Migrating Palo Alto Networks Firewall to Cisco Secure Firewall Threat Defense Using Firewall Migration Manager

Firewall Migration Manager
Updated September 1, 2026

© 2026 Cisco Systems, Inc. All rights reserved.

Abbreviated Cisco Trademarks

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)

Topics included

1 About Firewall Migration Manager.....5
Overview of Firewall Migration Manager.....6
Features in Firewall Migration Manager.....7
Default home page of Firewall Migration Manager.....10
How Palo Alto Networks Firewall to Firewall Threat Defense migration works.....11

2 Migration Requirements.....13
License requirements.....14
Platform requirements.....14
Device readiness and requirements.....14
Supported platforms and versions.....15
Firewall Management Center requirements.....16
Supported configurations.....16

3 Pre-Migration Tasks.....19
Download the Firewall Migration Manager.....20
Export the configuration from Palo Alto Networks Firewall.....20
Export configuration file from a Palo Alto Networks Firewall (not managed by panorama).....20
Export configuration file from a Palo Alto Networks Firewall (managed by Panorama).....21

4 Palo Alto Networks Firewall to Firewall Threat Defense Workflow.....23
Run the Firewall Migration Manager migration.....24
Upload the Palo Alto Networks Firewall configuration file.....24
Specify destination parameters.....25
Map Palo Alto Networks Firewall configurations with Firewall Threat Defense interfaces.....26
Review and validate the migration configuration.....27
Review the Firewall Migration Manager pre-migration report.....30
Review the Firewall Migration Manager post-migration report.....31

1 About Firewall Migration Manager

Topics:

- Overview of Firewall Migration Manager
- Features in Firewall Migration Manager
- Default home page of Firewall Migration Manager
- How Palo Alto Networks Firewall to Firewall Threat Defense migration works

Introduces the Firewall Migration Manager application and explains how it facilitates the migration process from Palo Alto Networks Firewall to Secure Firewall Threat Defense configurations.

Overview of Firewall Migration Manager

Learn how to use the Firewall Migration Manager to automate and streamline the migration of Palo Alto Networks Firewall configurations to Cisco Secure Firewall Threat Defense.

The Firewall Migration Manager is a network security application that automates the migration of supported Palo Alto Networks Firewall configurations to Cisco Secure Firewall Threat Defense. It parses source configurations, maps features, pushes policies to the Firewall Management Center, and streamlines the migration process for organizations seeking to upgrade their firewall solutions.

Why choose Firewall Migration Manager

Firewall migration may appear simple during planning, but execution is often complicated. Common challenges include configuration dependencies, parsing timeouts on large rule sets, and unexpectedly tight cutover windows. For many organizations these risks delay their security modernization efforts.

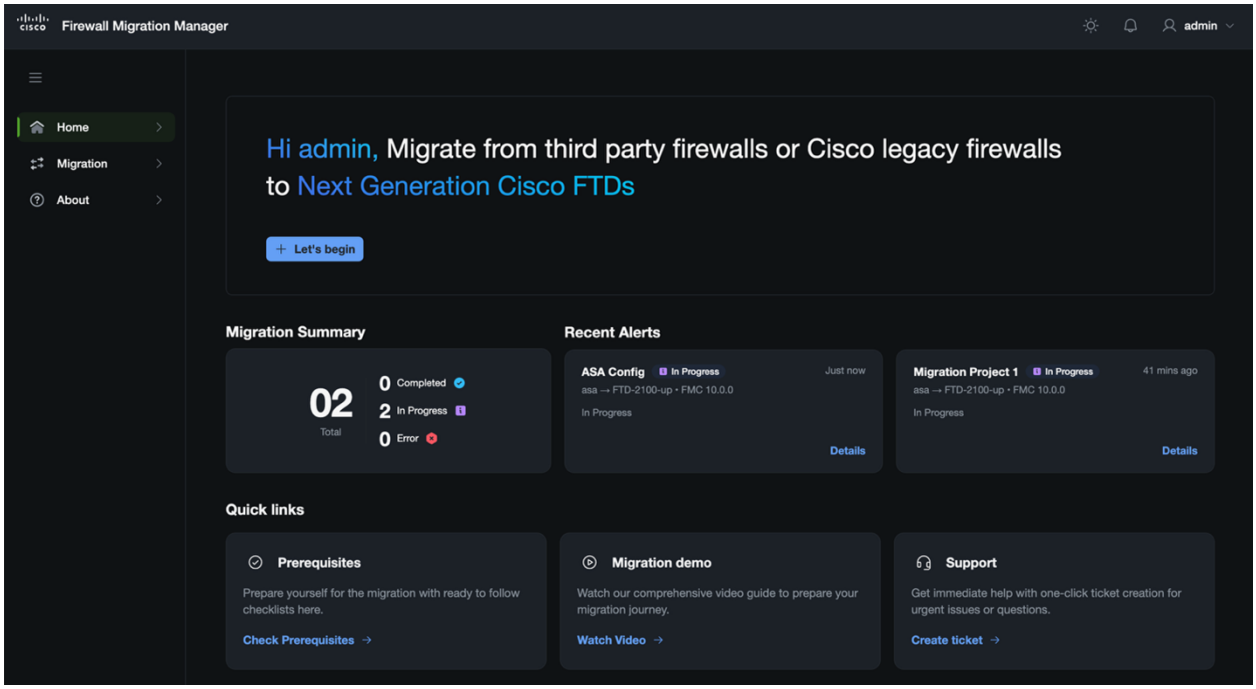
The Firewall Migration Manager an enterprise-ready product built for overcoming these challenges and to migrate seamlessly. The product helps customers and partners by offering predictable timelines, resilient workflows, and clear visibility at every stage of migration to Cisco Secure Firewall Threat Defense. As a result, migration becomes a strategic accelerator rather than a source of friction.

