure Firewall migration tool allows you to map the Check Point configuration with threat defense interfaces. For detailed steps, see Map Check Point Configurations with Secure Firewall Device Manager Threat Defense Interfaces.
13	Secure Firewall Migration Tool	To ensure that the Check Point configuration is migrated correctly, map the Check Point interfaces to the appropriate threat defense interface objects, security zones and interface groups. For detailed steps, see Map Check Point Interfaces to Security Zones and Interface Groups.
14	Secure Firewall Migration Tool	Optimize and review the configuration carefully and validate that it is correct and matches how you want to configure the threat defense device. For detailed steps, see Optimize, Review and Validate the Configuration to be Migrated.
15	Secure Firewall Migration Tool	This step in the migration process sends the migrated configuration to management center and allows you to download the post-migration report. For detailed steps, see Push the Migrated Configuration to Management Center.
16	Local Machine	Navigate to where you downloaded the post migration report and review the report. For detailed steps, see Review the Post-Migration Report and Complete the Migration.
17	Management Center	Deploy the migrated configuration from the management center to threat defense. For detailed steps, see Review the Post-Migration Report and Complete the Migration.

Prerequisites for Migration

Before you migrate your Check Point 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 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.

What to do next

Export the Check Point Configuration Files

Export the Check Point Configuration Files

You can export the Check Point Configuration for the following:

- Export the Check Point Configuration Files for R77
- Export the Check Point Configuration Files for r80-r82

Export the Check Point Configuration Files for r77

To export the Check Point configuration files for r77, perform the following:

- Export the Configuration Using Check Point Web Visualization Tool (WVT)
- Export Device Configuration Using Configuration Extractor, on page 33
- Zip the Exported Files

Export the Configuration Using Check Point Web Visualization Tool (WVT)

Procedure

Step 1 Open the command prompt on the workstation that has access to the Check Point Management Server.
Step 2 Download WVT from the Check Point Portal appropriate for the Check Point Firewall version.
Step 3 Unzip the WVT zip file.
Step 4 Create a new sub folder under the same root folder where the Check Point WVT tool is extracted.
Step 5 Change the directory on the command prompt to the directory where WVT is stored and execute the following commands:

```
C:\Web_Visualisation_Tool> cpdb2web.exe [-s management_server] [-u admin_name | -a certificate_file]
[-p password] [-o output_file_path] [-t table_names] [-c | -m gateway | -l package_names] [-gr] [-go]
[-w Web_Visualization_Tool_installation_directory]
```

For example,

```
C:\Web_Visualisation_Tool> cpdb2web.exe -s 172.16.0.1  -u admin -p admin123 -o  Outputs
```

A total of seven files are created in the *Outputs* directory when these commands are executed, where:

Command	Description
C:\Web_Visualisation_Tool	The root directory for the WVT tool.
172.16.0.1	The IP Address of the Check Point Management Server.
admin	The Check Point Management Server username.
Admin123	The Check Point Management Server password.
Outputs	The relative path to store output files.

Note
The name of the Security Policy and NAT Policy file must be `Security_Policy.xml` and `NAT_Policy.xml` respectively. If the filenames are different, rename them manually.

If there are multiple Security and NAT Policy files, ensure that you select and keep only the `Security_Policy.xml` and `NAT_Policy.xml` files of the Check Point device that you want to migrate.

What to do next

Export Device Configuration Using FMT-CP-Config-Extractor_v2.3.4-5381 Tool

Export Device Configuration Using Configuration Extractor

Procedure

Step 1 In the **Select Source Configuration** page, choose **Check Point (r75–r77)** and click **Start Migration**.

Step 2 On the **Configuration Extractor** pane, click **Connect** to the Check Point Security Gateway for which the policies are to be migrated using the Secure Firewall migration tool.

To connect, you require the following information:

a) IP Address
b) Port
c) Admin Username
d) Admin Password
e) Expert Password
f) (Optional) Virtual ID Number

Step 3 Wait until you see a `networking.txt` file downloaded to your local machine.

The following commands are executed in the background by the configuration extractor and is downloaded as the `networking.txt` file:

- **show hostname**
- **show version product**
- **show interfaces**
- **fw vsx stat**
- **show management interface**
- **show configuration bonding**
- **show configuration bridging**
- **show configuration interface**
- **show configuration static-route**
- **show ipv6-state**
- **show configuration ipv6 static-route**
- **netstat -rnv**

For example, 172.16.0.1 is the IP address of Check Point Firewall Gateway for which the policies are to be migrated.

Step 4 If you are trying to export configuration from a Check Point VSX (Virtual System eXtension) version R77 having a virtual ID, the following commands are executed in the background:

- **show hostname**
- **show version product**
- **show interfaces**
- **fw vsx stat**
- **fw vsx stat <vsid>**
- **set virtual system <vsid>**

  Tip
  vsid indicates the virtual system ID.

- **fw getifs**
- **show management interface**
- **show configuration bonding**
- **show configuration bridging**
- **show configuration interface**
- **show configuration static-route**
- **show ipv6-state**

- **show configuration ipv6 static-route**
- **netstat -rnv**

Step 5 Move the .txt file to the `Outputs` folder.

What to do next

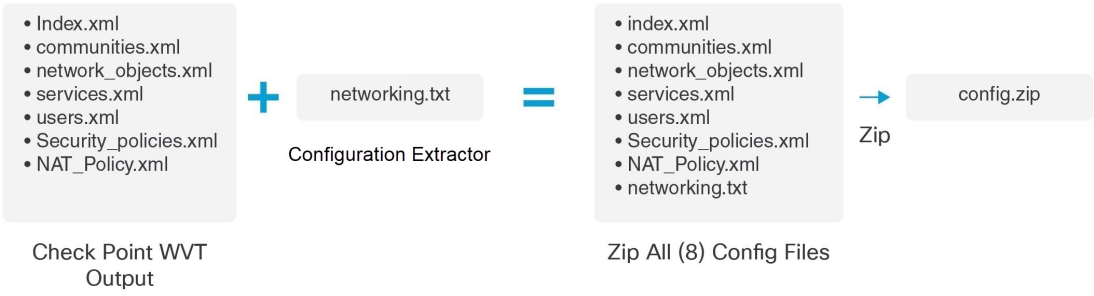
Zip the Exported Files

Zip the Exported Files

Procedure

Select all the eight files (seven from the Web Visualization Tool (WVT) and one .txt file from the Configuration Extractor) and compress them to a zip file.

