Migrating FDM-managed device to Cisco Secure Firewall Threat Defense Using Firewall Migration Manager

Firewall Migration Manager
Updated October 15, 2026

© 2026 Cisco Systems, Inc. All rights reserved.

Abbreviated Cisco Trademarks

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

Topics included

1 About Firewall Migration Manager.....5
Overview of Firewall Migration Manager.....6
Features in Firewall Migration Manager.....7
Default home page of Firewall Migration Manager.....10

2 Migration Requirements.....11
License requirements.....12
Platform requirements.....12
Device requirements.....12
Supported platforms and versions.....13
Firewall Management Center requirements.....14
FDM-managed device requirements.....15
Requirements and prerequisites for Threat Defense devices.....15
Supported FDM-managed device configurations for migration.....16
Guidelines and Limitations.....20
Obtain the FDM-managed device configuration File.....21
Export the FDM-managed device configuration file.....22
Connect to the FDM-managed device from Firewall Migration Manager.....25
Export PKI certificate from Device Manager and import into Firewall Management Center.....26
Retrieve AnyConnect packages and profiles.....27

3 FDM-managed device to Firewall Threat Defense Migration Workflow.....31
FDM-managed device to Firewall Threat Defense migration workflow.....32
Migrate FDM-managed device using Firewall Migration Manager.....32
Connect to Firewall Management Center and select a target device.....34
Map source configurations to the target device.....36
Review and validate the migration configuration.....37
Review the Firewall Migration Manager pre-migration report.....40
Review the Firewall Migration Manager post-migration report.....41

1 About Firewall Migration Manager

Topics:

- Overview of Firewall Migration Manager
- Features in Firewall Migration Manager
- Default home page of Firewall Migration Manager

Introduces the Firewall Migration Manager application and explains how it facilitates the migration process from FDM-managed device to Secure Firewall Threat Defense configurations.

Overview of Firewall Migration Manager

Learn how to use the Firewall Migration Manager to automate and streamline the migration of FDM-managed device configurations to Cisco Secure Firewall Threat Defense.

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

Why choose Firewall Migration Manager

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

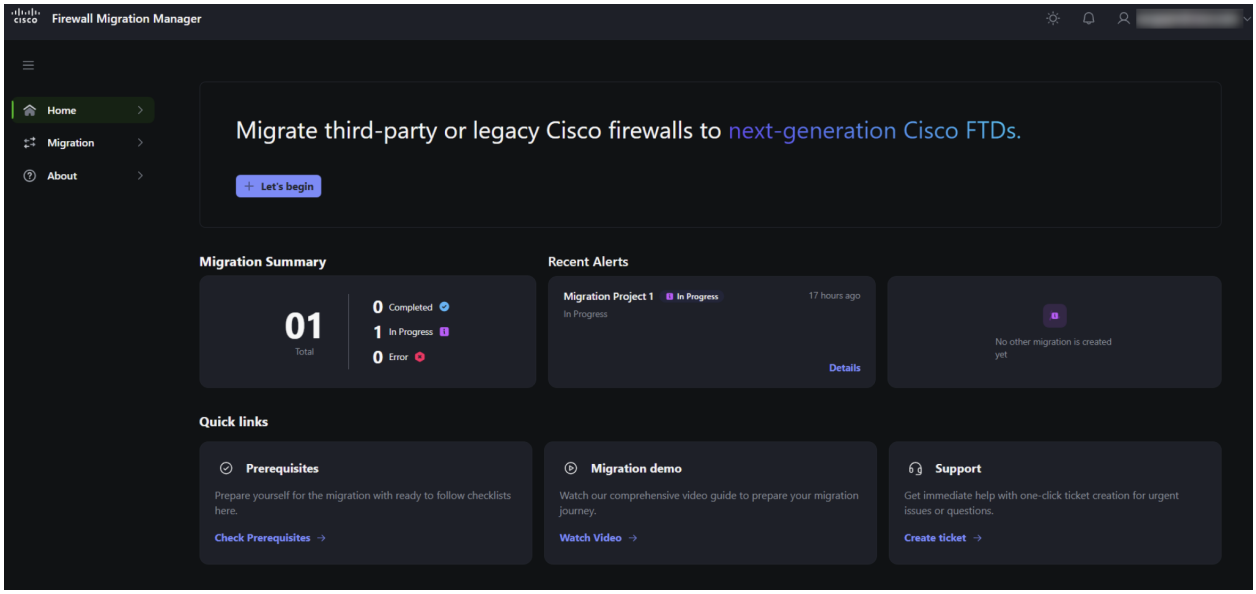
The Firewall Migration Manager an enterprise-ready product built for overcoming these challenges and to migrate seamlessly. The product helps customers and partners by offering predictable timelines, resilient workflows, and clear visibility at every stage of migration to Cisco Secure Firewall Threat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