Key features

- **Migration efficiency**: Firewall Migration Manager streamlines and accelerates the firewall migration process while maintaining accuracy and reliability.
- **Improvised GUI**: Use Firewall Migration Manager to replace fragmented manual workflows with a guided, wizard-driven orchestration, visual task tracking, parallel execution, and proactive status monitoring.
- **Pre-deployment validation and testing**: Allows teams to fully evaluate a migration plan before committing to deployment.
- **Enhanced reporting and traceability**: Provides richer migration reports and clearer audit trails, so every stakeholder—from the engineer running the job to Cisco reviewers—has the necessary visibility.
- **Broader platform coverage**: Cisco will continue to expand supported migration sources to include more platforms, helping more teams consolidate onto Cisco Secure Firewall Threat Defense.

Dashboard overview

The Firewall Migration Manager dashboard is a centralized management interface for tracking and troubleshooting network device migrations. It also provides visibility into the health and progress of migration projects.



Key functional areas:

- **Migration monitoring:** The **Migration Summary** tile provides a real-time status overview of all migration tasks and displays counts of completed, in progress, and blocked tasks.
- **Issue identification:** The **Recent Alerts** section helps you diagnose issues. It flags failed migration tasks, identifies the exact stage and cause of failure, and provides a brief explanation of the cause, such as configuration syntax issues or connectivity timeouts.
- **Resource and support hub:** The **Quick links** section provides immediate access to essential onboarding and troubleshooting resources, including:
  - **Prerequisites**: Review the checklist to confirm all prerequisites are met before starting a migration.
  - **Migration demo**: Watch the comprehensive video that guides you through your migration journey.
  - **Support**: Get immediate help with one-click ticket creation for urgent issues or questions.

Features in Firewall Migration Manager

Learn about the new features introduced in Firewall Migration Manager, including automated workflows, centralized dashboard monitoring, and intelligent configuration parsing. These features streamline the migration of legacy firewall configurations to Secure Firewall Threat Defense, improving visibility and efficiency throughout your transition process.

This table summarizes the new features in Firewall Migration Manager.

Release	Features	Details
10.0.1	Support for Palo Alto Networks Firewall to Firewall Threat Defense migration.	Firewall Migration Manager supports migration of the Palo Alto Networks Firewall configurations to a Firewall Threat Defense device.
	Enhanced pre-migration and post-migration reports.	Firewall Migration Manager offers enhanced pre-migration and post-migration reports for improved user experience and easier analysis of migrated configurations.
	Support for migration from layer 2 to layer 3 interfaces.	Firewall Migration Manager supports migration from layer 2 to layer 3 interfaces by converting compatible interface configurations to routed interfaces on the Firewall Threat Defense device.
	Support for VRF migration	Firewall Migration Manager offers migration support for VRFs.
	Support for BGP migration	Firewall Migration Manager offers migration support for BGP.
	Mapping of NAT zones based on the routing table	Firewall Migration Manager uses the routing table to derive NAT zone mappings during migration.
	Handling multiple IP addresses across interfaces	During migration, if a Palo Alto Networks Firewall interface has multiple IP addresses, the Firewall Migration Manager wizard prompts you to choose one IP address for the interface.
	Migration of policy hierarchy from Panorama	Firewall Migration Manager migrates the Palo Alto Networks Firewall policy hierarchy as nested access control policies in a Firewall Threat Defense device.
	Migration of external dynamic lists	Firewall Migration Manager supports migration of external dynamic lists.
	Support for bulk addition of applications in access policy rules.	Firewall Migration Manager supports bulk addition of applications in access policy rules during migration. This reduces the manual effort required to update application-based access policies after migration.

Release	Features	Details
10.0.0	Support for ASA to Firewall Threat Defense migration.	Firewall Migration Manager supports the migration of ASA configurations to a Firewall Threat Defense device.
	Auto-detection of target versions	Automatically identifies target device version and information for Firewall Management Center and Firewall Threat Defense to ensure accurate configuration alignment.
	Automated migration workflow	The Firewall Migration Manager reduces manual effort with automated transition of security policies, network objects, and device configurations from your existing environment to a Firewall Threat Defense device.
	Centralized dashboard support	The Firewall Migration Manager dashboard provides a unified, intuitive interface to streamline your migration journey. Designed to improve visibility and operational efficiency, the dashboard offers these capabilities: ▪ Migration overview: Monitor the status of all your migration projects in real-time and include counts for completed, in-progress, and error-state migrations. ▪ Proactive alerting: Stay informed with immediate visibility into recent migration alerts and project details. ▪ Quick links: Access critical resources directly from the dashboard, including pre-migration checklists, comprehensive video guides, and one-click support ticket creation. This centralized approach simplifies the transition from third-party or legacy firewalls to next-generation Cisco firewall platforms, ensuring a more organized streamlined migration process.
	Improved GUI	The Firewall Migration Manager offers an improved graphical user interface that unifies migration tasks in a wizard-driven orchestration platform. It prioritizes visual clarity, parallel task processing, and proactive status monitoring.
	Intelligent parsing	This feature automatically scans your configurations to identify items that are either unsupported or unreferenced. This helps you save time by focusing your manual cleanup efforts only on the items that require attention. This tool parses enterprise-scale configurations efficiently, handling thousands of rules in minutes.
	Migration history retention	Keeps migration history across different projects so you can track and revisit previous migrations.

Release	Features	Details
	Parallel migration support	To improve efficiency, this feature allows you to run up to 10 migration processes simultaneously, enabling bulk handling of your network transitions.
	Pause and resume	The Firewall Migration Manager allows tasks to be paused and resumed at any point without data loss. **In-Progress** can be accessed from the **Recent Alerts** tile on the home page or by clicking **Migration** under the main menu.