Note
Before you zip the files for migration, ensure that the `Security_Policy.xml` and `NAT_Policy.xml` files are for the Check Point device that you want to migrate to the threat defense.



Note
.tar or other compressed file types are not supported.

What to do next

Upload the Check Point Configuration File

Run the Migration

Launch the Secure Firewall Migration Tool

This task is applicable only if you are using the desktop version of the Secure Firewall migration tool. If you are using the cloud version of the migration tool hosted on Security Cloud Control, 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
- Review and verify the requirements in the Supported Target Management Center for Migration, on page 26 section.
- Ensure that your computer has a recent version of the Google Chrome browser to run the Secure Firewall migration tool. For information on how to set Google Chrome as your default browser, see Set Chrome as your default web browser.
- If you are planning to migrate a large configuration file, configure sleep settings so the system doesn't go to sleep during a migration push.

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 Check Point configuration to your computer, proceed to Upload the Check Point Configuration File.
- If you must extract information from a Check Point (r77) using the Secure Firewall migration tool, proceed to Export the Check Point Configuration Files for r77.
- If you must extract information from a Check Point (r80-r82) using the Secure Firewall migration tool, proceed to Export the Check Point Configuration Files for r80-r82.

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

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

Export the Check Point Configuration Files for r80-r82

Note Export of Check Point r80-r82 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-r82) Devices for Configuration Extraction using Live Connect
- Procedure to export the Check Point Configuration Files for r80-r82

Pre-Stage the Check Point (r80-r82) 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-r82) 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-r82) 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-r82 Gateway is complete.

For more information, see Figure 3.

Step 2 Create the username and password on the Check Point Security Manager for r80-r82:

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-r82.

What to do next

Export the Check Point Configuration Files for r80-r82

Export from Standalone Check Point Deployment

You must configure the credentials on the Check Point (r80-r82) 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-r82 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-r82.

What to do next

Export the Check Point Configuration Files for r80-r82

Export from Multi-Domain Check Point Deployment

You must configure the credentials on the Check Point (r80-r82) 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**.

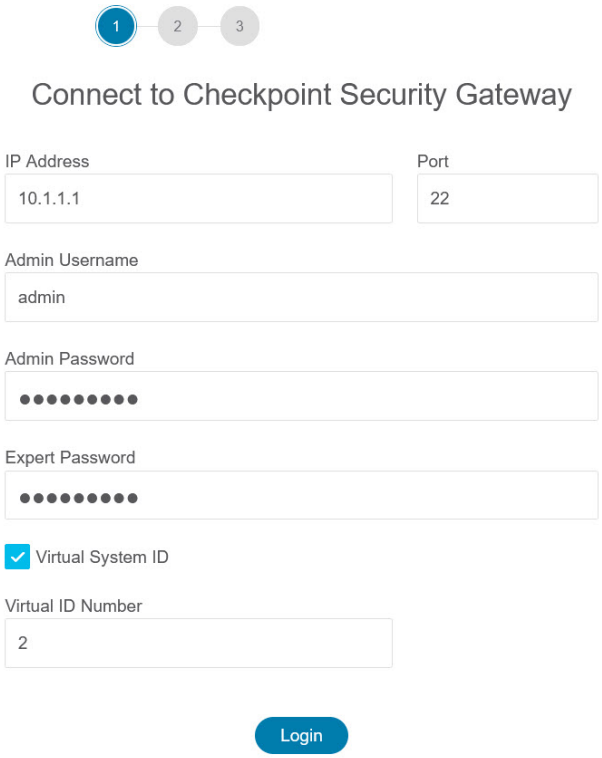
d) SSH into your Check Point Security Gateway and create a new password using the command:

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-r82.

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:

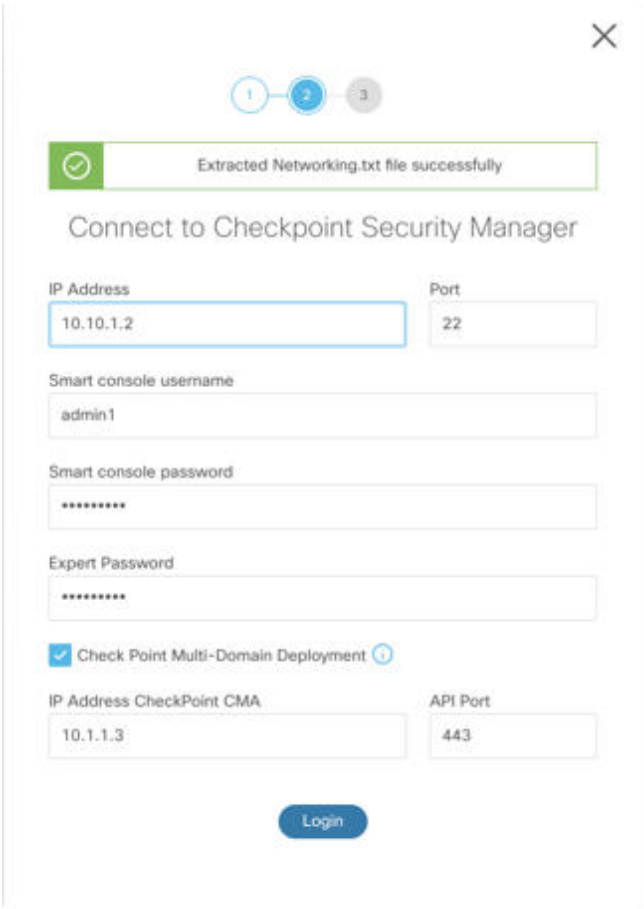
   set expert-password <password>

   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-r82.
- 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-r82

Use a Custom API Port for Check Point (r80-r82) 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-r82

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-r82) devices before migration, see Pre-stage the Check Point (r80-r82) Devices for Configuration Extraction Using Live Connect.

Note

- We recommend that you use Live Connect to extract the Check Point (r80-r82) configurations.
- Using a Check Point (r80-r82) 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-r82, perform the following:

Procedure

Step 1 Select Check Point (r80-r82) from the **Select Source Config** page.

