Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense Using Firewall Migration Manager

Firewall Migration Manager
Updated July 22, 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
Firewall Migration Manager overview.....6
Features in Firewall Migration Manager.....7
Default home page of Firewall Migration Manager.....10
How ASAPAN to threat defense migration works.....11

2 Migration Requirements.....13
License requirements.....14
Platform requirements.....14
Threat Defense device prerequisites for ASA migration.....14
Supported ASA and Firewall Threat Defense platforms.....15
Target Management Center requirements.....18
Supported software versions for firewall migration.....19
Supported, partially supported and unsupported configurations.....19
Migration guidelines and limitations.....24

3 Pre-migration Tasks.....29
Download the Firewall Migration Manager.....30
Obtain ASA configuration files.....30
Export the configuration file.....30
Connect to the ASA from Firewall Migration Manager.....31
Export PKI certificates from ASA and import into Management Center.....32
Retrieve AnyConnect packages and profiles.....32

4 ASA to Threat Defense Migration Workflow.....35
Run the migration.....36
Upload ASA source configuration.....36
Upload the ASAPAN configuration file.....36
Connect to the ASA from Firewall Migration Manager.....37
Specify destination parameters.....38
Map ASA configurations with Firewall Threat Defense interfaces.....42
Map ASA interfaces to security zones, interface groups, and VRFs.....43
Review and validate the migration configuration.....45
Review the pre-migration report.....55
Review the post-migration report.....56

1 About Firewall Migration Manager

Topics:

- Firewall Migration Manager overview
- Features in Firewall Migration Manager
- Default home page of Firewall Migration Manager
- How ASAPAN to threat defense migration works

Introduces the Firewall Migration Manager application and explains how it facilitates the migration process from ASA to threat defense configurations.

Firewall Migration Manager overview

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

The Firewall Migration Manager is a network security application that automates the migration of supported ASA 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.

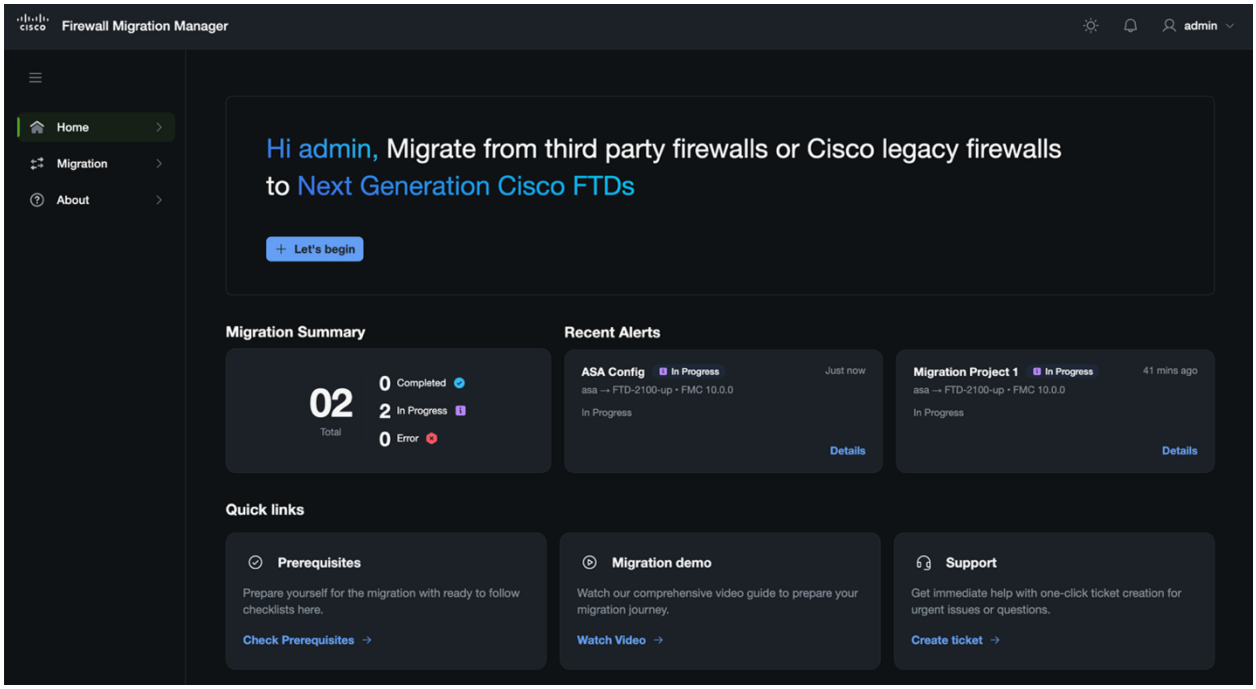
The Firewall Migration Manager an enterprise-ready product built for overcoming these challenges and to migrate seamlessly. The product helps customers and partners by offering predictable timelines, resilient workflows, and clear visibility at every stage of migration to Cisco Secure Firewall Threat 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 move from a manual, fragmented process to a unified, wizard-driven orchestration platform that prioritizes visual clarity, task parallelization, and proactive status monitoring.
- **Pre-deployment validation and testing**: Allows teams to fully evaluate a migration plan before committing to deployment.
- **Rule optimization**: Identifies opportunities to simplify firewall rules during migration, resulting in cleaner, more maintainable configurations.
- **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
10.1.0	Support for Check Point firewall to Firewall Threat Defense migration.	Firewall Migration Manager supports migration of the Check Point firewall configurations to a Firewall Threat Defense device.
	Multi-domain system configuration migration.	Firewall Migration Manager supports migration of Check Point firewall multi-domain system configurations.
	Support for Fortinet firewall to Firewall Threat Defense migration.	Firewall Migration Manager supports migration of the Fortinet firewall configurations to a Firewall Threat Defense device.
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 ASAPAN to threat defense migration works

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

Summary

ASA configuration migration is automated by Firewall Migration Manager, which ensures accurate parsing, validation, and deployment of ASA configurations to Cisco Secure Firewall Threat Defense.

Workflow

These stages describe how the ASA to threat defense migration works:

1. **Gather and parse configuration**: The Firewall Migration Manager collects information from the ASA device and parses its configuration.
2. **Map** ASA **configuration, interfaces, security zones to threat defense**: Interfaces, security zones, and interface groups are mapped to Threat Defense. You review and validate the mapping.
3. **Review pre-migration report**: The Migration Manager generates a report identifying unsupported, ignored, or erroneous configuration items, including any blocking errors.
4. **Remediate parsing errors**: The Migration Manager highlights parsing errors for you to resolve, along with the fix. You can rectify these errors to ensure seamless migration.
5. **Push validated configuration**: The Migration Manager pushes the validated configuration to the Secure Firewall Management Center and migrates the configuration to the destination device.
6. **Review post-migration report**: The 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
- Threat Defense device prerequisites for ASA migration
- Supported ASA and Firewall Threat Defense platforms
- Target Management Center requirements
- Supported software versions for firewall migration
- Supported, partially supported and unsupported configurations
- Migration guidelines and limitations

License requirements

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

While the Firewall Migration Manager is free and does not need a license, ensure that you must meet these licensing requirements:

- Firewall Threat Defense devices must have required entitlements for the features that you plan to use.

  The feature licenses can be Essentials, Malware, Intrusion Prevention System (IPS), Carrier, URL Filtering, or Secure Client licenses.

- If you have a virtual Firewall Management Center, you must have a license for Firewall Management Center Virtual.

  The required number of Firewall Management Center Virtual licenses depends on how many devices it manages.

For more information about Firewall Management Center, 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 an 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.

Threat Defense device prerequisites for ASA migration

Learn the prerequisites for migrating ASA configurations to a Threat Defense device managed by the management center. This overview outlines essential requirements for device registration, high availability, clustering, and interface configuration to ensure a successful migration.

To successfully migrate ASA configurations to a Threat Defense device managed by the management center, consider the following requirements:

- You do not need to add the target Threat Defense device to the management center before migration. Policies can be migrated to the management center for future deployment to a Threat Defense device.
- If a Threat Defense device is added to the management center, the target device must be registered with the management center.
- The target Threat Defense device can be configured for high availability.
- The Threat Defense device can be standalone or a container instance, but it must not belong to a cluster.
- For native Threat Defense devices, ensure there are at least as many used physical data and port channel interfaces (excluding "management-only" and subinterfaces) as those in the ASA device. Add required interfaces as needed.
- For container instances, ensure there are at least as many used physical interfaces, physical subinterfaces, port channel interfaces, and port channel subinterfaces (excluding "management-only") as those in the ASA device. Add required interfaces as needed.