Default home page of Firewall Migration Manager

Learn how to navigate the Firewall Migration Manager home page to monitor migration status, view recent alerts, access demonstration videos, and request technical support. This overview explains the primary dashboard components and provides guidance on interpreting migration status updates.

After you log in, the Firewall Migration Manager home page is displayed.

The home page has these main areas:

- **Migration summary**: Displays the total number of migrations performed, completed, in progress, and migrations that failed due to errors.
- **Recent Alerts**: Provides real-time status updates for migration tasks. The tile displays the migration project name, migration status, timestamp, and a brief description of the current phase or any action required.
- **Quick links**:
  - **Prerequisites**: Prepare yourself for the migration with ready to follow checklists.
  - **Migration demo**: Provides links to demonstration videos that highlight important capabilities and enhancements introduced in the latest release.
  - **Support**: Offers a one-click ticket creation process for immediate assistance via the **Create ticket** link.

Table 1: Migration Status

Status	Description	Action
In-progress	The migration task is currently active. The description displayed indicates the specific step being executed.	Users can monitor the progress and wait for the migration to complete. Click the **Details** link to go to the migration page.
Completed	The migration task has finished successfully.	None
Error	The migration task has failed.	Click the **Details** link to investigate the specific log or configuration issue causing the error.

How Palo Alto Networks Firewall to Firewall Threat Defense migration works

Learn how to migrate your Palo Alto Networks Firewall configurations to Firewall Threat Defense using the Firewall Migration Manager. This workflow covers configuration gathering, parsing, mapping, and validating configurations to ensure a successful transition to your destination device.

Summary

Firewall Migration Manager automates Palo Alto Networks Firewall the configuration migration by ensuring accurate parsing, validation, and deployment of Palo Alto Networks Firewall configurations to Firewall Threat Defense.

Workflow

These stages describe how the Palo Alto Networks Firewall to Firewall Threat Defense migration works:

1. **Gather and parse configuration**: Firewall Migration Manager collects information from the Palo Alto Networks Firewall device and parses its configuration.
2. Map **Palo Alto Networks Firewall configuration, interfaces, security zones to Firewall Threat defense**: Firewall Migration Manager maps interfaces, security zones, and interface groups to a Threat Defense device. You review and validate the mapping.
3. **Review pre-migration report**: Firewall Migration Manager generates a report that identifies unsupported, ignored, and erroneous configurations, including blocking errors and the reasons for them.
4. **Remediate parsing errors**: Firewall Migration Manager highlights parsing errors so that you can resolve them before migration.
5. **Push validated configuration**: Firewall Migration Manager pushes the validated configuration to the Firewall Management Center and migrates the configuration to the destination device.
6. **Review post-migration report**: Firewall Migration Manager generates a detailed report, covering fully migrated, partially migrated, or not migrated configurations. It lists fixes, identifies changes made to avoid conflicts, shows any skipped items, and documents migration failures or manual requirements.

2 Migration Requirements

Topics:

- License requirements
- Platform requirements
- Device readiness and requirements
- Supported platforms and versions
- Firewall Management Center requirements
- Supported configurations

Lists the licensing, platform, device, and configuration requirements for migrating from Palo Alto Networks Firewall to Firewall Threat Defense using the Firewall Migration Manager.

License requirements

Understand the licensing requirements for Firewall Migration Manager and the Firewall Management Center.

While the Firewall Migration Manager is free, ensure that your Management Center is properly licensed for Firewall Threat Defense features to support device registration and policy deployment.

To use Firewall Migration Manager and Firewall Management Center, you must meet these licensing requirements:

- Firewall Management Center must be properly licensed for the Firewall Threat Defense features that you plan to use.
- Proper licensing is required to register Firewall Threat Defense devices and deploy policies to them.

For more information refer to the Licenses section of *Cisco Secure Firewall Management Center Administration Guide*.

Platform requirements

Lists the supported operating systems, browser, and power management settings required for successful Firewall Migration Manager migrations.

The Firewall Migration Manager requires specific platform and configuration settings for proper operation. The supported environments and necessary settings are:

- **System requirements**:
  - Microsoft Windows 11 64-bit or later
  - macOS 14 or later

  You need internet connection to connect to Cisco.com.

  > **Note**
  >
  > If you want to perform migration in an air-gapped or isolated environment without internet access, contact Cisco TAC to obtain the air-gapped Firewall Migration Manager installer.

- **Power management (Windows):**: Set **Sleep** settings in **Power & Sleep** to **Never put the PC to sleep** during migration to prevent interruptions.
- **Power management (macOS)**: Configure **Energy Saver** settings so that the computer and hard disk remain active throughout the migration process.

Device readiness and requirements

Learn about the device requirements and prerequisites for migrating Palo Alto Networks Firewall configurations to Firewall Threat Defense.

When you migrate to the Firewall Management Center, it is not mandatory to have a target Firewall Threat Defense device added to it. You can migrate policies to a Firewall Management Center for future deployment to a Firewall Threat Defense device.

If Firewall Threat Defense device is added to the Firewall Management Center, before starting migration, ensure your target Firewall Threat Defense device meets these criteria:

- **Registration**: The target Firewall Threat Defense device must be registered with the Firewall Management Center.
- **Configuration state**:
  - Supports high availability (HA) configurations.
  - Supports standalone or container instances.
  - **Restriction**: The target Firewall Threat Defense device must not be part of a device cluster.
- **Interface mapping**:
  - If using container instances, the Firewall Threat Defense device must have a minimum interface count (physical, sub-interfaces, and port channels) equal to or greater than the source Palo Alto Networks Firewall device.
  - The Firewall Migration Manager supports mapping across different interface types such as physical interfaces to port channel interfaces.