Step 2 Click **Connect**.

Note
Live connect is available for Check Point (r80-r82) only.

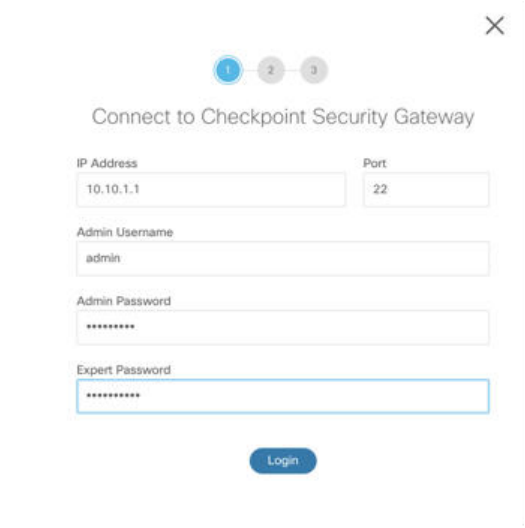
Step 3 Connect to Check Point Security Gateway. Perform the following:

a) Enter the following in the Check Point r80-r82 Security Gateway:

- IP Address
- SSH Port
- Admin Username

- Admin Password
- Expert Password

Figure 3: Connect to Check Point Security Gateway



b) Click **Login**.

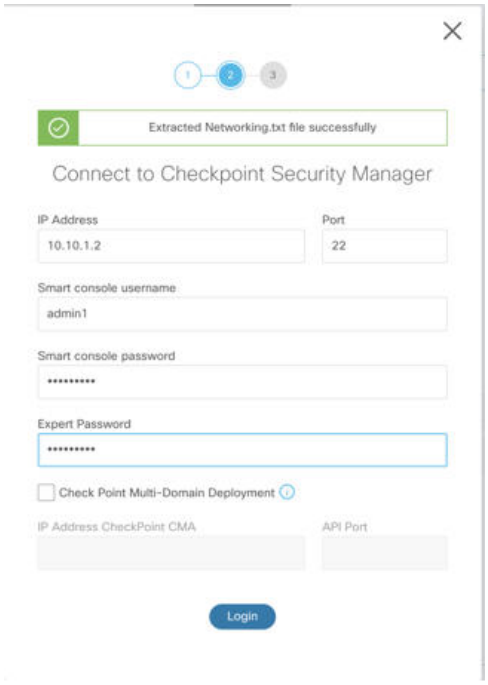
The Secure Firewall migration tool generates the *networking.txt* file that has device-specific configurations such as interface and route configurations. Store the *networking.txt* file in a local directory for the current session of the Secure Firewall migration tool.

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

a) Enter the following in the Check Point r80-r82 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**.

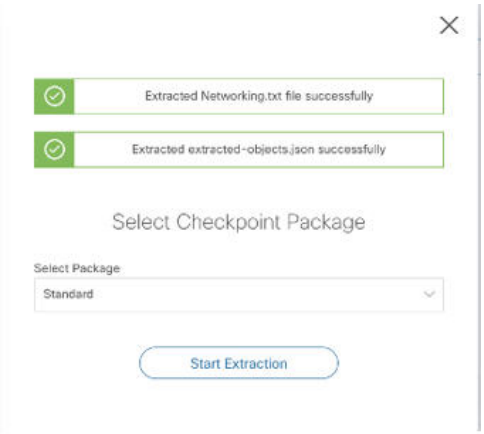
The Secure Firewall migration tool generates the *Extracted-objects.json* file that captures the complete network and service object configuration available in the Check Point Security Manager.

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.

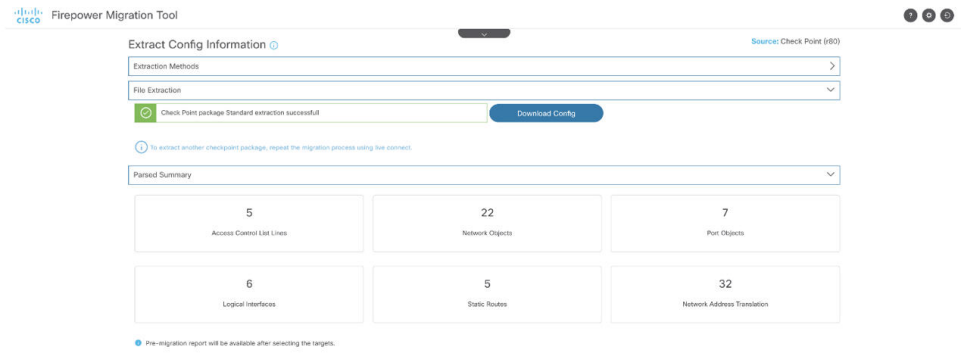
Step 5 Select the Check Point Policy Package that you want to migrate from the **Select Check Point Package** list, and click **Start Extraction**.

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-r82) configuration.

What to do next

Upload the Check Point Configuration File

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-r82) firewall.
- Download the current configuration if you must migrate the extracted Check Point (r80-r82) 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-r82 configuration:

- Perform Live Connect to extract the Check Point (r80-r82) 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.

Upload the Check Point Configuration File

Before you begin

Export the configuration file as .zip format.

Procedure

Step 1 On the **Extract Config Information** screen, in the **Manual Upload** section, click **Upload** to upload the Check Point configuration file.

Step 2 Browse to the location where the configuration file is stored. The configuration file is extracted for Check Point (r77) and downloaded using Live Connect for Check Point (r80-r82). Click **Open**.

The Secure Firewall migration tool uploads the configuration file. For large configuration files, this step takes longer time.

The pre-parsing process is now complete.

The Parsed Summary section displays the parsing status.

Step 3 Review the summary of the elements that the Secure Firewall migration tool detected and parsed in the uploaded configuration file.

Step 4 Click **Next** to select the target parameters.

What to do next

Specify Destination Parameters for the Migration Tool

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) If you want to migrate device-specific configurations like interfaces and routes, add the target Firewall Threat Defense to the Firewall Management Center. See Adding Devices to the Firewall Management Center
- If it requires you to apply IPS or file policy to ACL in the **Review and Validate** page, we highly recommend you create a policy on the Firewall Management Center before migration. Use the same policy, as the Secure Firewall migration tool fetches the policy from the connected Firewall Management Center. Creating a new policy and assigning it to multiple access control lists may degrade the performance and may also result in a push failure.