Supported ASA and Firewall Threat Defense platforms

Learn about the supported ASA and Firewall Threat Defense platforms for configuration migration using the Firewall Migration Manager, including essential requirements for virtual and cloud-based deployments.

Lists the supported ASA and Threat Defense platforms for migration using Firewall Migration Manager.

Supported source ASA platforms

You can use Firewall Migration Manager to migrate the configuration from these single or multi-context ASA platforms:

Supported source ASA platforms	ASA 5510 ASA 5520 ASA 5540 ASA 5550 ASA 5580 ASA 5506 ASA 5506W-X ASA 5506H-X ASA 5508-X ASA 5512-X ASA 5515-X ASA 5516-X ASA 5525-X ASA 5545-X ASA 5555-X ASA 5585-X with ASA only (the Firewall Migration Manager does not migrate the configuration from the) ASA FirePOWER module Cisco Secure Firewall 220 Series Firepower 1000 Series Cisco Secure Firewall 1200 Series Firepower 2100 Series Secure Firewall 3100 Series Firepower 4100 Series Secure Firewall 4200 Series Cisco Secure Firewall 6100 Series Firepower 9300 Series SM-24 SM-36 SM-40 SM-44 SM-48

	SM-56 ASA Virtual on VMware, deployed using VMware ESXi, VMware vSphere Web Client, or vSphere standalone client

Supported target Firewall Threat Defense platforms

Firewall Migration Manager can migrate a source ASA configuration to these standalone or container instance of the Firewall Threat Defense platforms:

Supported target firewall threat defense platforms	Cisco Secure Firewall 220 Series Firepower 1000 Series Cisco Secure Firewall 1200 Series Firepower 2100 Series Secure Firewall 3100 Series Firepower 4100 Series Secure Firewall 4200 Series Cisco Secure Firewall 6100 Series Firepower 9300 Series 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

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

Note

For each of these environments, after pre-staging as per the requirements, Firewall Migration Manager 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.

You must complete the prerequisites for pre-staging the Firewall Management Center or threat defense virtual before using the Firewall Migration Manager for a successful migration.

Note

The Firewall Migration Manager requires network connectivity to devices hosted in the cloud to either extract the source configuration (ASA Live Connect) or migrate the manually uploaded configuration to the Firewall Management Center in the cloud. Hence, ensure IP network connectivity is pre-staged before using the Firewall Migration Manager.

Target Management Center requirements

Learn about the requirements for using Management Center as a target for ASA migration, including supported software versions, smart licensing, and REST API configuration.

The Firewall Migration Manager supports migration to Threat Defense devices managed by the 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 Management Center Virtual as a target management center for migration.

The management center must meet these requirements for migration:

- **Supported software versions**: Use the Management Center version that is supported for migration, as described in Supported software versions for firewall migration on page 19.
- **Smart licensing**: Obtain and install smart licenses for Firewall Threat Defense that include all features that you plan to migrate from the ASA interface, as described in:
  - 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
- **REST API**: You have enabled Management Center for REST API.

  In the Management Center web interface, navigate to **System** > **Configuration** > **REST API Preferences** > **Enable REST API**, and then check the **Enable REST API** check box.

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

Supported software versions for firewall migration

Reference the compatible software versions required for Firewall Migration Manager, ASA, and Firewall Threat Defense migrations. This overview helps identify the minimum release requirements for your management center and devices to ensure a successful configuration migration process.

This section provides information on the minimum supported software versions for each component involved in firewall migrations:

Firewall Migration Manager versions

- Supported versions are available on the Software Download page.
- It is strongly recommended to always download and use the latest version for optimal support.

ASA

- Migration is supported from devices running ASA software version 8.4 and later.

Firewall Management Center (for source ASA configuration)

- Migration to Firewall Threat Defense devices is supported for Firewall Management Center running version 6.2.3 or later.
- Some features require later versions of Management Center and Threat Defense.

> **Note**
>
> For optimum migration, upgrade your Firewall Management Center to the recommended release version as listed at: software.cisco.com/downloads.

Firewall Threat Defense

The Firewall Migration Manager 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, see the Cisco Firewall Compatibility Guide.

- Migration is supported to devices running Firewall Threat Defense version 6.5 and later.
- For software and hardware compatibility details, refer to the Cisco Firewall Compatibility Guide.

Supported, partially supported and unsupported configurations

Reference the supported, partially supported, and unsupported configurations for the Firewall Migration Manager. Use this information to determine which settings migrate automatically and which require manual updates after you move your configuration to the Firewall Management Center.

Firewall Migration Manager can handle a range of configuration types for migration. The following reference lists which configurations are fully supported, partially supported, or unsupported, along with important notes for each.

Supported configurations

The Firewall Migration Manager can fully migrate these configurations:

- Network objects and groups
- User-based access control policy rules
- Service objects (except for service objects configured for a source and destination)

> **Note**
>
> Extended service objects (configured for source and destination) are not migrated, but ACL and NAT rules referencing them are migrated with full functionality.

- Service object groups (except for nested service object groups)

> **Note**
>
> Since nesting is not supported on Firewall Management Center, the migration manager expands the content of referenced rules, preserving full functionality.

- IPv4 and IPv6 FQDN objects and groups
- IPv6 conversion support (Interface, Static Routes, Objects, ACL, and NAT)
- Access rules that are applied to interfaces in the inbound direction and global ACL
- Auto NAT, Manual NAT, and object NAT (conditional)
- NAT rules that are configured with host '0.0.0.0'
- Static routes, ECMP routes, and PBR
- DHCP configurations including server, relay, and DDNS
- SNMP
- Physical interfaces
- Secondary VLANs on interfaces

> **Note**
>
> Secondary VLANs are not migrated to Firewall Threat Defense

- Subinterfaces (subinterface ID is always set to the same number as the VLAN ID on migration)
- Port channels
- Virtual tunnel interface (VTI)

- Dynamic VTI and IPv6
- Bridge groups (transparent mode only)
- IP SLA Monitor

  The Firewall Migration Manager creates IP SLA Objects, maps them with the specific static routes, and migrates the objects to Firewall Management Center.

  IP SLA monitor defines a connectivity policy to a monitored IP address and tracks the availability of a route to the IP address. The static routes are periodically checked for availability by sending ICMP echo requests and waiting for the response. If the echo requests are timed-out, the static routes are removed from the routing table and replaced with a backup route. SLA monitoring jobs start immediately after deployment and continue to run unless, you remove the SLA monitor from the device configuration, that is, they do not age out. The IP SLA monitor objects are used in the Route Tracking field of an IPv4 static route policy. IPv6 routes do not have the option to use SLA monitor through route tracking.

  > **Note**
  >
  > IP SLA Monitor is not supported for non-Firewall Threat Defense flow.

- Object Group Search

  Enabling object group search reduces memory requirements for access control policies. We recommend you to enable object group search that enhances optimal memory utilization by access policy on Firewall Threat Defense.

  > **Note**
  >
  > - Object Group Search is unavailable for Firewall Management Center or Firewall Threat Defense version earlier than 6.6.
  > - Object Group Search will not be supported for non-Firewall Threat Defense flow and will be disabled.

- Security Group Tag-based objects

  Security Group Tag (SGT) objects enables scalable and dynamic network security through the use of policy-based access control. When the Firewall Migration Manager detects SGT-based objects, verify the objects against the rules in the **Review and Validate Configuration** page.

  To migrate the SGT objects configuration, ensure that the management center and threat defense version are 7.0 or later.

- Time-based objects

  When the Firewall Migration Manager detects time-based objects that are referenced with access-rules, the Firewall Migration Manager migrates the time-based objects and maps them with respective access-rules. Verify the objects against the rules in the **Review and Validate Configuration** page.

  Time-based objects are access-list types that allow network access on the basis of time period. It is useful when you must place restrictions on outbound or inbound traffic on the basis of a particular time of the day or particular days of a week.

Note

- You must manually migrate timezone configuration from source to target FTD.
- Time-based object is not supported for non-Firewall Threat Defense flow and will be disabled.
- Time-based objects are supported on Firewall Management Center version 6.6 and above.