Key features

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

Dashboard overview

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



Key functional areas:

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

Features in Firewall Migration Manager

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

This table summarizes the new features in Firewall Migration Manager.

Release	Features	Details
10.1.0.2	Support for FDM-managed device to Firewall Threat Defense migration.	Firewall Migration Manager supports migration of the FDM-managed device configurations to a Firewall Threat Defense device.

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.
	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 application parses enterprise-scale configurations efficiently, handling thousands of rules in minutes.
	Migration history retention	

Release	Features	Details
		Keeps migration history across different projects so you can track and revisit previous migrations.
	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.

2 Migration Requirements

Topics:

- License requirements
- Platform requirements
- Device requirements
- Supported platforms and versions
- Firewall Management Center requirements
- FDM-managed device requirements
- Requirements and prerequisites for Threat Defense devices
- Supported FDM-managed device configurations for migration
- Guidelines and Limitations
- Obtain the FDM-managed device configuration File
- Export the FDM-managed device configuration file
- Connect to the FDM-managed device from Firewall Migration Manager
- Export PKI certificate from Device Manager and import into Firewall Management Center
- Retrieve AnyConnect packages and profiles

Lists the licensing, platform, device, and configuration requirements for migrating from FDM-managed device to Firewall Threat Defense using the Firewall Migration Manager.

License requirements

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

While the Firewall Migration Manager is free 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 are planning to perform migration in an air-gapped or isolated environment without internet access, contact Cisco TAC to obtain the air-gapped Firewall Migration Manager installer.

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

Device requirements

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

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

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

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

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

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

Supported platforms and versions

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

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

Component	Minimum Supported Version
FDM-managed device	7.2 and later
Firewall Management Center	7.2 and later
Target Firewall Threat Defense	7.2 and later

Supported source devices

- **Physical**: Firepower 1000, 2100, 4100, and Secure Firewall 200, 1200, 3100, 3200, 4200 series
- **Virtual**: Firewall Threat Defense, FDM Virtual on VMware, FVM, and Cloud (Azure/AWS).

> **Note**
>
> Secure Firewall 9300 Series and 6100 Series Firewall Threat Defense cannot be managed locally, it needs Management Center for management.

Supported target devices

- **Physical**: Firepower 1000, 2100, 4100, 9300 (SM modules), and Secure Firewall 220, 3100, 3200, 4200, 6100 series
- **Virtual**: Threat Defense on VMware (ESXi/vSphere Web client or standalone client) and Cloud (Azure/AWS).

> **Note**
>
> - For pre-requisites and pre-staging of Firewall Threat Defense Virtual in Azure, refer to Getting Started with Secure Firewall Threat Defense Virtual and Azure.
> - For pre-requisites and pre-staging of Firewall Threat Defense Virtual in AWS Cloud, refer to Threat Defense Virtual Prerequisites.

For each of these environments, once pre-staged 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.

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

Firewall Management Center requirements

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

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

- Smart Licensing: License requirements on page 12
- REST API:

  You must enable REST API (**System** (⚙) > **Configuration** > **REST API Preferences**).

> **Note**
>
> You must have an administrator user role in Firewall Management Center to enable REST API.

FDM-managed device requirements

Lists the requirements and prerequisites for the FDM-managed device configuration file.

You can obtain an FDM-managed device configuration bundle either manually or by connecting to a live FDM-managed device from Firewall Migration Manager. Manual upload is supported only for these options:

- Migrate Firewall Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware)
- Migrate Firewall Device Manager (Shared Configurations Only)

> **Note**
>
> A manual upload is not supported for **Migrate Firewall Device Manager (Includes Device & Shared Configurations)** option.