> **Note**
>
> The Firewall Migration Manager does not create sub-interfaces for target multi-instance Firewall Threat Defense devices. You must pre-configure them on the target device.

> **Warning**
>
> During the push migration, the Firewall Migration Manager automatically cleans and overwrites existing device-specific configurations (routes, interfaces, and so on). We highly recommend manual cleaning of the device prior to migration to avoid unintended data loss.

Supported platforms and versions

Explains the minimum hardware and software requirements needed for successful migration of Palo Alto Networks Firewall to Firewall Threat Defense using Firewall Migration Manager.

For a successful migration, ensure that your hardware and software versions align with these specifications:

Component	Minimum Supported Version
Source PAN-OS	6.1.x and later
Firewall Management Center	6.2.3.3 and later
Target Firewall Threat Defense	6.5 and later

Supported target device

- **Physical**: Firepower 1000, 2100, 4100, 9300 (SM modules), and Secure Firewall 220, 1200, 3100, 3200, 4200, 6100 series

- **Virtual**: Threat Defense on VMware (ESXi/vSphere) and Cloud (Azure/AWS).

Firewall Management Center requirements

Lists the prerequisites for using on-premises Firewall Management Center for Firewall Migration Manager.

The Firewall Migration Manager supports on-premises Firewall Management Center.

Prerequisites for on-premises Firewall Management Center

- **Smart licensing**: Install Smart Licensing for all features being migrated.
- **REST API**: Enabled REST API (**System** (⚙) > **Configuration** > **REST API Preferences**).

> **Note**
>
> You must have an administrator user role in Firewall Management Center to enable REST API. For more information on Firewall Management Center user roles, refer to User Roles.

Supported configurations

Lists the supported Palo Alto Networks Firewall configurations for migration using Firewall Migration Manager.

The Firewall Migration Manager categorizes Palo Alto Networks Firewall configurations based on feature parity with a Firewall Threat Defense device.

Fully supported configurations

- Network objects, groups, and zones (L2/L3/Virtual Wire).
- Service object groups.
- IPv4 and IPv6 FQDN objects, groups, and static routes.
- Access rules, Identity policies, NAT rules, and NAT zones.
- Interfaces:
  - Interface types: Physical, Sub-interfaces (VLAN-mapped), Loopback, Aggregate
  - Migration can handle multiple IP addresses across interfaces
  - Migration from layer 2 to layer 3 interfaces.
- Support for VRF and BGP migration
- Migration of policy hierarchy from Panorama
- Migration of external dynamic lists
- Bulk addition of applications in access rules

Partially supported configurations

- **Access Control Rules**: Migrated without advanced profile options (configure manually post-migration).
- **Service groups**: Mixed protocol groups containing TCP, UDP, and SCTP (SCTP is removed).
- **Object groups**: Mixed valid and invalid objects (invalid objects are stripped).
- **Dynamic objects**: Firewall Migration Manager do not support object groups.
- **Geolocation-based rules**

Unsupported configurations

- Time-based ACLs, and wildcard FQDNs.
- IPv6 NAT.
- NAT rules with FQDN objects in the translated source/destination (specific scenarios).
- OSPF and EIGRP.

> **Note**
>
> All policies (including unsupported ones) are migrated to the Firewall Management Center. The unsupported policies are set to the **Disabled** status for manual review and remediation.

3 Pre-Migration Tasks

Topics:

- Download the Firewall Migration Manager
- Export the configuration from Palo Alto Networks Firewall

Guides users through essential preparatory steps including downloading Firewall Migration Manager application, gathering configuration files, and collecting certificates and packages needed before beginning the firewall migration process.

Download the Firewall Migration Manager

Learn how to download the Firewall Migration Manager on your local Windows or macOS system.

Before you begin

- Ensure you have administrative rights to install Firewall Migration Manager on your local machine.
- You must have a Windows 11 64-bit machine or macOS version 14 or later, with internet connectivity to Cisco.com.

> **Note**
>
> If you want to perform migration in an air-gapped or isolated environment without internet access, contact Cisco TAC to obtain the air-gapped Firewall Migration Manager installer.

Procedure

1. Browse to Cisco Software Download Center and click Firewall Migration Manager.
2. Download the most recent version of the Firewall Migration Manager.

   Ensure that you download the executable file of Firewall Migration Manager for Windows or macOS machines.

Export the configuration from Palo Alto Networks Firewall

Lists the available methods for exporting configuration files from Palo Alto Networks Firewall, along with recommended best practices.

You can export the configuration file in these ways:

Export configuration file from a Palo Alto Networks Firewall (not managed by panorama)

Configure the Palo Alto Networks Firewall to export its configuration file for migration.

Procedure

1. Choose **Device** > **Setup** > **Operations**, and select **Save Named Configuration** <*file_name.xml*>.
2. Click **OK**.
3. Choose **Device > Setup > Operations**, and click **Export Named Configuration**.
4. Select the <*file_name.xml*> file.
5. Click **OK**.
6. Select the XML file that contains your running configuration <*file_name.xml*>, and click **Ok** to export the configuration file.
7. Save the exported file to a location, external to the firewall. You can use this backup to upload to the Firewall Migration Manager to migrate the configuration.
8. (Optional) If you have a NAT policy where the destination NAT has the same source and destination zones, perform these steps:

a) Run the **show routing route** command from CLI on the firewall.
b) Copy the routing table to a *.txt* file.
c) Add the *.txt* file to the folder where you will zip the .txt and the .xml files with the *panconfig.xml*.