- Site-to-Site VPN Tunnels
  - Site-to-Site VPN–When the Firewall Migration Manager detects crypto map configuration in the source, the Firewall Migration Manager migrates the crypto map to the Firewall Management Center VPN AS point-to-point topology.
  - Crypto map (static/dynamic) based VPN from ASA.
  - Route-based (VTI) ASA VPN.
  - Certificate-based VPN migration from ASA.
  - ASA trustpoint or certificates must be migrated to the Firewall Management Center manually as a pre-migration activity.
- Dynamic-Route Objects, BGP, and EIGRP.
  - Includes Policy-List, Prefix-List, Community List, Autonomous System (AS)-Path
- Remote Access VPN
  - **Protocols**: SSL and IKEv2
  - **Authentication methods**: AAA only, Client Certificate only, SAML, AAA, and Client Certificate
  - **AAA**: RADIUS, Local, LDAP, and AD
  - **Features**: Connection Profiles, Group-Policy, Dynamic Access Policy, LDAP Attribute Map, and Certificate Map, Standard or Extended ACL, RA VPN Custom Attributes and VPN load balancing
  - **Pre-migration tasks**:
    - Migrate ASA trustpoints manually to the Firewall Management Center as PKI objects.
    - Retrieve AnyConnect packages, Hostscan Files (Dap.xml, Data.xml, Hostscan Package), External Browser package, and AnyConnect profiles from the source ASA.
    - Upload all AnyConnect packages to the Firewall Management Center.
    - Upload AnyConnect profiles directly to the Firewall Management Center or from the Firewall Migration Manager.
    - Enable the **ssh scopy enable** command on the ASA to allow retrieval of profiles from the Live Connect ASA.
- WebVPN
  - Group security policies SSL clientless VPN tunnel protocols
  - Tunnel groups related to group policies that use Security Assertion Markup Language (SAML) as the authentication method

- Tunnel groups containing HTTPS-based application URLs

> **Note**
>
> If the aforementioned criteria are met, the SAML configurations and application URLs are migrated.

Partially supported configurations

The Firewall Migration Manager partially supports these configurations for migration. Some of these configurations include rules with advanced options that are migrated without those options. If the Firewall Management Center supports those advanced options, you can configure them manually after the migration is complete.

- Access control policy rules with advanced logging settings (e.g., severity and time-interval)
- Static routes configured with the track option
- Certificate-based VPN migration
- Dynamic-Route Objects (EIGRP and BGP)
- Route-Map

Unsupported configurations

The Firewall Migration Manager does not support these configurations for migration. If these configurations are supported in the Firewall Management Center, you can configure them manually after the migration is complete.

- NAT rules with the block allocation option
- Tunneling protocol-based access control policy rules

> **Note**
>
> Supported with a prefilter on Firewall Migration Manager and Firewall Management Center version 6.5.

- NAT rules with SCTP configuration
- Default route obtained through DHCP or PPPoE with SLA tracking
- SLA monitor schedule
- Transport mode IPsec transform-set
- ASA trustpoint migration to Firewall Management Center
- Transparent firewall mode for BGP
- ASA WebVPN to Zero Trust Application (ZTA) policy migration options not supported:
  - Importing WebVPN bookmarks
  - Local, RADIUS, and LDAP authentication methods
- Access list remarks

Migration guidelines and limitations

Review the migration guidelines and limitations for transitioning ASA configurations to Firewall Threat Defense using the Firewall Migration Manager. This reference covers supported object handling, VPN migration requirements, and configuration constraints to help you effectively prepare your environment for a successful migration.

Object and rule handling guidelines

The Firewall Migration Manager creates a one-to-one mapping for all supported objects and rules, regardless of usage in rules or policy.

Object optimization allows you to exclude unused objects from migration (objects not referenced in any ACLs and NATs).

- Unsupported objects and NAT rules are not migrated.
- Unsupported ACL rules are migrated as disabled rules into the Firewall Management Center.
- Outbound ACLs are **unsupported** and will not be migrated; outbound ACLs will be listed in the **ignored** section of the **Pre-Migration Report**.
- All supported crypto map VPN will be migrated as Firewall Management Center point-to-point topology.
- Unsupported or incomplete static crypto map VPN topologies are not migrated.
- When migrating from ASA multicontext to a single instance threat defense, the equal-cost multipath (ECMP) routing configurations are migrated to virtual routing and forwarding (VRF) configurations:
  - Interfaces and security zones in different contexts with the same name are renamed by adding an underscore and the context name.
  - ECMP routing configurations with VPN configurations are migrated to the global router (global VRF).

Configuration limitations

Migration of your source configuration has the following limitations:

- The system configurations are not migrated.
- Migration of a ACL policy that is applied to **over** 50 interfaces is not supported. Manually migrate such policies.
- Dynamic routing configurations cannot be migrated to Firewall Threat Defense. Migrate these manually.
- Devices in routed mode with bridge virtual interfaces (BVI), redundant interfaces, or tunneled interfaces cannot be migrated; devices in transparent mode with BVI can be migrated.
- Nested service object-groups or port groups are not supported; the Firewall Migration Manager expands the content during conversion.
- Extended service object groups with source and destination ports in a single line are split into multiple objects across multiple lines. Access control rules are converted with the same meaning.
- If the source configuration has access control rules that do not refer to specific tunneling protocols (like GRE, IP-in-IP and IPv6-in-IP), but these rules match unencrypted tunnel traffic, then on migration to the Firewall Threat Defense, the corresponding rules will not behave in the same way they do on the source. We recommend that you create specific tunnel rules for these in the Prefilter policy, on the Firewall Threat Defense.
- Supported crypto map will be migrated as point-to-point topology.
- If an AS-Path object with the same name in Firewall Management Center appears, then the migration stops with error message: "`Conflicting AS-Path object name detected in Firewall Management Center, please resolve conflict in Firewall Management Center to proceed further`"
- Redistribution from OSPF and Routing Information Protocol (RIP) into EIGRP is not supported.

- For PBR, ASA configuration has route-maps whereas management center does not use route-maps. The Firewall Migration Manager migrates the configuration inside a route-map applied to an interface.
- For route-maps with multiple sequence numbers, only the first sequence number will be migrated. All other sequence numbers will be ignored and shown in the pre-migration report.

Limitations for RA VPN migration

Remote Access VPN migration is supported with the following limitations:

- SSL settings migration is not supported due to API limitations.
- LDAP server is migrated with encryption type as "none".
- DfltGrpPolicy is not migrated as the policy is applicable for the entire Firewall Management Center. You can make the necessary changes directly on the Firewall Management Center.
- For a RADIUS server, if dynamic authorization is enabled, the AAA server connectivity should be through an interface and not dynamic routing. If ASA configuration is found with AAA server with dynamic authorization enabled without interface, the Firewall Migration Manager ignores dynamic authorization. You must enable dynamic-authorization manually after selecting an interface on the management center.
- ASA configuration can have an interface while calling address pool under tunnel-group. But the same is not supported on the management center. If there an interface is detected in the ASA configuration it is ignored by the Firewall Migration Manager and the address pool is migrated without the interface.
- ASA configuration can have keyword **link-selection/subnet-selection** for DHCP-server under tunnel group. But the same is not supported on the management center. If a DHCP server is detected in the ASA configuration with these keywords, it is ignored by the Firewall Migration Manager and the DHCP-server is pushed without the keywords.
- ASA configuration can have an interface while calling authentication server group, secondary authentication server group, authorization server group under tunnel group. But the same is not supported on the management center. If an interface is detected in the ASA configuration it is ignored by the Firewall Migration Manager and the commands are pushed without the interface.
- ASA configuration does not map Redirect ACL to a RADIUS server. Thus, there is no way to retrieve it from the Firewall Migration Manager. If redirect ACL is used in the ASA, it is left empty, and you must add and map it manually on the management center.
- ASA supports value from 0-720 for VPN-addr-assign local reuse delay. But the management center supports value from 0-480. If a value higher than 480 is found in the ASA configuration, it is set to maximum supported value 480 on the management center.
- Configuring IPv4 pool and DHCP useSecondaryUsernameforSession settings to the connection profile is not supported due to API issues.
- Bypass access control sysopt permit-VPN option is not enabled under RA VPN policy. However, if required, you can enable it from the management center.
- AnyConnect client module and profile values can be updated under group policy only when the profiles are uploaded from Firewall Migration Manager to the management center.
- You need to map the certificates directly on the management center.
- IKEv2 parameters are not migrated by default. You must add them through the management center.

ASA migration guidelines

The migration of the ACL log option follows the best practices for Firewall Threat Defense. The log option for a rule is enabled or disabled based on the source ASA configuration. For rules with an action of **deny**, the Firewall Migration Manager configures logging at the beginning of the connection. If the action is **permit**, the Firewall Migration Manager configures logging at the end of the connection.