Before proceeding with the migration, ensure these prerequisites for FDM-managed device are met:

- Firewall Migration Manager supports configuration file from both global and per-virtual domain (VDOM) export.
- The configuration file must meet these requirements:
  - Contains only valid device manger CLI configurations.
  - Includes the version number.
  - Must not contain syntax errors.
  - Must have an extension of .zip.
  - Has a fully exported configuration that is exported from the device manager. For more information, refer to Export FDM-managed device configuration file.
  - Include at least one .txt file containing the configuration.
  - Keys should be provided for encrypted bundle. For unencrypted bundle, the encryption key can be left empty.
  - Has not been hand-coded or manually altered.

Requirements and prerequisites for Threat Defense devices

Requirements and prerequistes for threat defense devices, which need to reviewed before migrating Secure Firewall ASA, ASA with FPS, FDM-managed devices, Fortinet, Check Point, and PAN firewall configurations using Firewall Migration Manager.

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

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

- The target threat defense device must be registered with the management center.

> **Note**
>
> This is applicable only when you choose either **Migrate Firewall Device Manager (Shared Configurations Only)** migration option or **Migrate Firewall Device Manager (Includes Device and Shared Configurations) to FTD Device (New Hardware)** migration option.

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

> **Note**
>
> - Subinterfaces are not created by Firewall Migration Manager, only interface mapping is allowed.
> - Mapping across different interface types is allowed, for example: physical interface can be mapped to a port channel interface.

Supported FDM-managed device configurations for migration

Lists the fully, partially, and unsupported FDM-managed device configurations for migration.

Review the fully, partially, and unsupported FDM-managed device configurations for migration.

Supported FDM-managed device configurations

Firewall Migration Manager can fully migrate these FDM-managed device configurations:

- Network objects and groups
- Service objects (except for those service objects configured for a source and destination)

> **Note**
>
> Although Firewall Migration Manager does not migrate extended service objects (configured for a source and destination), referenced ACL and NAT rules are migrated with full functionality.

- Service object groups, except for nested service object groups

> **Note**
>
> Since nesting is not supported on the Firewall Management Center, Firewall Migration Manager expands the content of the referenced rules. The rules, however, are migrated with full functionality.

- IPv4 and IPv6 address FQDN objects and groups
- IPv6 address conversion support (interface, static routes, objects, ACL, and NAT)
- Access Control Policy
- Auto NAT and Manual NAT
- Static routes, ECMP routes
- Physical interfaces
- Secondary VLANs on FDM-managed device interfaces are not migrated to Firewall Threat Defense.
- Subinterfaces (subinterface ID will always be set to the same number as the VLAN ID on migration)
- Aggregate interfaces (Port channels)
- Virtual tunnel interface (VTI)
- Bridge groups (transparent mode only)
- IP SLA Monitor

  Firewall Migration Manager creates IP SLA Objects, maps the objects 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.
- Object Group Search

  Enabling object group search reduces memory requirements for access control policies that include network objects. 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 shared configuration flow and will be disabled.
  > - Time-based objects

- Time-based objects

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

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

Note

- You must manually migrate timezone configuration from source Fortinet firewall to the target Firewall Threat Defense device.

- Site-to-Site VPN Tunnels
  - Site-to-Site VPN–When Firewall Migration Manager detects crypto map configuration in the source FDM-managed device, 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 FDM-managed device
  - Route-based (VTI) FDM VPN
  - Certificate-based VPN migration from FDM-managed device
  - FDM-managed device trustpoint or certificates migration to the Firewall Management Center must be performed manually and is part of the pre-migration activity.
- Dynamic-Route Objects, BGP, and EIGRP
  - Policy-List
  - Prefix-List
  - Community List
  - Autonomous System (AS)-Path
- Remote Access VPN
  - SSL and IKEv2 protocol.
  - Authentication methods–AAA only, Client Certificate only, SAML, AAA, and Client Certificate.
  - AAA–Radius, Local, LDAP, and AD.
  - Connection Profiles, Group-Policy, Dynamic Access Policy, LDAP Attribute Map, and Certificate Map.
  - Standard and Extended ACL.
  - As part of pre-migration activity, perform the following:
    - Migrate the FDM-managed device 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 FDM-managed device.
    - Upload all AnyConnect packages to the Firewall Management Center.
    - Upload AnyConnect profiles directly to the Firewall Management Center or from Firewall Migration Manager.