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) In the **Domain** drop-down list, select the domain to which you are migrating.

   If you want to migrate to a Firewall Threat Defense device, you can only migrate to the Firewall Threat Defense devices available in the selected domain.

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

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

a) Click the **Cloud-delivered FMC** radio button.
b) Choose the region and paste the 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 Click **Proceed**.

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 Check Point configuration.

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

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

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

Check Point firewall migration to Firewall Management Center or Firewall Threat Defense 6.7 or later with the Remote deployment enabled is supported by the Secure Firewall migration tool. Migration of Interface and Routes must be done manually.

- 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 Check Point 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 the Check Point configuration in the **Device Configuration**, **Shared Configuration**, and **Optimization** sections. You can further modify the default selection, according to your requirements.
- For Check Point, under **Shared Configuration**, select the relevant **Access Control** option:
  - Global Policy—When you select this option, the source, and destinations zone for the ACL policy are migrated as **Any**.
  - Zone-Based Policy—When you select this option, source, and destination zones are derived based on the predicative route-lookup through routing mechanism for the source and destination network objects or groups.

    Note

Route-lookup is limited to Static routes and Dynamic routes (PBR and NAT are not considered) and depending on the nature of the source and destination Network Object-Groups, this operation may result in rule explosion.

The routing information is obtained from the `networking.txt` file. This file is the output of the FMT-CP-Config-Extractor_v4.0.1-8248 Tool that uses **netstat -rnv** command to gather the routing table. For more information, see Export Device Configuration Using FMT-CP-Config-Extractor_v4.0.1-8248 Tool.

IPv6 Route-lookup for Zone-Based policies is not supported in this release. Ensure that all the rules of the Global Policy or of the Zone-Based Policy are migrated successfully.

Under **Device Configuration**, choose interfaces, routes, and site-to-site VPN tunnel configurations to be migrated from your Check Point firewall. Note that you can migrate only a policy-based (cryptomap) site-to-site VPN tunnel configuration.

- (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 Check Point 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 53

Review the Pre-Migration Report

Procedure

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

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

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

Note

Each table in the pre-migration report displays 30 entries. For more than 30 entries, you must download the CSV file by clicking the icon on top-right of the table.

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

- **Overall Summary**—Overall summary of the supported Check Point configuration elements that can be successfully migrated to Firepower Threat Defense. For example, Policy Names, Rule Counts etc.
- **Configuration Lines with Errors**—Information about Check Point configuration elements that couldn't be migrated successfully due to parsing issues by the Migration Tool. Rectify these errors in the Check Point device, generate a new configuration file, and upload this file to the Migration Tool before proceeding with the migration.
- **Ignored Configuration**—List of all the Check Point configuration elements that are ignored by FMT during migration and will not be carried forward to the target system.

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

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

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

Map Check Point Firewall Configurations with Firewall Threat Defense Interfaces

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

On the **Map FTD Interface** screen, the Secure Firewall migration tool retrieves a list of the interfaces on the Firewall Threat Defense device. By default, the Secure Firewall migration tool maps the interfaces in Check Point and the Firewall Threat Defense device according to their interface identities. For example, the 'management-only' interface on the Check Point interface is automatically mapped to the 'management-only' interface on the Firewall Threat Defense device and is unchangeable.

The mapping of Check Point interface to the Firewall Threat Defense interface differs based on the Firewall Threat Defense device type:

- If the target Firewall Threat Defense is of native type:
  - The Firewall Threat Defense must have equal or a greater number of used Check Point interfaces or port channel (PC) data interfaces (excluding management-only and subinterfaces in the Check Point configuration). If the number is less, add the required type of interface on the target Firewall Threat Defense.
  - Subinterfaces are created by the secure Firewall migration tool based on physical interface or port channel mapping.
- If the target Firewall Threat Defense is of container type:

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

Before you begin

Make sure you have connected to the Firewall Management Center and chosen the destination as Firewall Threat Defense. For more information, see Specify Destination Parameters for the Secure Firewall Migration Tool, on page 50.

Note This step is not applicable if you are migrating to a Firewall Management Center without a Firewall Threat Defense device.

Procedure

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

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

You do not need to map subinterfaces. The Secure Firewall migration tool maps subinterfaces on the Firewall Threat Defense device for all subinterfaces in the Check Point configuration.

Step 2 When you have mapped each Check Point interface to a Firewall Threat Defense interface, click **Next**.

What to do next

Map the Check Point interfaces to the appropriate Firewall Threat Defense interface objects, security zones, and interface groups. For more information, see Map Check Point Interfaces to Security Zones and Interface Groups.

Map Check Point Interfaces to Security Zones and Interface Groups

To ensure that the Check Point configuration is migrated correctly, map the Check Point interfaces to the appropriate Firewall Threat Defense interface objects, security zones and interface groups. In an Check Point configuration, access control policies and NAT policies use interface names (nameif). In Firewall Management Center, those policies use interface objects. In addition, Firewall Management Center policies group interface objects into the following:

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

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

Procedure

Step 1 On the **Map Security Zones and Interface Groups** screen, review the available interfaces, security zones, and interface groups.

Step 2 To map interfaces to security zones and interface groups that exist in Firewall Management Center, or that is available in configuration files as Security Zone type objects and is available in the drop-down list, do the following:

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

Step 3 To map interfaces to security zones and interface groups that exist in Firewall Management Center, or that is available in Check Point (r80-r82) configuration files as Security Zone type objects and is available in the drop-down list, do the following:

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

Step 4 You can manually map or auto-create the security zones and interface groups.

Step 5 To map the security zones and interface groups manually, perform the following:

a) Click **Add SZ & IG**.
b) In the **Add SZ & IG** dialog box, click **Add** to add a new security zone or Interface Group.
c) Enter the security zone name in the **Security Zone** column. The maximum characters allowed is 48. Similarly, you can add an interface group.
d) Click **Close**.