Object migration guidelines

The Firewall Migration Manager and Firewall Threat Defense have different configuration guidelines for objects. For example, one or more objects can have the same name in with one object name in lowercase and the other object name in uppercase, but each object must have a unique name, regardless of case, in Firewall Threat Defense. To accommodate such differences, the Firewall Migration Manager analyzes all objects and handles their migration in one of the following ways:

- Each object has a unique name and configuration–The Firewall Migration Manager migrates the objects successfully without changes.
- The name of an object includes one or more special characters that are not supported by the Firewall Management Center–The Firewall Migration Manager renames the special characters in the object name with a "_" character to meet the Management Center object naming criteria.
- An object has the same name and configuration as an existing object in the Firewall Management Center–The Firewall Migration Manager reuses the Secure Firewall Management Center object for the Secure Firewall Threat Defense configuration and does not migrate the object.
- An object has the same name but a different configuration than an existing object in Secure Firewall Management Center–The Firewall Migration Manager reports object conflict and allows you to resolve the conflict by adding a unique suffix to the name of the object for migration purposes.
- Multiple objects have the same name but in different cases–The Firewall Migration Manager renames such objects to meet the Secure Firewall Threat Defense object naming criteria.

The Firewall Migration Manager analyzes both name and configuration of all objects and object groups. However, XML profiles in remote-access VPN configurations are analyzed only using the name.

The Firewall Migration Manager supports discontiguous network mask (Wildcard mask) objects migration if the destination Firewall Management Center is 7.1 or later.

```
ASA example:
object network wildcard2
subnet 2.0.0.2 255.0.0.255
```

Guidelines and limitations for ASA WebVPN to ZTA migration

Before attempting an ASA WebVPN to ZTA migration, make sure you read these points thoroughly:

- The target management center and threat defense device must be running Version 7.4 or later.
- The target threat defense device must be using Snort3 as the detection engine.
- The ASA trustpoint certificates (IdP and pre-authentication) must be manually uploaded to the target management center before migration.
- The application SSL certificates, along with their private keys, must be uploaded to the target management center before migration.
- Local, RADIUS, and LDAP authentication methods are not supported.
- You can assign only one ZTA policy to a threat defense device.

Guidelines and limitations for firewall threat defense devices

As you plan to migrate your ASA configuration to Firewall Threat Defense, consider these 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 Firewall Migration Manager cleans the device automatically and overwrites from the ASA 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.

- The Firewall Migration Manager can create subinterfaces on the native instance of the Firewall Threat Defense device based on the ASA configuration. Manually create interfaces and port channel interfaces on the target Firewall Threat Defense device before starting migration. For example, if your ASA configuration is assigned with specific interfaces and port channels, you must create them on the target Firewall Threat Defense device before the migration:

  > **Note**
  >
  > Manual creation of sub-interfaces or port-channels applies only to chassis-managed devices. For other devices, Firewall Migration Manager creates sub-interfaces or port-channels based on the source configuration structure.

  - 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 Firewall Migration Manager, only interface mapping is allowed.

- The Firewall Migration Manager can create subinterfaces and Bridge-Group Virtual Interfaces (transparent mode) on the native instance of the Firewall Threat Defense device that is based on the ASA configuration. Manually create interfaces and port channel interfaces on the target Firewall Threat Defense device before starting migration. For example, if your ASA configuration is assigned with specific 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

3 Pre-migration Tasks

Topics:

- Download the Firewall Migration Manager
- Obtain ASA configuration files
- Export PKI certificates from ASA and import into Management Center
- Retrieve AnyConnect packages and profiles

Outlines the preparatory steps required before migrating from ASA to Secure Firewall Threat Defense, including downloading migration tools, gathering configuration files, and collecting necessary certificates and packages.

Download the Firewall Migration Manager

Learn how to download the Firewall Migration Manager for installation on your local Windows or macOS system. This topic also explains how to access the cloud-hosted version of the application through your Security Cloud Control tenant to begin migrating your firewall configurations.

Download the Firewall Migration Manager to migrate your firewall configurations to Secure Firewall devices.

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.

Procedure

1. Browse to https://software.cisco.com/download/home/286345745/type and click Firewall Migration Manager.
2. Download the most recent version of the Firewall Migration Manager.

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

Obtain ASA configuration files

Learn how to acquire ASA configuration files for migration to Secure Firewall by manually exporting the configuration or using the live connection method in the Firewall Migration Manager.

You can use one of the following methods to obtain a configuration file:

- Export the configuration file from the device. Refer to Export the configuration file on page 30.
- Connect to the ASA using Firewall Migration Manager to retrieve the configuration file. Refer to Connect to the ASA from Firewall Migration Manager on page 31.

Export the configuration file

Learn how to export your ASA configuration file to a .cfg or .txt format for manual upload to the Firewall Migration Manager. This process ensures your existing firewall settings are correctly prepared for migration to a Threat Defense device.

Export the ASA configuration file to manually upload it to the Firewall Migration Manager for migration purposes.

Perform this task only if you want to manually upload a configuration file for migration. If you prefer to connect directly to ASA and from Firewall Migration Manager, you can skip to that step.

Do not manually edit or modify the configuration file after export. Such changes are not migrated and may create errors in the migration process or cause it to fail. For example, opening and saving the configuration file in a terminal can add extra white space or blank lines that the Firewall Migration Manager cannot parse.

Also, ensure the file does not include the --More-- keyword, which would cause migration failure.

Procedure

1. Use the `show running-config` command on the ASA device or context that you are migrating and copy the configuration from there.

Refer to View the Running Configuration section in *Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide*.

Alternatively, use Adaptive Security Device Manager (ASDM) for the ASA device or context that you want to migrate and click **File** > **how Running Configuration in New Window** to obtain the configuration file.

> **Note**
>
> For a multi-context device, use the `show tech-support` command to obtain the configurations for all contexts in a single file.

2. Save the configuration file as a .cfg or .txt file.

   You cannot upload configuration files with other extensions to Firewall Migration Manager.

3. Transfer the exported configuration file to your computer, ensuring it's accessible where the Firewall Migration Manager is installed.

Connect to the ASA from Firewall Migration Manager

Configure Firewall Migration Manager to connect to your ASA device, and extract the configuration for migration.

Enable Firewall Migration Manager to retrieve configuration data from an ASA device for migration to Secure Firewall Threat Defense.

Use Firewall Migration Manager to access an ASA device and extract all necessary configuration information for migrating to Secure Firewall Threat Defense.

Before you begin

- For a single-context ASA, obtain the management IP address, administrator credentials, and enable password.
- For a multi-context ASA, obtain the IP address for the admin context, administrator credentials, and enable password.

> **Note**
>
> If the ASA does not have an Enable Password, you can leave that field blank in Firewall Migration Manager.

Procedure

1. On the **Select firewalls** window, choose **Live Connect** option in the **Select configuration extraction method** area.
2. Enter the **IP Address/Hostname/FQDN** of the ASA:
   - For single-context ASA, enter the management IP address or hostname.
   - For multi-context ASA, enter the IP address or hostname of the admin context.
3. Enter the administrator credentials in the **Connect to Firewall** dialog box:

- Fill in the **Username**, **Password**, and **Enable Password** fields.
- If the ASA does not have an **Enable password** configured, leave that field blank.

4. Optional: Select the **HitCount** option to compute and display rule usage statistics, which helps evaluate rule effectiveness before migration.

   This allows you to evaluate the efficacy and relevance of the rule before migration.

5. Click **Connect & extract configuration**.
   - Firewall Migration Manager connects to the ASA and extracts its configuration.
   - Once extraction completes, the system identifies if your ASA uses single-context or multi-context mode and displays the available contexts for migration.

What to do next

Specify the Firewall Threat defense device details in **Target information** section. See, Specify destination parameters on page 38.

Export PKI certificates from ASA and import into Management Center

Configure the migration of certificate-based VPN from ASA to Management Center by exporting PKI certificates and importing them as PKI objects.

Export PKI certificates from ASA and import them into Management Center to enable certificate-based VPN migration.

The Firewall Migration Manager supports migration of certificate-based VPN into the management center.

ASA uses the trustpoint model for storing certificates in the configuration.

A trustpoint is a container in which certificates are stored. ASA trustpoint can store up to two certificates.

In the destination management center, migrate the ASA trustpoint or the VPN certificates manually as PKI objects as part of the pre-migration activity.

Procedure

1. Use the following command to export the PKI certificate through the CLI from the source ASA config with the keys to a PKCS12 file:

   ```
   ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
   ```

2. Import the PKI certificate into a management center (**Object Management PKI Objects)**. For more information, see PKI Objects in the *Firepower Management Center Configuration Guide*.

   The manually created PKI objects can now be used in the Firewall Migration Manager under the Trustpoint section in Remote Access VPN tab in the **Optimize, Review, and Validate** page.

Retrieve AnyConnect packages and profiles

Configure AnyConnect packages and profiles retrieval from ASA devices to prepare for Remote Access VPN migration.

This task enables you to retrieve essential AnyConnect packages and profiles from source ASA devices for use in Remote Access VPN migration to the management center.