- Malware and file policies
  - Firewall Migration Manager adds the malware and file policies from your FDM-managed device to the respective rules in an access control policy, which gets pushed to the target management center.
  - Default file policies such as Block Malware All and Malware Cloud Look up - No Block are created.
- SSL decryption policies
- SNMP
  - For SNMPv1 and SNMPv2, ensure the community string is updated manually in the **Optimize, Review and Validate Configuration** page.
  - For SNMPv3, ensure the user authentication and user encryption passwords are provided manually in the **Optimize, Review and Validate Configuration**.

Partially supported FDM-managed device configurations

Firewall Migration Manager partially supports these FDM-managed device 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 that are configured with advanced logging settings, such as severity and time-interval.
- Static routes that are configured with the track option.
- Certificate-based VPN migration.
- Dynamic-Route Objects, EIGRP, and BGP
  - Route-Map

Unsupported FDM-managed device configurations

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

- SGT-based access control policy rules
- SGT-based objects
- User-based access control policy rules
- NAT rules that are configured with the block allocation option
- Objects with an unsupported ICMP type and code
- Tunneling protocol-based access control policy rules

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

- NAT rules that are configured with SCTP
- NAT rules that are configured with host ‘0.0.0.0’
- Default route obtained through DHCP or PPPoE with SLA tracking

- SLA monitor schedule
- Transport mode IPsec transform-set
- FDM-managed device trustpoint migration into Firewall Management Center
- Transparent firewall mode for BGP
- SNMPv3 user groups and host groups

Objects in FDM-managed device and Threat Defense

An FDM-managed device configuration file contains these objects that you can migrate to threat defense:

- Network objects
- Service objects, which are called port objects in Threat Defense
- IP SLA objects
- Time-based objects
- VPN objects (IKEv1/IKEv2 Policy, IKEv1/IKEv2 IPsec-Proposal)
- Dynamic route objects (Policy-List, Prefix-List, Community-List, AS-Path, Access-List, and Route-Map)
- BGP and EIGRP supported in routed mode
- RA VPN objects
- Group policy
- AAA objects (Radius, SAML, Local Realm, AD/LDAP/LDAPS Realm)
- Address pool (IPv4 and IPv6)
- Connection profile
- LDAP attribute map
- IKEv2 policy
- IKEv2 IPsec-Proposal
- Certificate map
- DAP
- Intrusion policy
- Intrusion rules

Guidelines and Limitations

Lists the guidelines for migrating FDM-managed device configurations.

Review these guidelines for FDM-managed device configurations before the migration.

Guidelines for FDM-managed device migration

- Each FDM-managed device object has a unique name and configuration–Firewall Migration Manager migrates the objects successfully without changes.

- The name of an FDM-managed device object includes one or more special characters that are not supported by the management center—Firewall Migration Manager renames the special characters in the object name with a "_" character to meet the management center object naming criteria.
- An FDM-managed device object has the same name and configuration as an existing object in the management Center—Firewall Migration Manager reuses the management center object for the threat defense configuration and does not migrate the FDM-managed device object.
- Multiple FDM-managed device objects have the same name but in different cases—Firewall Migration Manager renames such objects to meet the threat defense object naming criteria.

> **Note**
>
> 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.

Limitations for FDM-managed device configuration

Migration of your source FDM-managed device configuration has these limitations:

- Dynamic routing protocols, like OSPF, are not automatically migrated.
- If the source FDM-managed device 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 on the FDM-managed device, then, on migration to the threat defense, the corresponding rules will not behave in the same way they do on the FDM-managed device. We recommend that you create specific tunnel rules for these in the Prefilter policy, on the threat defense.
- Supported FDM-managed device crypto map will be migrated as point-to-point topology.

Limitations for RA VPN Migration

Remote Access VPN migration is supported with these limitations:

- Custom attributes, SSL settings and VPN load balancing migration is not supported.
- For a radius server, if dynamic authorization is enabled, the AAA server connectivity should be through an interface and not dynamic routing. If FDM-managed device configuration is found with AAA server with dynamic authorization enabled without interface, Firewall Migration Manager ignores dynamic authorization. You must enable dynamic-authorization manually after selecting an interface on the management center.
- 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.