These steps are not mandatory for migration. If you do not perform these steps, the destination zones will not be mapped during the Firewall Migration Manager migration and will be included in the Migration reports.

Note

Use the **show routing route** command to extract the routing table details. Paste the extracted output in a notepad.

Export configuration file from a Palo Alto Networks Firewall (managed by Panorama)

Configure and retrieve the configuration file from a Palo Alto Networks Firewall managed by Panorama.

The configuration must be extracted from the gateway if your device is managed by Panorama. Merge the Panorama configuration with the gateway and extract the configuration.

Before you begin

Log in to the Palo Alto Networks Firewall web UI using a super-user account.

Procedure

1. Choose **Device** > **Support** > **Tech Support File**.
2. Click **Generate Tech Support File**.
3. Click **Download Tech Support File** once the generated file is available.
4. Unzip and Untar the file and then navigate to the path *|opt|pancfg|mgmt|saved-configs|* to retreive the *merged-running-config.xml* file.
5. (Optional) If you have a NAT policy where the destination NAT has the same source and destination zones, perform these steps:
   a) Run the **show routing route** command from CLI on the firewall.
   b) Copy the routing table to a *.txt* file.
   c) Add the *.txt* file to the folder where you will zip the .txt and the .xml files with the *panconfig.xml*.

   These steps are not mandatory for migration. If you do not perform these steps, the destination zones will not be mapped during the Firewall Migration Manager migration and will be included in the Migration reports.

   Note

   For a Panorama-managed Palo Alto Networks Firewall with hierarchical policies, export the Panorama configuration backup, rename it `panorama_running-config.xml`, and zip it with the gateway configuration and the `route.txt` file.

4 Palo Alto Networks Firewall to Firewall Threat Defense Workflow

Topics:

- Run the Firewall Migration Manager migration
- Upload the Palo Alto Networks Firewall configuration file
- Specify destination parameters
- Map Palo Alto Networks Firewall configurations with Firewall Threat Defense interfaces
- Review and validate the migration configuration
- Review the Firewall Migration Manager pre-migration report
- Review the Firewall Migration Manager post-migration report

Guides users through the complete workflow for migrating Palo Alto Networks Firewall configurations to Firewall Threat Defense, including configuration mapping, validation, review, pre-migration reporting, and post-migration reporting.

Run the Firewall Migration Manager migration

Configure the Firewall Migration Manager to initiate a new migration workflow from the desktop interface.

Run the migration to initiate the workflow for transferring your Palo Alto Networks Firewall configuration to the target Firewall Threat Defense using the desktop version of Firewall Migration Manager.

This procedure is applicable only if you are using the desktop version of the Firewall Migration Manager.

Before you begin

- Download the Firewall Migration Manager from Cisco.com.
- Review and verify the requirements in the Supported Target Management Center for Migration section.
- If you plan to migrate a large configuration file, configure sleep settings so the system doesn't go to sleep during a migration push.

Procedure

1. From the Firewall Migration Manager GUI, from the left pane, click **Migration**.
2. Click **Start new migration** on the top-right of the window.

   The migration workflow is initiated.

   Alternatively, you can click **Lets Begin** on the home page to start the migration workflow.
3. Select **Palo Alto Networks** from the **Select source** drop-down list.

What to do next

Upload the Palo Alto Networks Firewall configuration for migration. Refer to Export the configuration from Palo Alto Networks Firewall on page 20.

Upload the Palo Alto Networks Firewall configuration file

Configure the manual upload of the Palo Alto Networks Firewall configuration file for migration.

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

Use this procedure to manually upload the source configuration file.

Before you begin

Export the configuration file as .cfg or .txt from the source Palo Alto Networks Firewall device.

Procedure

1. Select **Manual Upload** radio button in **Select configuration extraction method** area.
2. You have two options to initiate the upload:
   - Click inside the dashed-box area and browse to select the configuration file to upload.
   - Drag and drop the file into the area with the dashed border.
3. Click **Proceed**.

The Palo Alto Networks Firewall configuration file is uploaded and ready for migration processing.

What to do next

Provide details to the target device to which you want to migrate the configuration. Refer to, Specify destination parameters on page 25.

Specify destination parameters

Configure the destination parameters required for migrating device configurations to the Firewall Management Center.

Before you begin

- Obtain the IP address of the Firewall Management Center.
- (Optional) If you want to migrate device-specific configurations like interfaces and routes, add the target device to the Firewall Management Center. Refer to 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 Firewall Migration Manager 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

1. On the **Target information** screen, configure these parameters:
   a) Choose **Firewall Management Center** from the drop-down list.
   b) Enter the IP address or Fully-Qualified Domain Name (FQDN) of the Firewall Management Center.

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

   c) Click **Connect**.
2. In the **Login to target FMC** dialog box, enter the username and password of the dedicated account, and click **Login**.

   The Firewall Migration Manager logs in to the Firewall Management Center and retrieves a list of devices that are managed by that Firewall Management Center. You can view the progress of this step in the console.
3. In the **Device Selection** section, you can either select a device that you want to migrate to, or if you do not have a device, you can migrate the shared policies (Access Control Lists, NAT, and Objects) of the configuration to the Firewall Management Center.
4. Click the **Select FTD** drop-down list and select the device where you want to migrate the configuration.

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

> **Note**
>
> At minimum, the native device you choose must have the same number of physical or port channel interfaces as the configuration that you are migrating. At minimum, the container instance of the 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 Palo Alto Networks Firewall configuration. However, these interfaces do not have to have the same names on both devices.

5. Click **Next**.

Map Palo Alto Networks Firewall configurations with Firewall Threat Defense interfaces

Configure interface mappings between Palo Alto Networks Firewall configurations and Firewall Threat Defense devices to ensure proper migration compatibility.