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

a) Click **Auto-Create**.
b) In the **Auto-Create** dialog box, check one or both of **Interface Groups** and **Zone Mapping**.
c) Click **Auto-Create**.

The Secure Firewall migration tool gives these security zones the same name as the Check Point interface, such as **outside** or **inside**, and displays an "(A)" after the name to indicate that it was created by the Secure Firewall migration tool. The interface groups have an `_ig` suffix added, such as **outside_ig** or **inside_ig**. In addition, the security zones and interface groups have the same mode as the Check Point interface. For example, if the Check Point logical interface is in L3 mode, the security zone and interface group that is created for the interface is also in L3 mode.

Step 6 When you have mapped all interfaces to the appropriate security zones and interface groups, click **Next**.

Optimize, Review and Validate the Configuration

Before you push the migrated Check Point 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.



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

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

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

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

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



Note By default, the Inline Grouping option is enabled.

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

Secure Firewall Migration Tool ACL Optimization Overview

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

The ACL optimization supports the following ACL types:

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

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

- 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 Check Point 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

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

Object Optimization

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

- Unreferenced objects—You can choose not to migrate unreferenced objects at the beginning of the migration.
- Duplicate objects—If an object already exists on Firewall Management Center, instead of creating a duplicate object, the policy is reused.
- Inconsistent objects—If there are objects with similar names but different content, the object names are modified by the Secure Firewall migration tool before the migration push.

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) To download the identified ACL optimization rules, click **Download Report**.
b) Select rules and choose **Actions** > **Migrate as disabled** or **Do not migrate** and apply one of the actions.
c) 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.

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 Check Point configuration file. For example, if a Check Point 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.

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 apply a Firewall Management Center file policy to one or more access control policies, check the box for the appropriate rows, choose **Actions** > **File Policy**.

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

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

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

g) 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.

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

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

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

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

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

Step 3 Click the following tabs and review the configuration items:

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

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

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

Step 6 For configurations containing several site-to-site VPN tunnel configurations, to update the preshared keys for multiple entries at once, follow the steps below:

- Select the site-to-site VPN configuration entries for which you want to update the preshared keys.
- Click download () to export the table to an editable Excel sheet.
- Enter the preshared keys in the respective columns against each VPN configuration and save the file. For VPN configurations containing both IKEv1 and IKEv2 versions of IKE, ensure you enter two values in the column separated by a comma.
- Click upload (). The migration tool reads the entries in the Excel and automatically adds them to the corresponding preshared key columns of the VPN configurations.

Note
To update a preshared key that was missed to be updated as part of the bulk update, use the default method of selecting the entry and choosing **Actions** > **Update Pre-Shared Key** or export the Excel, update the key, and import it.

If the target threat defense device already has a site-to-site VPN topology configured, the migration tool detects it and prompts you to choose if you want to delete it. If you choose to delete it, the migration tool deletes it for you, without you having to log in to the management center to manually delete it. If you choose **No**, you need to manually delete any existing VPN configurations on the target threat defense device to continue the migration.

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

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

During validation, the Secure Firewall migration tool connects to 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 9 When the validation is complete, if the **Validation Status** dialog box shows one or more object conflicts, do the following:

a) Click **Resolve Conflicts**.

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

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

For example, you might be prompted to add a suffix to the object name to avoid a conflict with the existing 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 10 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 11 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 62.

Push the Migrated Configuration to Firewall Management Center

You cannot push the migrated Check Point 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 Check Point 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 for Check Point and Complete the Migration

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 ASA configuration was migrated:

Note
Each table in the pre-migration report displays 30 entries. For more than 30 entries, you must download the CSV file by clicking the icon on top-right of the table.

- **Migration Summary**—A summary of the configuration that was successfully migrated from Check Point to Firepower Threat Defense.

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

- **Selective Policy Migration**—Details of the specific Check Point features selected for migration and Interface Mapping are available.

- **Migration Conversions**—Conversion and push details which includes the following:
  - Network/Service object handling
  - List of partially migrated configurations with reasons
  - List of Unsupported configurations with reason
  - Expanded Access Control Rules

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: Check Point 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 66

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 Use the Check Point Web Visualization Tool and FMT-CP-Config-Extractor_v4.0.1-8248 Tool to collect the Check Point device configurations that you are trying to migrate and save a copy of the Check Point configuration files.

Step 2 Review the Check Point configuration zip file.

Step 3 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 4 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 5 (Optional) If your source Check Point configuration has bond interfaces, create port channels (EtherChannels) on the target Firepower 2100 series device.

For more information, see Configure EtherChannels and Redundant Interfaces.

Step 6 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 31.

Step 7 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 50.

Step 8 Map the Check Point interfaces with the Firewall Threat Defense interfaces.

Note
The Secure Firewall migration tool allows you to map an Check Point interface type to the Firewall Threat Defense interface type.

For example, you can map a bond interface in Check Point to a physical interface in Firewall Threat Defense.

For more information, see Map the Check Point Interfaces with Threat Defense Interfaces.

Step 9 While mapping logical interfaces to security zones, click **Auto-Create** to allow the Secure Firewall migration tool to create new security zones. To use existing security zones, manually map the Check Point logical interfaces to the security zones.

For more information, see Map Check Point Logical Interfaces to Security Zones and Interface Groups.

Step 10 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 11 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 for Check Point and Complete the Migration, on page 63.

Step 12 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 64.

Procedure

Step 1 Connect to the Check Point Security Gateway through the Gaia Console.

Step 2 Shutdown the Check Point interfaces of intended Security Gateway through the Gaia console.

Step 3 (Optional) Access the Firewall Management Center and configure dynamic routing, platform settings, and other features that are not migrated by the Secure Firewall migration tool that are needed manually for the Firepower 2100 series device.

Step 4 Clear the Address Resolution Protocol (ARP) cache on the surrounding switching infrastructure.

Step 5 Perform basic ping tests from surrounding switching infrastructure to the Firepower 2100 series device interface IP addresses, to make sure that they are accessible.