Obtain the FDM-managed device configuration File

Describes the methods for obtaining FDM-managed device configuration file.

You can use one of these methods to obtain an FDM-managed device configuration file:

- Export the FDM Configuration File
- Connect to the FDM-managed device from Firewall Migration Manager on page 25

Export the FDM-managed device configuration file

Follow these steps to export and download the configuration file for an FDM-managed device.

This task is only required if you want to manually upload an FDM-managed device configuration file. The configuration file from the device manager can be exported using the threat defense API. When the configuration is exported, the system creates a ZIP file. The ZIP file can be downloaded to the local workstation. The configuration itself is represented as objects defined using attribute-value pairs in a JSON-formatted text file.

When you do an export, you must specify which configurations to be included in the export file. A full export includes all the configuration in the export zip file.

The export zip file might include the following:

- Attribute-value pairs that define each configured object. All configurable items are modeled as objects, not just those which are called “objects” in the device manager.
- Remote Access VPN, the AnyConnect packages, and any other referenced files such as the Client profile XML files, the DAP XML file, and Hostscan packages.
- Referenced clean list or custom detection list if you have configured custom file policies.

Procedure

1. Create the JSON object body for the export.

   Example
   Following is an example of the JSON object.

```
  "diskFileName": "string",
  "encryptionKey": "*********",
  "doNotEncrypt": false,
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": true,
  "entityIds": [
    "string"
  ],
  "jobName": "string",
  "type": "scheduleconfigexport"
}
```

   The attributes are,

   - **diskFileName**–(Optional) The name of the export zip file. If you do not specify a name, the system generates a name by default. Even if you specify a name, the system might append characters to the name to ensure uniqueness. The name has a maximum length of 60 characters.
   - **encryptionKey**–An encryption key for the zip file. If you do not want to encrypt the file, skip this field, and specify **doNotEncrypt: true** instead. If you specify a key, use the key to open the zip file after you download it to your local machine. The exported configuration file exposes the secret keys, passwords, and other sensitive data in clear text (otherwise they cannot be imported). In this case you might want to apply an encryption key to protect sensitive data. The system uses AES 256 encryption.
   - **doNotEncrypt**–(Optional) Whether the export file should be encrypted (false), or not encrypted (true). The default is false, which means you must specify a non-empty encryption key attribute. If you specify true, then the encryption key attribute is ignored.
   - **configExportType**–You can select any of the following export types for exporting the configuration files:

    - FULL_EXPORT–Includes the entire configuration in the export file. **This is the default option and should be selected for migration.**

- **deployedObjectsOnly**–(Optional) Whether to include objects in the export file only if they have been deployed. The default is false, which means all pending changes are included in the export. Specify true to exclude pending changes.
- **entityIds**–A comma-separated list of the identities with a set of starting-point objects enclosed in [brackets]. The list is required for a PARTIAL_EXPORT job. Each item the list could be either a UUID value or an attribute-value pair matching patterns like "id=uuid-value", "type=object-type" or "name=object-name". For example, "type=networkobject"
    - The type can be a leaf entity, such as network object, or an alias of a set of leaf types. Some typical type aliases are: network (NetworkObject and NetworkObjectGroup), port (all TCP/UDP/ICMP port, protocol and group types), url (URL objects and groups), ikepolicy (IKE V1/V2 policies), ikeproposal (Ike V1/V2 proposals), identitysource (all identity sources), certificate (all certificate types), object (all object/group types that would be listed in the device manager on the Objects page), interface (all network interfaces, s2svpn (all site-to-site VPN related types), ravpn (all RA VPN related types), vpn (both s2svpn and ravpn).
    - All the objects and their outgoing referential descendants will be included in the PARTIAL_EXPORT output file. All the unexportable objects will be excluded from the output even if you specify their identities. Use the GET method for the appropriate resource types to obtain the UUIDs, types, or names for the target objects.