AnyConnect profiles are optional and can be uploaded through the management center or Firewall Migration Manager.

Before you begin

- Remote Access VPN on the management center requires at least one AnyConnect package.
- If the configuration consists of Hostscan and External Browser package, you must upload these packages.

  All packages must be added to the management center as part of the pre-migration activity.
- Dap.xml and Data.xml must be added through the Firewall Migration Manager.

Procedure

1. Use the following command to copy the required package from the source ASA to an FTP or TFTP server:

```
Copy <source file location:/source file name> <destination>
ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1
<----- Example of copying Anyconnect Package.
ASA# copy disk0:/ external-sso- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1
<----- Exampleof copying External Browser Package.
ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Example
of copying Hostscan Package.
ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <----- Example of copying Dap.xml
ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Example of copying
 Data.xml
ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Example of copying
Anyconnect Profile.
```

2. Import the downloaded packages to management center (**Object Management** > **VPN** > **AnyConnect File**).
   a. Dap.xml and Data.xml must be uploaded to the management center from the Firewall Migration Manager in the **Review and Validate** > **Remote Access VPN** > **AnyConnect File** section.
   b. AnyConnect profiles can be uploaded directly to the management center or through the Firewall Migration Manager in the **Review and Validate** > **Remote Access VPN** > **AnyConnect File** section.

      The manually uploaded files can now be used in the Firewall Migration Manager.

4 ASA to Threat Defense Migration Workflow

Topics:

- Run the migration
- Upload ASA source configuration
- Specify destination parameters
- Map ASA configurations with Firewall Threat Defense interfaces
- Map ASA interfaces to security zones, interface groups, and VRFs
- Review and validate the migration configuration
- Review the post-migration report

Guides users through the complete workflow for migrating from Adaptive Security Appliance to Firewall Threat Defense, covering configuration upload, parameter mapping, validation, pre-migration reporting, and post-migration reporting.

Run the migration

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

Run the migration to initiate the workflow for transferring your ASA configuration to the target Secure Firewall Management Center using the desktop version of the Migration Manager.

This task 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.
- Ensure that your computer has a recent version of the Google Chrome browser to run the Firewall Migration Manager. 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.

Follow these steps to run the migration:

Procedure

1. From the Firewall Migration Manager GUI, click **Migration** > **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.
2. Select **Cisco ASA** from the **Select source** drop-down list.

The migration workflow is initiated and ready to accept the ASA configuration for processing.

What to do next

You must upload the ASA configuration for migration. See Upload the ASAPAN configuration file on page 36.

Upload ASA source configuration

Lists the methods available for uploading your ASA source configuration to Firewall Migration Manager.

Firewall Migration Manager provides multiple options for uploading your ASA source configuration. You can use the method that best fits your environment and workflow:

- **Manual upload via the user interface**: Upload the ASA configuration file to Firewall Migration Manager through the user interface, see Manually upload the ASA configuration file.
- **Automatic retrieval from the ASA device**: Connect to the ASA device from the Firewall Migration Manager to retrieve the configuration automatically, see Connect to the ASA from Firewall Migration Manager on page 31.

Upload the ASAPAN configuration file

Configure the manual upload of the ASAPAN configuration file for migration.

This task uploads the source ASAPAN configuration file to initiate the migration process.

> **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 ASAPAN 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 ASAPAN 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. See, Specify destination parameters on page 38Specify destination parameters.

Connect to the ASA from Firewall Migration Manager

Configure Firewall Migration Manager to connect to your ASA device, and extract the configuration for migration.

Enable Firewall Migration Manager to retrieve configuration data from an ASA device for migration to Secure Firewall Threat Defense.

Use Firewall Migration Manager to access an ASA device and extract all necessary configuration information for migrating to Secure Firewall Threat Defense.

Before you begin

- For a single-context ASA, obtain the management IP address, administrator credentials, and enable password.
- For a multi-context ASA, obtain the IP address for the admin context, administrator credentials, and enable password.

> **Note**
>
> If the ASA does not have an Enable Password, you can leave that field blank in Firewall Migration Manager.

Procedure

1. On the **Select firewalls** window, choose **Live Connect** option in the **Select configuration extraction method** area.
2. Enter the **IP Address/Hostname/FQDN** of the ASA:
   - For single-context ASA, enter the management IP address or hostname.
   - For multi-context ASA, enter the IP address or hostname of the admin context.
3. Enter the administrator credentials in the **Connect to Firewall** dialog box:
   - Fill in the **Username**, **Password**, and **Enable Password** fields.
   - If the ASA does not have an **Enable password** configured, leave that field blank.
4. Optional: Select the **HitCount** option to compute and display rule usage statistics, which helps evaluate rule effectiveness before migration.

   This allows you to evaluate the efficacy and relevance of the rule before migration.
5. Click **Connect & extract configuration**.
   - Firewall Migration Manager connects to the ASA and extracts its configuration.
   - Once extraction completes, the system identifies if your ASA uses single-context or multi-context mode and displays the available contexts for migration.

What to do next

Specify the Firewall Threat defense device details in **Target information** section. See, Specify destination parameters on page 38.

Specify destination parameters

Configure the target Firewall Management Center connection and device selection for ASA migration using the Firewall Migration Manager.

This task enables you to establish connectivity to the target Firewall Management Center and select the appropriate destination device or configuration type for migrating ASA configurations.

Before you begin

- Obtain the IP address for the Firewall Management Center for On-Prem Firewall Management Center.
- Create a dedicated account for the Firewall Migration Manager in the Firewall Management Center with sufficient privileges to access the REST API, as described in User Accounts for Management Access.

- 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 you need to apply IPS or file policy to ACL in the **Review and Validate** page, we recommend creating the 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.

Follow these steps to specify destination parameters:

Procedure

1. In the **Target information** area, select the target Management Center from the drop-down list.
2. Enter the IP address, host name, or fully qualified domain name (FQDN) of the target management center and click **Connect**.

   The **Login to target FMC** dialog box appears.
3. Enter the **Username** and **Password** to connect to the Firewall Management Center.

   The Firewall Migration Manager synchronizes with the management center and retrieves the list of devices that appears in the subsequent steps.
4. In the **Device selection** area you have two options:

   Note

   In the **Device selection** section, you can either select a Threat Defense device that you want to migrate to, or if you do not have a Threat Defense device, you can migrate the shared policies (Access Control Lists, NAT, and Objects) of the ASA configuration to the Firewall Management Center.

   - **Select FTD**: To select either a single device or an HA pair, choose Threat Defense device from the drop-down list.

Note

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

Note

The native Threat Defense device you choose must have at least as many physical or port channel interfaces as the ASA configuration being migrated. The container instance of the Threat Defense device must also have at least the same number of physical or port channel interfaces and subinterfaces. You must configure the device with the same firewall mode as the ASA configuration. However, these interfaces do not have to have the same names on both devices.

Note

FDM 5505 migration support is available for shared policies only when the supported target threat defense platform is Firewall 1010 with management center version 6.5 or later. Device-specific policies are not supported. If you proceed without threat defense, Firewall Migration Manager does not push any configurations or policies to the threat defense. Interfaces, routes, and site-to-site VPN, which are threat defense device-specific configurations, will not be migrated. All other supported configurations–such as shared policies and objects, including NAT, ACLs, and port objects–will be migrated. Remote Access VPN is a shared policy and can be migrated even without threat defense.

Table 2: ASA firewall features and supported firewall management center or firewall threat defense versions

Firewall features	Supported Management Center or Threat Defense version
ASA with remote deployment	6.7 or later
Crypto Map Site-to-Site VPN	6.6 or later
Virtual Tunnel Interface (VTI) and Route-based (VTI)	6.7 or later
Dynamic-Route Objects and BGP	7.1 or later
Remote Access VPN	• Management Center 7.2 or later • Threat Defense 7.0 or later.
EIGRP	• Management Center 7.2 or later • Threat Defense 7.0 or later.

Firewall features	Supported Management Center or Threat Defense version
PBR	• Management Center 7.3 or later • Threat Defense 7.3 or later.
ECMP	• Management Center 7.1 or later • Threat Defense 6.5 or later.
WebVPN	• Management Center 7.4 or later • Threat Defense 7.4 or later
SNMP	• Management Center 7.4 or later • Threat Defense 7.4 or later
DHCP Relay, Server, and DDNS	• Management Center 7.4 or later • Threat Defense 7.4 or later

Note

To migrate Site-to-Site VPN, VTI, and Route-based (VTI) interfaces, Firewall Threat Defense must be configured on Firewall Management Center.