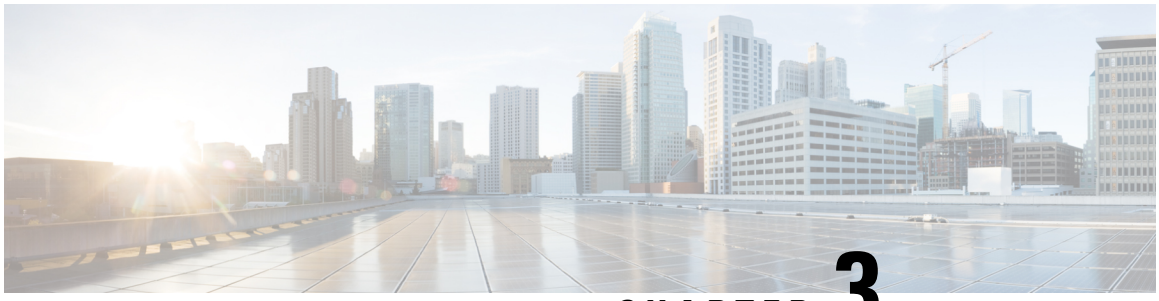
Step 6 Perform basic ping tests from devices which require layer 3 routing to Firepower 2100 series device interface IP addresses.

Step 7 If you are assigning a new IP address to the Firepower 2100 series device and not reusing the IP address assigned to the Check Point 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 8 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 67

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 Check Point 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 2: 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 3: Extensive Telemetry

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

Table 4: Source Check Point Information

Data Point	Description	Example Value
Time	The time and date when the telemetry data is collected	2023-04-25 10:39:19
Source Type	The source device type	Check Point
Source Device Serial Number	Serial number of Check Point	Serial number of device if exists.
Source Device Model Number	Model number of Check Point	
Source Device Version	Version of Check Point	R77.30
Source Config Counts	The total number of lines in the source configuration	504
Firewall Mode	The firewall mode configured on Check Point - routed or transparent	ROUTED
Context Mode	The context mode of Check Point. This can be single or multi-context.	SINGLE
Check Point Config Statistics:		
ACL Counts	The number of ACLs which are attached to access group	46

Data Point	Description	Example Value
Access Rules Counts	The total number of access rules	46
NAT Rule Counts	The total number of NAT rules	17
Network Object Counts	The number of network objects configured in Check Point	34
Network Object Group Counts	The number of network object groups in Check Point	6
Port Object Counts	The number of port objects	85
Port Object Group Counts	The number of port object groups	37
Unsupported Access Rules Count	The total number of unsupported access rules	3
Unsupported NAT Rule Count	The total number of unsupported NAT access rules	0
FQDN Based Access Rule Counts	The number of FQDN -based access rules	7
Time range Based Access Rule Counts	The number of time range based access rules	1
SGT Based Access Rule Counts	The number of SGT-based access rules	0
Summary of Config lines that Tool is not able to parse		
Unparsed Config Count	The number of config lines that are unrecognized by the parser	68
Total Unparsed Access Rule Counts	The total number of unparsed access rules	3

Table 5: Target Management Device (Firewall Management Center) Information

Data Point	Description	Example Value
Target Management Version	The target version of Firewall Management Center	6.2.3.3 (build 76)
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
Migration Tool Version	The version of the migration too1	1.1.0.1912

Table 6: Migration Summary

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

Table 7: Secure Firewall Migration Tool Performance Data

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

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

Telemetry Check Point Example File for r77

The following is an example of a telemetry data file on the migration of Check Point configuration to Firewall Threat Defense:


```
{
  "metadata": {
    "contentType": "application/json",
    "topic": "migrationtool.telemetry"
  },
  "payload": {
    "Check Point_config_stats": {
      "Ipv6_access_rule_counts": 0,
      "Ipv6_bgp_count": 0,
      "Ipv6_nat_rule_count": 0,
      "Ipv6_network_counts": 24,
      "Ipv6_static_route_counts": 6,
      "access_rules_counts": 63,
      "acl_counts": 63,
      "fqdn_based_access_rule_counts": 0,
      "nat_rule_counts": 0,
      "network_object_counts": 143,
      "network_object_group_counts": 31,
      "no_of_fqdn_based_objects": 0,
      "ospfv3_count": 0,
      "port_object_counts": 370,
      "port_object_group_counts": 55,
      "sgt_based_access_rules_count": 0,
      "timerange_based_access_rule_counts": 0,
      "total_unparsed_access_rule_counts": 0,
      "tunneling_protocol_based_access_rule_counts": 0,
      "unparsed_config_count": 15,
      "unsupported_access_rules_count": 0,
      "unsupported_nat_rule_count": 0
    },
    "context_mode": "SINGLE",
    "error_description": null,
    "error_message": null,
    "firewall_mode": "ROUTED",
    "log_info_acl_count": 0,
    "migration_status": "SUCCESS",
    "migration_summary": {
      "access_control_policy": [
        [
          {
            "access_rule_counts": 63,
            "apply_file_policy_rule_counts": 0,
            "apply_ips_policy_rule_counts": 0,
            "apply_log_rule_counts": 0,
            "do_not_migrate_rule_counts": 0,
```

```
            "enable_Global-ACL-Policy": true,
            "enable_Zone-Specific-ACL-Policy": false,
            "enable_hit_count": false,
            "expanded_acp_rule_counts": 1,
            "name": "FTD-Mig-1566804327",
            "partially_migrated_acl_rule_counts": 0,
            "update_rule_action_counts": 0
          }
        ]
      ],
      "interface_counts": 12,
      "interface_group_counts": 0,
      "interface_group_manually_created_counts": 0,
      "nat_Policy": [
        [
          {
            "NAT_rule_counts": 0,
            "do_not_migrate_rule_counts": 0,
            "name": "Doesn't Exist",
            "partially_migrated_nat_rule_counts": 0
          }
        ]
      ],
      "network_object_rename_counts": 0,
      "network_object_reused_counts": 0,
      "object_group_counts": 15,
      "objects_counts": 54,
      "port_object_rename_counts": 0,
      "port_object_reused_counts": 5,
      "security_zone_counts": 13,
      "security_zone_manually_created_counts": 0,
      "static_routes_counts": 22,
      "sub_interface_counts": 11
    },
    "migration_tool_version": "2.0.3169",
    "rule_change_acl_count": 0,
    "source_config_counts": 0,
    "source_device_model_number": "Check Point Model Not Exists",
    "source_device_serial_number": null,
    "source_device_version": "R77.30",
    "source_type": "Check Point",
    "system_information": {
      "browser": "Chrome/76.0.3809.100",
      "operating_system": "Windows NT 10.0; Win64; x64"
    },
    "target_device_model": "Cisco Firepower 9000 Series SM-24 Threat Defense",
    "target_device_version": "76",
    "target_management_type": "6.4.0.4 (build 31)",
    "target_management_version": "6.4.0.4 (build 31)",
    "template_version": "1.1",
    "time": "2019-08-26 12:55:40",
    "tool_analytics_data": {
      "objectsplit_100_count": 0
    },
    "tool_performance": {
      "config_push_time": 725,
      "conversion_time": 29,
      "migration_time": 1020
    }
  },
  "version": "1.0"
}
```