  For example, to export all network objects, plus an access rule named myaccessrule, and two objects identified by UUID, you can specify:

```
"entityIds": [
   "type=networkobject",
   "id=bab3e3cd-8c70-11e9-930a-1f12ee87d473",
   "name=myaccessrule",
   "acc2e3cd-8c70-11e9-930a-1f12ee87b286"
   ]",
```

- **jobName**–(Optional) Giving the export job a name will make it easier to find it when you retrieve job status.
- **type**–The job type is always **scheduleconfigexport**.

2. Post the object.

   Example
   The curl command would look like the following:

```
  curl -X POST --header 'Content-Type: application/json' --header 'Accept:
application/json' -d '{ \
   "configExportType": "FULL_EXPORT", \
   "type": "scheduleconfigexport" \
}' 'https://10.89.5.38/api/fdm/latest/action/configexport'
```

3. Verify the response.

   You should get a response code of 200. If you posted the minimum JSON object, the successful response body would look like the following:

```
{
  "version": null,
  "scheduleType": "IMMEDIATE",
  "user": "admin",
  "forceOperation": false,
```

```
  "jobHistoryUuid": "c7a8ba61-629a-11e9-8b8d-0fcc3c9d6d0b",
  "ipAddress": "10.24.5.177",
  "diskFileName": "export-config-1",
  "encryptionKey": null,
  "doNotEncrypt": true
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": false,
  "entityIds": null,
  "jobName": "Config Export",
  "id": "c79be920-629a-11e9-8b8d-85231be77de0",
  "type": "scheduleconfigexport",
  "links": {
    "self": "https://10.89.5.38/api/fdm/latest
/action/configexport/c79be920-629a-11e9-8b8d-85231be77de0"
  }
}
```


4. Check the status of configuration export.

   It takes some time for an export to complete. The larger the configuration, the more time the job will require. Check the job status to ensure it completes successfully before you try to download the file.

   The simplest way to retrieve status is to use **GET /jobs/configexportstatus**. For example, the curl command would look like the following:

```
curl -X GET --header 'Accept: application/json'
'https://10.89.5.38/api/fdm/latest/jobs/configexportstatus'
```

   A successfully completed job diplays the following status:


```
{
  "version": "hdy62yf5xp3vf",
  "jobName": "Config Export",
  "jobDescription": null,
  "user": "admin",
  "startDateTime": "2019-04-19 13:14:54Z",
  "endDateTime": "2019-04-19 13:14:56Z",
  "status": "SUCCESS",
  "statusMessage": "The configuration was exported successfully",
  "scheduleUuid": "1ef502ad-62a5-11e9-8b8d-074ebc750708",
  "diskFileName": "export-config-1.zip",
  "messages": [],
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": false,
  "entityIds": null,
  "id": "1f0aad8e-62a5-11e9-8b8d-bb1ebb4d1300",
  "type": "configexportjobstatus",
  "links": {
    "self": "https://10.89.5.38/api/fdm/latest
/jobs/configexportstatus/1f0aad8e-62a5-11e9-8b8d-bb1ebb4d1300"
  }
}
```


5. Download the export file.

   When an export job completes, the export file is written to the system disk and is called a configuration file. You can download this export file to your local machine using the **GET /action/downloadconfigfile/{objId}**.

To get a list of the available files, use the GET /action/configfiles method.

```
curl -X GET --header 'Accept: application/json'
'https://10.89.5.38/api/fdm/latest/action/configfiles'
```

The response would show a list of items, each of which is a configuration file. For example, the following list shows 2 files. The id for all files are default and as a best practice you can ignore the ID and use the diskFileName instead.

```
{
  "items": [
    {
      "diskFileName": "export-config-2.zip",
      "dateModified": "2019-04-19 13:32:28Z",
      "sizeBytes": 10182,
      "id": "default",
      "type": "configimportexportfileinfo",
      "links": {
       "self": "https://10.89.5.38/api/fdm/latest/action/configfiles/default"

      }
    },
    {
      "diskFileName": "export-config-1.zip",
      "dateModified": "2019-04-19 13:14:56Z",
      "sizeBytes": 10083,
      "id": "default",
      "type": "configimportexportfileinfo",
      "links": {
       "self": "https://10.89.5.38/api/fdm/latest/action/configfiles/default"

      }
    }
  ],
```

Download the file using the diskFileName as the object ID.

```
curl -X GET --header 'Accept: application/octet-stream'
'https://10.89.5.38/api/fdm/latest/action/downloadconfigfile/export-config-2.zip'
```

The file is downloaded to your default downloads folder. If you are issuing the GET method from the API Explorer, and your browser is configured to prompt for download location, you will be prompted to save the file.