When migrating Palo Alto Networks Firewall configurations to Firewall Threat Defense, it is essential that the target device has an equal or greater number of physical and port channel interfaces than the Palo Alto Networks Firewall configuration. The interface names do not need to match, allowing flexibility in mapping. Firewall Migration Manager retrieves interface lists and provides default mappings based on interface identity. For example, 'management-only' interfaces are mapped automatically and cannot be changed.

Before you begin

Make sure you have connected to the Firewall Management Center and chosen the destination as Firewall Threat Defense. For more information, refer to Specify destination parameters on page 25.

Procedure

1. Review the interface lists for both Palo Alto Networks Firewall configurations and the target Firewall Threat Defense device in the **Mappings** screen.
2. If you want to change an interface mapping, click the drop-down list in the **FTD Interface** column and choose the interface that you want to map to that Palo Alto Networks Firewall interface.

> **Note**
>
> - Management-only interfaces are mapped automatically and cannot be changed.
> - Once an interface is assigned, it cannot be selected again.
> - Manual mapping of physical interfaces, port-channel and sub-interfaces is required only when the target device operates in multi-instance mode.

3. You can map Palo Alto Networks Firewall firewall interfaces automatically using the **Auto Map** button.

Review, validate and edit the mapping, if required.

Review and validate the migration configuration

Review and validate the migrated Palo Alto Networks Firewall configuration before deployment.

Review and validate the migrated Palo Alto Networks Firewall configuration to ensure accuracy and resolve any conflicts before pushing it to Firewall Management Center.

Before you push the migrated Palo Alto Networks Firewall configuration to Firewall Management Center, review the configuration carefully and resolve any conflicts. Firewall Migration Manager identifies issues and allows you to remediate them directly. You can also associate policies such as IPS and file policies to access control rules, make changes to objects, and optimize the configuration before deployment.

> **Note**
>
> If you close the Firewall Migration Manager at the **Review** page, your progress is saved and you can resume the migration later. To resume the migration, click **Migration** on the main menu, and then select the migration project name on the **Migration Projects** window.

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.

Procedure

1. In the left pane of the Firewall Migration Manager click **Review**,
2. Click **Download Pre-Migration Report** to review the pre-migration report. For more information, refer to Review the pre-migration report.
3. Click **Access Control** hyperlink in the **Shared configurations** area and do the following:
   a. For each entry in the table, review the mappings and verify that they are correct.
   b. If you do not want to migrate one or more access control list policies, select the relevant rows by checking the boxes next to each policy. Then, from the **Bulk actions** drop-down menu, click **Do not migrate**.

      All rules that you choose not to migrate are grayed out in the table.
   c. 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.
3. 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.

d. 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**.

e. In the **File Policy** dialog box, 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 box, 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**.

In the **Rule Action** dialog from the **Actions** drop-down, you can either choose **ACP** or **Prefilter** tabs:

4. Click these tabs and review the configuration items:
   - Interfaces
   - Routes (Static, BGP)
   - Access Control
   - NAT
   - Objects (Network objects, User objects, Dynamic objects, Security Intelligence Feeds, Port objects, URL objects, Dynamic route objects, and VLAN objects)
   - Site-to-Site VPN
   - Remote Access VPN

> **Note**
>
> For site-to-site and remote access VPN configurations, VPN filter configurations and extended access list objects pertaining to them are migrated and can be reviewed under the respective tabs.
>
> Access List objects displays Standard and Extended ACL used in BGP, and Remote Access VPN.
>
> 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.

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

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

6. In the **Dynamic-Route objects** section, review all the supported objects that are migrated.
7. 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**.
8. 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.
9. In the **Remote Access VPN** section, review all objects corresponding to remote access VPN that are migrated from Palo Alto Networks Firewall to the Firewall Management Center.
   - **Policy Assignment**: Review and validate your connection profiles, their VPN protocols, targeted devices, and the names of the VPN interfaces. To rename a connection profile, select the corresponding entry and choose **Actions** > **Rename**.
   - **IKEV2**: Review and validate your IKEv2 protocol configurations, if any, and the source interfaces mapped with them.
   - **AnyConnect or Secure Client packages**: Ensure that you have the AnyConnect or Secure Clientpackages and the required trustpoint certificates in the Firewall Management Center.
   - **Address Pool**: Review all the IPv4 and IPv6 pools that are displayed here.
   - **Group-Policy**: Select or remove the user profile, management profile, and client module profile from this area, which displays group policies with client profiles, management profiles, client modules, and group policies without profiles. If a profile was added in the AnyConnect file area, it is displayed as preselected. You can select or remove the user profile, management profile, and client module profile.
   - **Connection Profile**: Review all connection profiles/tunnel groups that are displayed here.
   - **Trustpoints**: Trustpoint or PKI object migration from the Palo Alto Networks Firewall to the Firewall Management Center is part of the premigration activity and is required for successful migration of remote access VPN. Map the trustpoint for Global SSL, IKEv2, and interfaces in the **Remote Access Interface** section to proceed with the migration. Global SSL and IKEv2 Trustpoint are mandatory if the LDAPS protocol is enabled.

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

10. Optional: To download the details for each configuration item in the grid, click **Download**.

11. Any issues in migration are listed in **Actions** area, along with a description of the error. Click **Remediate** to resolve the issues.

    For example, you might be prompted to add a suffix to the object name to avoid a conflict with an existing Firewall Management Center object. Select the row with issue and click **Actions** > **Add suffix** to add a default suffix. Otherwise you can manually replace it with one of your own.

    > **Note**
    >
    > When the errors are resolved, a tick mark appears next to each error. Ensure that all issues are resolved before proceeding with migration.