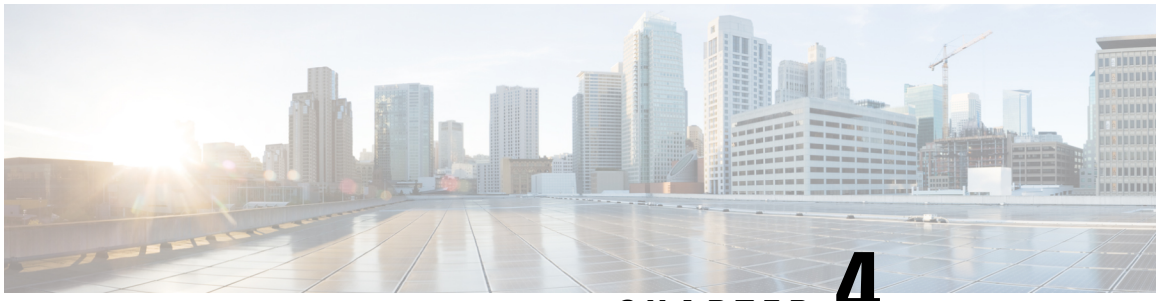
Telemetry Check Point Example File for r80

The following is an example of a telemetry data file on the migration of Check Point configuration to Firewall Threat Defense :


```
{
"Check Point_config_stats":{
        "Ipv6_access_rule_counts":0,
        "Ipv6_bgp_count":0,
        "Ipv6_nat_rule_count":0,
        "Ipv6_network_counts":3,
        "Ipv6_static_route_counts":0,
        "access_rules_counts":726,
        "acl_category_count":0,
        "acl_counts":726,
        "fqdn_based_access_rule_counts":0,
        "nat_rule_counts":335,
        "network_object_counts":7645,
        "network_object_group_counts":268,
        "no_of_fqdn_based_objects":0,
        "port_object_counts":1051,
        "port_object_group_counts":66,
        "s2s_vpn_tunnel_counts":0,
        "sgt_based_access_rules_count":0,
        "timerange_based_access_rule_counts":0,
        "total_unparsed_access_rule_counts":0,
        "tunneling_protocol_based_access_rule_counts":0,
        "unparsed_config_count":234,
        "unsupported_access_rules_count":0,
        "unsupported_nat_rule_count":0},
        "context_mode":"SINGLE",
        "error_description":"No data.",
        "error_message":"push failed for object network",
        "firewall_mode":"ROUTED",
        "log_info_acl_count":0,
        "migration_status":"FAIL",
        "migration_summary":{
          "access_control_policy":[
           [
           {
               "access_rule_counts":0,
               "apply_file_policy_rule_counts":0,
               "apply_ips_policy_rule_counts":0,
               "apply_log_rule_counts":0,
               "do_not_migrate_rule_counts":0,
               "enable_Global-ACL-Policy":true,
               "enable_Zone-Specific-ACL-Policy":false,
               "enable_hit_count":false,
               "expanded_acp_rule_counts":1,
               "name":"Doesn't Exist",
               "partially_migrated_acl_rule_counts":0,
               "total_acl_element_counts":389416,
               "update_rule_action_counts":0
            }
        ]
        ],
        "interface_counts":11,
        "interface_group_counts":0,
        "interface_group_manually_created_counts":0,
        "nat_Policy":[
        [
            {
                "NAT_rule_counts":0,
                "do_not_migrate_rule_counts":0,
```

```
        "name":"Doesn't Exist",
        "partially_migrated_nat_rule_counts":0
    }
]
],
"network_object_rename_counts":0,
"network_object_reused_counts":0,
"object_group_counts":222,"objects_counts":7148,
"port_object_rename_counts":2,
"port_object_reused_counts":30,
"prefilter_control_policy":[
   [
     {
        "do_not_migrate_rule_counts":0,
        "name":null,
        "partially_migrated_acl_rule_counts":0,
        "prefilter_rule_counts":0
      }
    ]
    ],
"security_zone_counts":11,
"security_zone_manually_created_counts":0,
"static_routes_counts":0,
"sub_interface_counts":8,
"time_out":false},
"migration_tool_version":"2.1.4283",
"mtu_info":{"interface_name":null,
"mtu_value":null},
"rule_change_acl_count":0,
"selective_policy":
        {
        "acl":true,
        "acl_policy":true,
        "application":false,
        "csm":false,
"interface":true,
"interface_groups":true,
"migrate_tunneled_routes":false,
"nat":true,
"network_object":true,
"policy_assignment":true,
"populate_sz":false,
"port_object":true,
"routes":true,
"security_zones":true,
"unreferenced":true},
"source_config_counts":0,
"source_device_model_number":"Check Point Model Not Exists",
"source_device_serial_number":null,
"source_device_version":"R77.30",
"source_type":"Check Point",
"system_information":
{
"browser":"Chrome/80.0.3987.163","operating_system":
"Macintosh; Intel Mac OS X 10_15_4"},
"target_device_model":"Cisco Firepower 4110 Threat Defense",
"target_device_version":"76",
"target_management_type":"6.5.0 (build 63)",
"target_management_version":"6.5.0 (build 63)",
"template_version":"1.1",
"time":"2020-04-16 04:50:05",
"tool_analytics_data":{"objectsplit_100_count":6},
"tool_performance":
        {
```

```
                    "config_push_time":1457,
                    "conversion_time":279,
                    "migration_time":2637
                }
            }
```



CHAPTER 4

Troubleshooting Migration Issues

- Troubleshooting for the Secure Firewall Migration Tool, on page 77
- Logs and Other Files Used for Troubleshooting, on page 78
- Troubleshooting Check Point File Upload Failures, on page 78

Troubleshooting for the Secure Firewall Migration Tool

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

Some of the common scenarios where the migration process fails for a Check Point configuration are:

- Files missing from the Check Point Config.zip.
- Invalid files are detected by the Secure Firewall migration tool in the Check Point Cofig.zip
- If the Check Point configuration file is of any compressed file type other than .zip.