Note

- For ASA 5505, the device-specific configs (Interface and routes) and shared policies (NAT, ACLs, and Objects) can be migrated only when the supported target Firewall Threat Defense platform is Firewall 1010 with Firewall Management Center version 6.5 or later.
- If the target Firewall Threat Defense is not FPR-1010 or the target Firewall Management Center is earlier than 6.5, ASA 5505 migration support is applicable for shared policies only. Device specifics will not be migrated.
- You can select only FPR-1010 in the Select Device drop-down list as the source config is ASA 5505.
- ASA-SM migration support is for shared policies only. Device specifics will not be migrated.

- **Migrate to shared configurations**: To migrate shared configurations directly without device selection, select **Migrate to shared configurations** radio button.

> **Note**
>
> Only the shared configuration is pushed to management center. Users can later select the Threat Defense device in management center to complete the process.

5. Click **Next**.

The target Firewall Management Center connection is established and the selected device or shared configuration option is configured for the ASA migration process.

What to do next

Map ASA configurations with Firewall Threat Defense interfaces on page 42.

Map ASA configurations with Firewall Threat Defense interfaces

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

This task establishes the proper interface mappings between ASA configurations and Firewall Threat Defense devices to ensure successful migration of network configurations.

When migrating ASA 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 ASA 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 (e.g., 'management-only' interfaces are mapped automatically and cannot be changed).

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

- **Native type**:
  - The Firewall Threat Defense must have equal or a greater number of used ASA interfaces or port channel (PC) data interfaces (excluding management-only and subinterfaces in the ASA configuration). If the number is less, add the required type of interface on the target Firewall Threat Defense.
  - Subinterfaces are created by the Firewall Migration Manager based on physical interface or port channel mapping.
- **Container type**:
  - The Firewall Threat Defense must have equal or a greater number of used ASA interfaces, physical subinterfaces, port channel, or port channel subinterfaces (excluding management-only in ASA 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 ASA then you can create the additional physical or physical subinterfaces on the target Firewall Threat Defense.
  - Subinterfaces are not created by the Firewall Migration Manager. 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 on page 38.

Procedure

1. Review the interface lists for both ASA configurations and the target Firewall Threat Defense device on 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 ASA 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 subinterfaces is required only when the target device operates in multi-instance mode.

3. When you have mapped each ASA interface to a Firewall Threat Defense interface, proceed to Map ASA interfaces to security zones, interface groups, and VRFs on page 43.

Map ASA interfaces to security zones, interface groups, and VRFs

Configure interface mappings to security zones, interface groups, and VRFs to ensure proper ASA configuration migration.

Map ASA interfaces to appropriate Firewall Threat Defense interface objects, security zones, interface groups, and VRFs for proper configuration migration.

Note

If your ASA configuration does not include Access Lists and NAT rules or if you choose not to migrate these policies, you can skip this step and proceed to Review and validate the migration configuration on page 45.

To ensure that the ASA configuration is migrated correctly, map the ASA interfaces to the appropriate Firewall Threat Defense interface objects, security zones and interface groups, and VRFs. In an ASA 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.
- VRFs–An interface can belong to only one VRF configuration.

The Firewall Migration Manager allows one-to-one mapping of interfaces with security zones, interface groups, and VRFs; 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

1. On the **Mappings** page click **Security zones** tab to review the security zones and **Interface groups** tab to review the interface groups.
2. Map interfaces to existing security zones and interface groups.

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

   a. Click the **Security zones** tab, choose the security zone for the interface from the drop-down list.

   b. Click the **Interface groups** tab, choose the interface group for the interface from the drop-down list.

   c. Click the **VRF** tab, and choose the VRF configurations for the interface.

   > **Note**
   >
   > If you are setting up a threat defense HA pair as part of the migration, you can add or auto map security zones and interface groups for both primary and secondary peers. Note that the security zones and interface groups of the secondary peer are same as those of the primary peer.

3. Create and map security zones, interface groups, and VRFs manually.
   a) Click **Add Zone and Interface Groups**.
   b) In the **Add Security Zones & Interface Groups** dialog box, enter the security zone name, and click **Add**.

      The maximum characters allowed is 48.

   c) Click **Interface groups (IG)** tab, enter the interface group name, and click **Add**.

      Same for adding VRF.

   d) Click **Save and Close**.

   > **Note**
   >
   > If you are performing a merged-configuration migration and one of your contexts had VPN configuration, it does not get displayed here to be mapped to an interface, because it gets migrated to the global router directly.

4. Auto-create and map security zones and interface groups.
   a) Click **Auto create** button.
   b) Check **Security zones** and **Interface groups** check box in **Confirm Auto-Creation** dialog box and click **Auto create**.

   The Firewall Migration Manager gives these security zones the same name as the ASA interface, such as outside or inside, and displays an "(A)" after the name to indicate that it was created by the Firewall Migration Manager. 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 ASA interface. For example, if the ASA logical interface is in L3 mode, the security zone and interface group that is created for the interface is also in L3 mode.

5. Proceed to the next step when all interfaces are mapped.

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

What to do next

Review and validate the migration configuration on page 45.

Review and validate the migration configuration

Review and validate the migrated ASA configuration before deployment.

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

Before you push the migrated ASA 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.

The source ASA device may be managed by CSM or ASDM. When you enter more than one item (object or inline values) in the source or destination address, or source or destination service, CSM or ASDM automatically creates an object group. The naming conventions for these object groups that are used by CSM and ASDM are CSM_INLINE and DM_INLINE respectively.

When you opt to clear the inline grouping CSM or ASDM managed configurations, the predefined objects are replaced with the actual object or member name. If you do not clear the CSM or ASDM managed configurations, the predefined object names will be retained for migration.

For example, 10.21.44.189 and 10.21.44.190 are members of an object group and are renamed with the predefined names such as object-group DM_INLINE_NETWORK_1 and object-group DM_INLINE_NETWORK_2.

> **Note**
>
> By default, the Inline Grouping option is enabled.

Procedure

1. On the **Review** screen, click **Download report** to review the pre-migration report. For more information, see Review the pre-migration report on page 55
2. Click **Access Control** hyperlink in the **Shared configurations** area and do the following:
   a. For each entry in the Access control policy rules 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 ASA configuration file. For example, if an ASA 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 Firewall Migration Manager 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 Firewall Migration Manager appends an "_UNSUPPORTED" suffix to the name.
   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:

- ACP–Every access control rule has an action that determines how the system handles and logs matching traffic. You can either perform an allow, trust, monitor, block, or block with reset action on an access control rule.
- Prefilter–A rule's action determines how the system handles and logs matching traffic. You can either perform a fastpath and block.

> **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.
>
> ACL Rule Category–The Firewall Migration Manager preserves the Rule sections in the CSM managed ASA configuration and migrates them as ACL categories on Firewall Management Center.
>
> Policy capacity and limit warning–The Firewall Migration Manager compares the total ACE count for the migrated rules with the supported ACE limit on the target platform.
>
> Based on the comparison result, the Firewall Migration Manager displays a visible indicator and a warning message if the total count of migrated ACE exceeds threshold or if it approaches the threshold of the supported limit of target device.
>
> You can optimize or decide not to migrate if the rules exceed the ACE Count column. You can also complete the migration and use this information to optimize the rules after a push on the Firewall Management Center before deployment.

> **Note**
>
> The Firewall Migration Manager does not block any migration despite the warning. 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.

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

- Access Control
- Objects (Access List Objects, NETWORK Objects, Port Objects, VPN Objects, Security Group Tag Objects, and Dynamic-Route Objects)
- NAT
- Interfaces
- Routes
- DHCP
- SNMP
- Site-to-Site VPN Tunnels
- Remote Access VPN
- WebVPN

> **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, EIGRP, and RA 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.

4. On the NETWORK objects and the Port objects tabs, review all the NETWORK objects, NETWORK groups, port objects, port groups, and their values.

   To rename an object or object group, double-click the name, edit the name and press Enter.

   > **Note**
   >
   > - If you do not want to migrate one or more network objects or port objects, check the box for the appropriate rows, choose **Actions** > **Do not migrate**, and then click **Save**.
   > - The objects and groups which are not chosen to be retained are not migrated and are replaced with the retained objects in the configurations they were used, such as in ACL and NAT configurations. This ensures the list of objects being migrated is fully optimized and there are no duplicate objects migrated.

5. On the **Security group tag objects** tab, review all the values. To rename an object or object group, double-click the name, edit the name and press Enter.

   SGT objects support multi-context configuration. The tag value must range from 0 to 65535.

> **Note**
>
> To migrate the SGT objects configuration, ensure that the management center and threat defense version are 7.0 or later.