12. After you have completed your review, click **Validate**, check the check box at the bottom of the screen to confirm migration and click **Begin Migratio**n.

    You can close this window while migration is in progress. You'll receive a notification if the migration status changes. You can resume the workflow on the main menu by selecting **Migration**, and click the migration project name.

13. Click **Next**.

    After a successful migration, a summary appears on the screen with a link to the post-migration report.

14. Click **Download report** to download and save the post-migration report.

    A copy of the post-migration report is also saved in the Resources folder in the same location as the Firewall Migration Manager.

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

What to do next

Review the post-migration report.

Review the Firewall Migration Manager pre-migration report

Review the pre-migration report to identify potential migration issues and understand the migration process before proceeding.

This report offers a detailed summary of the migration process, covering key aspects such as identified errors, unreferenced objects, and ignored configuration lines. We recommend that you familiarize yourself thoroughly with this report because some rules may not get migrated completely. This, in turn, could impact your original setup, restrict authorized traffic, or allow unintended traffic. We highly recommend that you refine rules and policies in Firewall Management Center to ensure optimal traffic management and system performance post-migration.

Procedure

1. Navigate to the location where you downloaded the **Pre-migration report**.

> **Note**
>
> A copy of the **Pre-migration report** is also saved in the `Resources` folder in the same location as the Firewall Migration Manager.

2. Open the **Pre-migration report** and carefully review its contents to identify issues, if any, that may cause the migration to fail.

   The **Pre-migration report** includes the following information:

   - **Overall Summary**–A summary of the supported configuration elements in Palo Alto Networks Firewall, which can be successfully migrated to Firewall Management Center.

     While connecting to a live Palo Alto Networks Firewall, the summary includes the hit count information, the number of times a Palo Alto Networks Firewall rule was encountered and its timestamp information.

   - **Unsupported Configuration**–This section displays the details of Palo Alto Networks Firewall configuration elements that are not migrated by Firewall Migration Manager. Review each item, and if required configure the equivalent manually before or after migration. Unsupported rules may alter the original configuration, restrict authorized traffic, or permit unwanted traffic if not addressed.

   - **Ignored Configuration**–This section displays the details of Palo Alto Networks Firewall configuration elements that are unsupported by Firewall Management Center, or not parsed by Firewall Migration Manager because they are irrelevant to the target device. Review these lines and verify whether each feature is supported in Firewall Management Center. If required, configure the features manually in Firewall Management Center.

   - **Unreferenced Configuration**–It displays the details of Palo Alto Networks Firewall configuration elements that are defined in the source configuration but are not used in any access-group, prefix list, VPN, or policy. These items will not be migrated. Review each item to determine whether it should be removed from source configuration or manually configured on the target device.

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

Review the Firewall Migration Manager post-migration report

Review the post-migration report to understand how your Palo Alto Networks Firewall configuration was migrated to a Firewall Threat Defense device and identify any configurations that require manual migration.

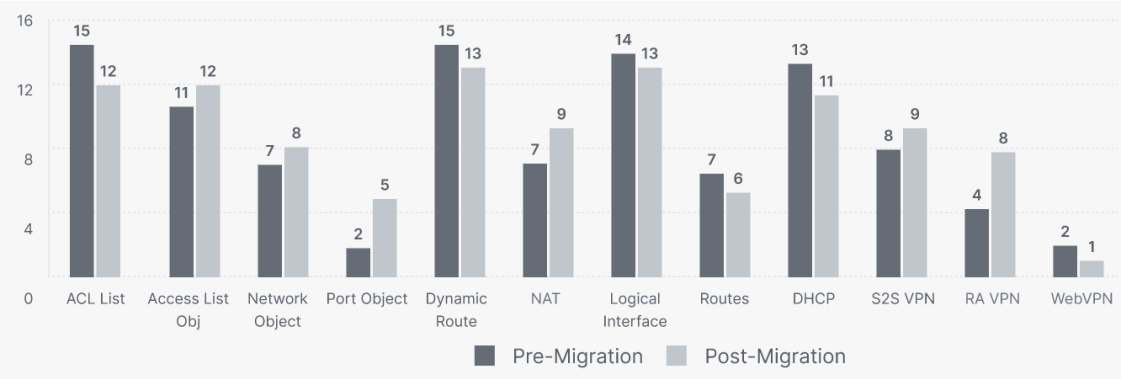
The post-migration report provides details about the source and target devices chosen for migration. It includes information about selected policies, interface and zone mapping, ACL rules under various categories, ACL optimization, and the overall view of optimization performed on the configuration file. It also provides details about partially migrated configurations and errors that occurred during migration. The report also offers guidance on resolving these errors.

Procedure

1. Navigate to where you downloaded the **Post-migration report**.
2. Open the post-migration report and carefully review its contents to understand how your Palo Alto Networks Firewall configuration was migrated:

   - **Report overview**

- **Summary Overview**–Displays a comparison chart that illustrates the difference between the count of pre-migration and post-migration states.



- **Device Details**–Summary of source and target devices used in migration.

- **Network Mapping**
  - **Policies Selected for Migration**–Displays device configuration features that you chose to migrate. The section will display if the features were successfully migrated. It will also display the set of features that you chose not to migrate. This section helps you review the features and decide if you want to manually add the features that were not migrated in management center.
  - PAN **Interface to Interface Mapping**–Details of the successfully migrated interfaces and how you mapped the interfaces on the Palo Alto Networks Firewall configuration to the interfaces on the Firewall Threat Defense device. Confirm that these mappings match your expectations.

    Note

    This section is not applicable for migrations without a destination Firewall Threat Defense device or if **Interfaces** are **not** selected for migration.