Note

A successful download will result in a 200 return code and no response body.

Connect to the FDM-managed device from Firewall Migration Manager

Configure FMM to connect to an FDM-managed device and migrate necessary configuration settings.

Before you begin

Firewall Migration Manager can connect to an FDM-managed device that you want to migrate and extract the required configuration information. Live connect to FDM-managed device is supported for all three use cases.

- Download and open the Firewall Migration Manager.
- Select the use case you want to carry out for FDM-managed device to management center migration.
- Obtain the management IP address, administrator credentials of the device manager.

Procedure

1. On the **Source Configuration** screen, in the **Connect to Firewall** section, click **Connect** to connect to the FDM-managed device that you want to migrate
2. In the **Connect to Firewall** section, enter the following information:
   a. In the **IP Address/Hostname/FQDN** field, enter the management IP address or hostname of the FDM. Click **Login**.
   b. In the **Username**, **Password** fields enter the appropriate administrator login credentials.
   c. Click **Connect & extract configuration**.

   When Firewall Migration Manager connects to the FDM-managed device, a series of compliance checks are performed on the FDM-managed device before proceeding with the migration. These checks are covered in the pre-requisites and best practices section. If the checks are successful, the migration proceeds to the next step.

   Firewall Migration Manager connects to the FDM-managed device, and once the compliance check succeeds, the tool starts extracting configuration information. When the extraction completes successfully, the parsed summary page is displayed.

   The **Parsed Summary** section displays the parsing status.
3. Review the summary of the elements that Firewall Migration Manager detected and parsed, from the FDM-managed device.
4. Click **Next**, to select the target parameters.

What to do next

Connect to Firewall Management Center and select a target device on page 34

Export PKI certificate from Device Manager and import into Firewall Management Center

Configure and migrate a PKI certificate between Device Manager and Firewall Management Center.

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

The imported FDM-managed device configuration bundle contains the certificate payload along with the keys. This can be imported on the management center

In the destination management center, migrate the trustpoint or the VPN certificates manually as PKI objects as part of the pre-migration activity. This activity must be performed before starting the migration using Firewall Migration Manager.

Procedure

1. From the configuration bundle, copy the certificate payload (Value between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----) and key (Value between -----BEGIN RSA PRIVATE KEY----- and -----END RSA PRIVATE KEY-----).

   Example


```
   "type":"identitywrapper",
   "action":"CREATE",
   "data":{
      "version":"girr7veykdjvx",
      "name":"RA_VPN_Cert",
      "cert":"-----BEGIN
[redacted]
 CERTIFICATE-----",
      "privateKey":"-----BEGIN RSA PRIVATE
[redacted]
 RSA PRIVATE KEY-----",
      "issuerCommonName":"mojave-rsa-root-2048-sha384.cisco.com, CN =
mojave-rsa-root-2048-sha384.cisco.com",
      "issuerCountry":"US",
      "issuerOrganization":"Cisco",
      "subjectCommonName":"fdm-ra-vpn-cert.cisco.com, CN = 172.16.10.50",
      "subjectCountry":"US",
      "subjectDistinguishedName":" C = US, O = Cisco, CN =
fdm-ra-vpn-cert.cisco.com, CN = 172.16.10.50",
      "subjectOrganization":"Cisco",
      "validityStartDate":"Jan  1 12:00:00 2012 GMT",
      "validityEndDate":"Sep  1 12:00:00 2034 GMT",
      "isSystemDefined":false,
      "keyType":"RSA",
      "keySize":2048,
      "allowWeakCert":false,
      "signatureHashType":"SHA1",
      "weakCertificate":true,
      "id":"9d0a8efb-01fa-11ed-8d7b-1f4809c453ac",
      "type":"internalcertificate"
   }
}
```


2. Import the PKI certificate into the management center (**ObjectManagement** > **PKIObjects**).

   For more information, refer to Firewall Management Center Configuration Guide.