6. In the **Dynamic-Route objects** section, review all the supported objects that are migrated.
7. In the **Routes** section, review the following routes that are displayed:
   - Static–Displays all IPv4 and IPv6 static routes.
   - BGP–Displays all the BGP routes.
   - EIGRP–Displays all the EIGRP routes.
   - ECMP–Displays all the ECMP zones and associated VRFs.
   - PBR–Displays all the PBR routes.
8. Under the **DHCP** tab, review and validate the following tabs:
   - DHCP Server: Review all the IP address pools and the corresponding interfaces.
   - DHCP Relay: Review the DHCP Relay server IP addresses, interfaces to which the DHCP server is associated with, and the Relay-enabled interfaces.
   - DDNS: Under DDNS Update Methods tab, review the DDNS method names, types, the DDNS update intervals, and which records are configured to be updated by the DHCP Server (A or PTR records).
9. Under the **SNMP** tab, review, validate, and work with the configurations based on whether you have SNMPV1/V2 or SNMPV3 configurations on your ASA device.

   Based on whether you have SNMPV1/V2 or SNMPV3 configurations on your ASA device, the configurations gets displayed in SNMPV1/V2 tab or SNMPV3 tab.

   SNMPV1/V2:
   - Host Server Name: The hostname of the SNMP host
   - IP Address: The IP address of the SNMP host
   - Community String: The SNMP community string that must be provided manually. Select the host and navigate Actions > Update Community String to provide the community string. This must be the same as the community or username that is configured for the SNMP service.
   - Validation State: The host server's validation state that will be created in the target management center.

   SNMPV3:
   - User Name: The username for SNMP host
   - Authentication Password: Click Actions to provide the authentication password for the user
   - Encryption Password: Click Actions to provide the privacy password for the user
   - Validation State: The user's validation state that will be created in the target management center
10. In the **Site-to-Site VPN Tunnels** section, review all the supported VPN tunnels that are migrated from ASA to Firewall Management Center.

You must enter the values for preshared key and the PKI object for each VPN topology for validation for all the rows. Failure to update will be marked as incomplete and the Firewall Migration Manager will not allow to proceed to validation.

> **Note**
>
> For a live connect ASA, the preshared keys are retrieved automatically by the migration manager; for a manually uploaded configuration, use the more system: running-config to retrieve the hidden keys and provide them manually in the preshared Key column.

> **Note**
>
> Trustpoint or PKI object migration from ASA to Firewall Management Center is part of the pre-migration activity and is required for successful migration of certificate-based VPN migration.

11. Optional: Click **Add Hub & Spoke Topology** to configure a hub and spoke VPN topology using the target threat defense as the hub node and selecting one or more ASA peer interfaces as the spoke nodes.

> **Note**
>
> You can select spoke nodes of the same IKE versions only. For instance, you cannot choose one spoke node of IKEv1 and another spoke node of IKEv2 IKE version.

Based on the IKE version of the selected spoke nodes, configure or verify the following:

- IKE Version–Verify that the IKE version of the selected nodes is checked.
- Endpoints–Verify that the target threat defense device is by default selected as the hub node, the spoke nodes you selected from the list, and their VPN interfaces and protected source and remote networks.
- IKEv1 Settings or IKEv2 Settings
  - Authentication Type–The two supported authentication methods are preshared key and certificate. See Deciding Which Authentication Method to Use in the *Cisco Secure Firewall Management Center Device Configuration Guide*.
- Advanced
  - Enable Aggressive Mode–Select this negotiation method for exchanging key information if the IP address is not known and DNS resolution might not be available on the devices.
  - IKE Keepalive–Enable or disable this for the keepalive monitoring.
  - Threshold–Specify the IKE keep alive confidence interval. This interval is the number of seconds allowing a peer to idle before beginning keep alive monitoring. The minimum and default interval is 10 seconds; the maximum interval is 3600 seconds.
  - Retry Interval–Specify number of seconds to wait before the IKE keep alive retries. The default is 2 seconds, the maximum is 10 seconds.

- IPsec
  - Crypto Map Type–A crypto map combines all the components required to set up IPsec security associations (SA). When two peers try to establish an SA, they must each have at least one compatible crypto map entry. The IPsec security negotiation uses the proposals defined in the crypto map entry to protect the data flows specified by that crypto map's IPsec rules. Choose static or dynamic for this deployment's crypto map.
  - Transform Sets–Select the IPsec proposal that you want to use for the IKE version nodes you selected.
    - Enable Security Association (SA) Strength Enforcement–Check this checkbox to ensure that the encryption algorithm used by the child IPsec SA is not stronger (in terms of the number of bits in the key) than the parent IKE SA.
    - Enable Reverse Route Injection–Check this checkbox to enable reverse route injection which automatically inserts static routes into routing for networks and hosts, which are protected by a remote tunnel group list.
    - Enable Perfect Forward Secrecy–Check this checkbox to generate and use a unique session key for each encrypted exchange. The unique session key protects the exchange from subsequent decryption, even if the entire exchange was recorded and the attacker has obtained the preshared or private keys used by the endpoint devices.
  - Modulus Group–Choose the Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. See Deciding Which Diffie-Hellman Modulus Group to Use in the *Cisco Secure Firewall Management Center Device Configuration Guide* for more information.
  - Lifetime Duration–The number of seconds you want a security association to exist before expiring. The default is 28,800 seconds.
  - Lifetime Size–The volume of traffic (in kilobytes) that can pass between IPsec peers using a given security association before it expires. The default is 4,608,000 kilobytes. Infinite data is not allowed.

If you have an existing site-to-site hub and spoke VPN configuration on one of the devices in the management center, you can choose to add your target threat defense device as one of the spokes to it. Choose Add to existing Hub & Spoke Topology, select the topology to which you want to add your device, and select Interface and Protected Networks.

12. In the **Remote Access VPN** section, review all objects corresponding to remote access VPN that are migrated from ASA to the management center.

-
- Anyconnect Packages: Retreive the AnyConnect packages, Hostscan Files (Dap.xml, Data.xml, Hostscan Package), External Browser package, and AnyConnect profiles should be retrieved from the source ASA device for migration.

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

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

  Ensure that the correct Dap.xml file is retrieved from the source firewall. Validations are performed on the dap.xml file that are available in the configuration file. You must select all the files that are required for validation and upload them. Failure to update marks as incomplete and the Firewall Migration Manager does not proceed with validation.
- AAA–Authentication servers of Radius, LDAP, AD, LDAP, SAML, and Local Realm type are displayed. Update the keys for all AAA servers. From Firewall Migration Manager 3.0, the preshared keys are retrieved automatically

for a Live Connect ASA. You can also upload the source configuration with the hidden keys using `more system:running-config` file. To retrieve the AAA authentication key in clear text format, follow the below steps

> **Note**
>
> These steps should be performed outside the Firewall Migration Manager.

a. Connect to the ASA through the SSH console.

b. Enter the `more system:running-config` command.

c. Go to the **aaa-server and local user** section to find all the AAA config and the respective key values in clear text format.

```
ciscoASA#more system:running-config

!

aaa-server Test-RADIUS (inside) host 2.2.2.2

 key <key in clear text>     <-----The radius key is now displayed in
clear text format.

aaa-server Test-LDAP (inside) host 3.3.3.3

ldap-login-password <Password in clear text> <-----TheLDAP/AD/LDAPS
password is now displayed in clear text format.

username Test_User password <Password in clear text> <-----The Local
user
        password is shown in clear text.
```

> **Note**
>
> If the password for the local user is encrypted, you can internally check for the password or configure a new one on the Firewall Migration Manager. LDAPS requires domain on management center. You must update domain for encryption type LDAPS.

- Unique AD Primary Domain is required on Firewall Management Center for an AD server. If a unique domain is identified, it will be displayed on the Firewall Migration Manager. If conflict is found, you must enter a unique AD primary domain to push the objects successfully.

  For AAA server with encryption set to LDAPS, ASA supports IP and hostname or domain but the management center supports only hostname or domain. If ASA config contains hostname or domain, it is retrieved and displayed. If ASA config contains the IP address for LDAPS, enter a domain in the **AAA** section under **Remote Access VPN**. You must enter the domain that can be resolved to the IP address of the AAA server.

  `If the ldap-base-dn is: ou=Test-Ou,dc=gcevpn,dc=com`

  The **AD Primary Domain** is the field starting with dc, with dc=gcevpn, and dc=com that forms the primary domain. The AD primary domain would be gcevpn.com.

  LDAP-base-dn example file:

`cn=asa,OU=ServiceAccounts,OU=abc,dc=abc,dc=com:`

Here, dc=abc, and dc=com will be combined as abc.com to form the AD Primary Domain.