Secure Firewall Migration Tool Support Bundle

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

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

   The Help support page appears.

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

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

3. Click **Download**.

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

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

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

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

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

Logs and Other Files Used for Troubleshooting

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

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

Troubleshooting Check Point File Upload Failures

If the Check Point configuration file fails to upload, the reason is typically because the Secure Firewall migration tool could not parse one or more lines in the file.

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

- Unparsed file—Look at the end of the file to identify the last ignored line of the Check Point configuration file that was successfully parsed.
- Unexpected file—Invalid files detected for Check Point. For example, when zipped using Mac OS, Mac system files are created. Remove the Mac files.
- (For r75–r77.30 only) Incorrectly named files—When Security Policy and NAT Policy files are not named correctly for Check Point. Rename ACL and NAT files correctly.
- Missing files—Some files are missing from the Check Point config.zip file. Add the required files.

Note For r77, manually extract the missing configuration file. For more information, see Export the Check Point Configuration Files for r77.

For r80-r82, use Live Connect to extract the correct configuration file for the secure Firewall migration tool. For more information, see Export the Check Point Configuration Files for r80-r82.

Troubleshooting Example for Check Point: Cannot Find Member of Object Group (For r75–r77.30 Only)

In this example, the Check Point configuration file upload and parsing failed because of error in the configuration of an element.

Procedure

Step 1 Review the error messages to identify the problem.

This failure generates the following error messages:

Location	Error Message
Secure Firewall migration tool message	Check Point config files parsed with errors. See the Pre-Migration Report error section for parsing errors and Post-Migration Report for push errors that occurs during the push stage.
Log file	[ERROR | objectGroupRules] > "ERROR, SERVICE_GROUP_RULE not applied for port-group object [services_epacity_nt_abc] as CheckPoint object [ica] does not exist in <service> table;" [INFO | objectGroupRules] > "Parsing object-group service:[services_gvxs06]" [INFO | objectGroupRules] > "Parsing object-group service:[services_iphigenia]" [INFO | objectGroupRules] > "Parsing object-group service:[Services_KPN_ISP]"

Step 2 Open the Check Point `services.xml` file.

Step 3 Search the object-group with name as services_gvxs06.

Step 4 Create the missing member for the object-group using the smart dashboard.

Step 5 Export the configuration file again. For more information, see Export the Check Point Configuration Files.

Step 6 If there are no more errors, upload the new Check Point configuration zip file to the Secure Firewall migration tool and continue with the migration.

Troubleshooting Example for Check Point (r80-r82) for Live Connect

Example 1: Request details on Check Point Security Manager.

In this example, the Secure Firewall migration tool requests the details for Check Point Security Manager.

Review the error messages to identify the problem. This failure generates the following error messages:

Location	Error Message
Secure Firewall migration tool message	Screen requests to provide details for Check Point Security Manager.
Log file	[ERROR | connect_cp] > "Unable to extract the Extracted-objects.json file due to credentials with insufficient privileges, time-out issues and so on. Refer Secure Firewall migration tool UG for more info." 127.0.0.1 - - [20/Jul/2020 17:20:43] "POST /api/CP/connect HTTP/1.1" 500 -

Incorrect credentials. Follow the steps as mentioned to pre-stage credentials. The credentials used must have a */bin/bash* shell profile on Check Point Gaia for Check Point Security Manager. The same credentials must be staged on Check Point Smart Console Application for Check Point Security Manager with Super User privileges for a normal deployment. The privileges must be Super User if using multi-domain deployment. For more information, see Pre-stage the Check Point (r80-r82) Devices for Configuration Extraction Using Live Connect.

Example 2: Bad File Format

In this example, the Secure Firewall migration tool migration is blocked due to bad file format.

Review the error messages to identify the problem. This failure generates the following error messages:

Location	Error Message
Secure Firewall migration tool message	Blocked
Log file	[ERROR | cp_device_connection] > "Bad file format" 2020-07-20 17:10:57,347 [ERROR | connect_cp] > "Unable to download .tar file." 127.0.0.1 - - [20/Jul/2020 17:10:57] "GET /api/CP/generate_tar_file?package=Standard HTTP/1.1" 500 -

Incorrect credentials. Follow the steps as mentioned to pre-stage credentials. The credentials used must have a */bin/bash* shell profile on Check Point Gaia for Check Point Security Manager. The same credentials must be staged on Check Point Smart Console Application for Check Point Security Manager with Super User privileges. The Super User privileges must be granted if using multi-domain deployment. For more information, see Pre-stage the Check Point (r80-r82) Devices for Configuration Extraction Using Live Connect.

Example 3: Blocked VSX Feature is UNSUPPORTED in Threat Defense

In this example, the Secure Firewall migration tool migration fails due to the blocked VSX feature in the threat defense.

Review the error messages to identify the problem. This failure generates the following error messages:

Location	Error Message
Secure Firewall migration tool message	Blocked VSX Feature is UNSUPPORTED in FTD.

Location	Error Message
Log file	[ERROR | config_upload] > "VSX Feature is UNSUPPORTED in FTD" Traceback (most recent call last)

Problem Description–This error occurs as the **fw vsx stat** command is deprecated starting with Check Point r80.40.

As a workaround, follow these steps:

1. Unzip the *config.zip* file.
2. Open the *networking.txt* file.

   Here is an example of the sample output:

   ```
   firewall> fw vsx stat
   Deprecated command, Please see sk144112 for alternative
   Deprecated commands: cphaprob cpinfo cplic fw ips raidconfig fwaccel
   ```

   Replace this manually as follows:

   ```
   firewall> fw vsx stat
   VSX is not supported on this platform
   ```

3. Select all the files and compress them to .zip extension.