  - Source **Interface Names to Security Zones and Interface Groups**–Details of the successfully migrated Palo Alto Networks Firewall logical interfaces and name and how you mapped them to security zones and interface groups in a Firewall Threat Defense device. Confirm that these mappings match your expectations.

    Note

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

- **Object & ACL Anomalies**
  - **Object Conflict Handling**–Details of objects that were split or renamed to avoid conflicts in management center.
  - **ACL Category Conflict Handling**–The category names that were trimmed to fit Firewall Management Center naming limits.
  - **Optimization**–Objects renamed to avoid conflicts, or reused where an identical object already existed in Firewall Management Center.

    - **Reused Objects**–The objects that already existed in Firewall Management Center with identical configuration, so the Firewall Migration Manager reused them instead of creating duplicates.
    - **Access Control Rules, NAT, and Routes You Chose Not to Migrate**–Details of the rules that you choose not to migrate with the Firewall Migration Manager. Review these rules that were disabled by the Firewall Migration Manager and were not migrated. Review these lines and verify that all the rules you chose are listed in this section. If required, you can configure these rules manually.

- **Migration Issues**
    - **Partially Migrated Configuration**–Details of the Palo Alto Networks Firewall rules that were only partially migrated, including rules with advanced options where the rule could be migrated without the advanced options. Review these lines, verify whether the advanced options are supported in Firewall Management Center, and if so, configure these options manually.
    - **Policy Rules Failing Zone Lookup**–Rules that could not resolve a source or destination zone during migration.
    - **Expanded Access Control Rules**–Details of Palo Alto Networks Firewall access control policy rules that were expanded from a single Palo Alto Networks Firewall point rule into multiple Firewall Threat Defense rules during migration.

- **Action Taken on Features**
    - **Action Taken on Converted Features**–VPN policies and deprecated settings that were automatically adjusted during migration.
    - **Actions Taken on Access Control Rules**
        - **Access Rules You Chose Not to Migrate**–Details of the Palo Alto Networks Firewall access control rules that you choose not to migrate with the Firewall Migration Manager. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.
        - **Access Rules with Rule Action Change**–Details of all Access Control Policy Rules that had 'Rule Action' changed using the Firewall Migration Manager. Rule Action values are: Allow, Trust, Monitor, Block, Block with reset. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.
        - **Access Control Rules that have IPS Policy and Variable Set Applied**–Details of all Palo Alto Networks Firewall access control policy rules that have IPS Policy applied. Review these rules carefully and determine whether the feature is supported in a Firewall Threat Defense device.
        - **Access Control Rules that have File Policy Applied**–Details of all Palo Alto Networks Firewall access control policy rules that have File Policy applied. Review these rules carefully and determine whether the feature is supported in a Firewall Threat Defense device.
        - **Access Control Rules that have Rule 'Log' Setting Change**–Details of the Palo Alto Networks Firewall access control rules that had 'Log setting' changed using the Firewall Migration Manager. The Log Setting values are - False, Event Viewer, Syslog. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.
        - **Access Control Rules that have failed Zone-lookup**–Details of the Palo Alto Networks Firewall access control rules that fail the Route-lookup operation and that is populated in the **Post-Migration Report**. The Firewall Migration Manager performs the route-lookup operation based on the route (static and connected) information in the source configuration to populate the destination security zones in the access rules.
        - **Access Control Rules for Tunneled Protocols**–Details of tunnel rules that are migrated as a prefilter tunnel rule during migration.

- **Errors & Failures**–Items that failed to push to Firewall Management Center. Each entry lists the issues and the fix that resolves the issue.

  Error report may indicate an incorrect migrated configuration or a conflict within the Firewall Management Center caused by existing configurations or unsupported features. Review these errors and resolve them using the provided remedies. Verify the corrections before proceeding or resuming the configuration push to the target Firewall Management Center.

> **Note**
>
> An unsupported rule that was not migrated causes issues with unwanted traffic getting through your firewall. We recommend that you configure a rule in Firewall Management Center to ensure that this traffic is blocked by a Firewall Threat Defense device.

> **Note**
>
> If you need to apply IPS or file policy to an ACL in the **Review and Validate** page, create a policy on the Firewall Management Center before migration. This is highly recommended. Use the same policy, as the Firewall Migration Manager fetches the policy from the connected Firewall Management Center. Assigning a new policy to multiple targets can degrade performance and may result in a push failure.

For more information about supported features in Firewall Management Center and Firewall Threat Defense, refer to the Firewall Management Center Configuration Guides.

3. In Firewall Management Center, do the following:
   a) Review the migrated configuration for the Firewall Threat Defense device to confirm that all expected rules and other configuration items, including the following, were migrated:
      - Interfaces
      - Routes (Static, BGP)
      - Access Control
      - NAT
      - Objects (Network objects, User objects, Dynamic objects, Security Intelligence Feeds, Port objects, URL objects, Dynamic route objects, and VLAN objects)
      - Site-to-Site VPN
      - Remote Access VPN

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

      For information on how to configure these items and rules, refer to Firewall Management Center Configuration Guides. These are examples of configuration items that require manual configuration:
      - Platform settings, including SSH and HTTPS access, as described in Platform Settings for Threat Defense.
      - Syslog settings, as described in Configure Syslog.
      - Dynamic routing, as described in Routing Overview for Threat Defense.

- Service policies, as described in FlexConfig Policies.
- VPN configuration, as described in Threat Defense VPN.
- Connection log settings, as described in Connection Logging.

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

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

   The Firewall Migration Manager assigns the policies to the Firewall Threat Defense device. Verify that the changes are reflected in the running configuration. To help you to identify the policies that are migrated, the description of those policies includes the hostname of the Palo Alto Networks Firewall configuration.