`cn=admin, cn=users, dc=fwsecurity, dc=cisco, dc=com:`

AD Primary Domain is fwsecurity.cisco.com. AD Primary Domain is retrieved automatically and displayed on the Firewall Migration Manager.

> **Note**
>
> AD Primary Domain value needs to be unique for each Realm object. In case a conflict is detected or if the Firewall Migration Manager is unable to find the value in the ASA config, you are requested to enter an AD Primary Domain for the specific server. Enter the AD Primary Domain to validate the configuration.

- **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.

  The custom attribute related to the specific group-policy is displayed in the **AnyConnect Custom Attribute** tab. You can select the custom attribute and validate it.
- **Connection Profile**–Review all connection profiles/tunnel groups that are displayed here.
- **Trustpoints**–Trustpoint or PKI object migration from the ASA to the management center is part of the premigration activity and is required for successful migration of remote access VPN. Map the trustpoint for Global SSL, IKEv2, and interfaces in the **Remote Access Interface** section to proceed with the migration. 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 ASA, it can be selected under **Override SAML**.

  For information on exporting PKI certificates from ASA, see Export PKI certificates from ASA and import into Management Center on page 32.
- **Certificate Maps**–Certificate maps are displayed here.
- **VPN Load Balancing**–VPN load balancing Configurations are displayed here.

  For VPN load balancing, the Firewall Migration Manager will fetch the encryption key if **more system: running-config** configuration is uploaded. You can manually update the encryption key using **Actions** > **Update Keys**.
- Under the **WebVPN** tab, the Migration Manager lists all the WebVPN policies that it detected in the source ASA device. WebVPN policies include any ASA group policy with SSL clientless VPN tunnel protocol configurations and tunnel groups that are referenced to policies using SAML authentication. Ensure you review the tabs associated with your WebVPN configurations before proceeding:
  - **Zero Trust Application Policy**: Provide a different value by selecting the policy and navigating **Actions** > **Update Zero Trust Policy fields**
    - **Policy Name**: The policy's name that will get migrated.

- **Domain Name**: User-defined domain name that must be manually provided. This domain name resolves to the threat defense interface from where the private applications are accessed. The domain name is used to generate the ACS URL for all private applications in an Application Group.
- **Identity Certificate**: The identity certificate that you imported into the target management center before migration. This must be done as part of the premigration tasks.
- **Security Zones**: The corresponding security zones associated with the policy.
- **Global Port Pool**: The port range for the policy. A unique port from this pool is assigned to each application.

- **Application Group**
  - **Application Group**: Review the **Application Group Settings** including application group name, re-authentication interval, and security zones.

    Under the **SAML IdP Metadata** tab, you can choose to manually configure application group name, entity ID for the service provider, single sign-on URL for the SAML identity provider (IdP), and IdP certificate or choose **Configure Later**

    The **Applications** tab lets you review or configure application-specific settings such as application name, external URL, application URL, application certificate, and application group.

- **Standalone Applications**: Review or configure **Application Settings** for standalone applications, including application name, external URL, application URL, application certificate, re-authentication interval, and security zones. The **SAML IdP Metadata** tab lets you manually configure IdP metadata settings for standalone applications or configure later. The tabs include application group name, entity ID, single sign-on URL, and IdP certificate.

To update the fields, click **Actions** and choose to update the various fields.

After the migration is successful, ensure you do a thorough review of the configurations that you migrated to the management center and when ready, deploy it to your threat defense device.

13. Optional: To download the details for each configuration item in the grid, click Download.
14. 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.

15. Click **Optimize** button at the bottom of the screen.

    The Migration Manager performs the optimization and displays an optimization summary with optimization data including retained and duplicate objects. For a detailed version of the optimization report, refer to the post-migration report.

16. 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.

17. Click **Next**.

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

18. 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.

19. 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 on page 56.

Review the pre-migration report

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

Review the pre-migration report to identify errors, unreferenced objects, and ignored configuration lines that may impact migration success or system performance.

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 ASA, which can be successfully migrated to Firewall Management Center.

     While connecting to a live ASA, the summary includes the hit count information, the number of times an ASA rule was encountered and its timestamp information.

   - **Configuration Lines with Errors**–This section displays the details of ASA configuration elements that cannot be successfully migrated because the Firewall Migration Manager could not parse them. Correct these errors in

the source device, generate a new configuration file, and then upload the new configuration file to the Firewall Migration Manager before proceeding with migration.

- **Unsupported Configuration**–This section displays the details of ASA 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 ASA configuration elements that are unsupported by Firewall Management Center, or not parsed by 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
- **Object and Object Groups Conflict Resolution**–This section displays the details of ASA network and service objects and object, service, and protocol object groups that have conflicts across the contexts you are trying to migrate. To view detailed information about these object conflicts, click the **Link for Conflict Count**; you can check the reason for the conflicts and also know how the Migration Manager is handling the conflicts.
- **Ignored Configuration**–This section displays the details of ASA configuration elements that are not supported by the Firewall Management Center or the Firewall Migration Manager. The Firewall Migration Manager does not parse these lines. Review these lines, verify whether each feature is supported in Firewall Management Center. If the feature is not supported, plan to configure it manually.
- **Unreferenced Configuration**–It displays the details of ASA 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, see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Review the post-migration report

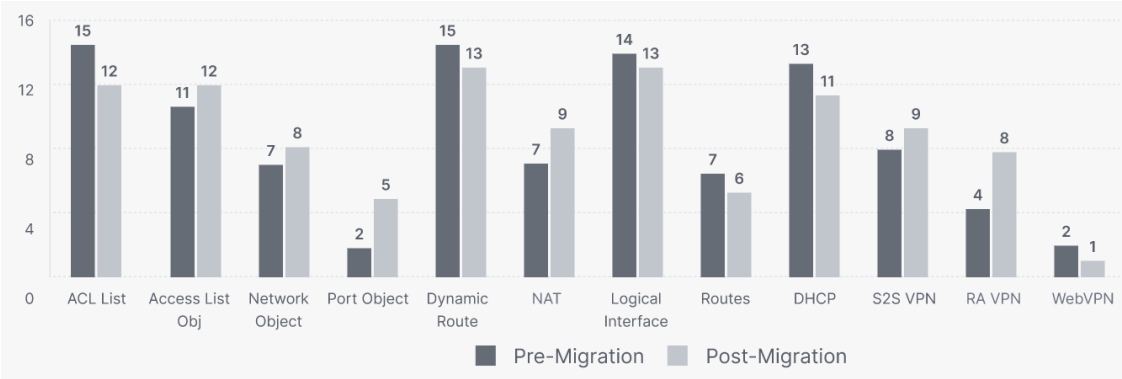
Review the post-migration report to understand how your ASA configuration was migrated to Firewall Threat Defense and identify any configuration items that require manual migration.

This task helps you understand the migration results, verify successful configuration migration, and identify any unsupported or partially migrated configuration items that require manual configuration on the Firewall Threat Defense device.

The Post-migration report provides details on 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 on partially migrated configurations and errors that occurred during migration. The report 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 ASA 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.
  - ASA **Interface to Interface Mapping**–Details of the successfully migrated interfaces and how you mapped the interfaces on the ASA configuration to the interfaces on the Firewall Management Center 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.

  - **Interface to ECMP Zone Mapping**–Details of interfaces assigned to ECMP zones on the target device.
  - Source **Interface Names to Security Zones and Interface Groups**–Details of the successfully migrated ASA logical interfaces and name and how you mapped them to security zones and interface groups in Firewall Threat Defense. Confirm that these mappings match your expectations.

    Note

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

- **Object & 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 ASA 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 ASA access control policy rules that were expanded from a single ASA 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 ASA 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 ASA access control policy rules that have IPS Policy applied. Review these rules carefully and determine whether the feature is supported in Firewall Threat Defense.
        - **Access Control Rules that have File Policy Applied**–Details of all ASA access control policy rules that have File Policy applied. Review these rules carefully and determine whether the feature is supported in Firewall Threat Defense.
        - **Access Control Rules that have Rule 'Log' Setting Change**–Details of the ASA 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 ASA 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 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 management center.

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

> **Note**
>
> If you need to apply IPS or file policy to an ACL in the **Review and Validate** page, create a policy on the management center before migration. This is highly recommended. Use the same policy, as the Firewall Migration Manager fetches the policy from the connected 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, see Management Center Configuration Guide, Version 6.2.3.

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:
      - Access control lists (ACL)
      - Network Address Translation rules
      - Port and network objects
      - Routes
      - Interfaces
      - IP SLA objects
      - Object Group Search
      - Time-based objects
      - VPN objects
      - Site-to-Site VPN Tunnels

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

      For information on how to configure these items and rules, see the Management Center Configuration Guide. 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 ASA configuration.