   The manually created PKI objects can now be used in Firewall Migration Manager in the **Review and Validate Page** under the **VPN Tunnels** section.

Retrieve AnyConnect packages and profiles

Configure and download AnyConnect packages and profiles from the device manager.

Before you begin

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

- Ensure that Remote Access VPN on the management center has at least one AnyConnect package.

- Ensure that the Hostscan and External Browser packages are uploaded if they are a part of the configuration.
- Confirm all packages added to the management center as pre-migration activity.
- Ensure that the `Dap.xml` and `Data.xml` files are added through Firewall Migration Manager.

Procedure

1. Check the packages available on the device manager to download.

   Use the **GET /object/anyconnectpackagefiles** API to view the packages on the device.

   ```
   curl -X GET --header 'Accept: application/json' '
    https://10.89.5.38/api/fdm/v6/object/anyconnectpackagefiles'
   ```

   This command retrieves the available AnyConnect packages on the device manager.

   ```
   {
     "items": [
       {
         "version": "gx5yk7xkdsosu",
         "name": "anyconnect-win-4.10.02086-webdeploy-k9.pkg",
         "md5Checksum": "63e4a86fc7c68d7769b6a1b2976ffa73",
         "description": null,
         "diskFileName": "12f0988e-01fb-11ed-8d7b-07ecdd54c7bf.pkg",
         "platformType": "WINDOWS",
         "id": "133f2dbf-01fb-11ed-8d7b-89d64ab04e18",
         "type": "anyconnectpackagefile",
         "links": {
           "self": "
   https://10.89.5.38/api/fdm/v6/object/anyconnectpackagefiles/133f2dbf-01fb-11ed-8d7b-89d64ab04e18"

         }
       }
     ],
   }
   ```

   The `diskFilename` from the response is used to download the AnyConnect package.

2. Download the AnyConnect package.

   Use the **GET /action/downloaddiskfile/{objId}** to download the AnyConnect package to the local workstation. The object ID to be used is the diskFileName (12f0988e-01fb-11ed-8d7b-07ecdd54c7bf.pkg) of the AnyConnect package response.

   ```
   curl -X GET --header 'Accept: application/octet-stream'
   '
   https://10.89.5.38/api/fdm/v6/action/downloaddiskfile/12f0988e-01fb-11ed-8d7b-07ecdd54c7bf.pkg'
   ```

3. Check for available AnyConnect profiles on the device manager.

> **Note**
>
> The AnyConnect profiles are automatically retrieved from the device manager by Firewall Migration Manager. This step is only required if you want to manually upload the AnyConnect profile.

Use the **GET /object/anyconnectclientprofiles** to check the available profiles on the device manager.

```
curl -X GET --header 'Accept: application/json'
'https://10.196.155.3:12272/api/fdm/v6/object/anyconnectclientprofiles'
```

The following response will be displayed:

```
  "items": [

    {
      "version": "jqtwzirf36qke",
      "name": "AnyConnect_VPN_Profile",
      "md5Checksum": "e4ba581f84daec6f24c209f9f7f9e1fb",
      "description": null,
      "diskFileName": "1629395a-0384-11ed-8d7b-ab1a2a5ad583.xml",
      "anyConnectModuleType": "ANY_CONNECT_CLIENT_PROFILE",
      "id": "1754c10b-0384-11ed-8d7b-6b8e36ae1285",
      "type": "anyconnectclientprofile",
    }
  ]
}
```

The `diskFilename` from the response is used to download the AnyConnect profile.

4. Download the AnyConnect profile.

   Use the **GET /action/downloaddiskfile/{objId}** to download the AnyConnect package to the local workstation. The objId to be used is the diskFileName (1629395a-0384-11ed-8d7b-ab1a2a5ad583.xml) from the AnyConnect profiles response.

   ```
   curl -X GET --header 'Accept: application/octet-stream'
   'https://10.196.155.3:12272/api/fdm/v6/action/downloaddiskfile/1629395a-0384-11ed-8d7b-ab1a2a5ad583.xml'
   ```

5. Import the downloaded packages to management center (**ObjectManagement >)** > **VPN** > **AnyConnect File**.

   a. `Dap.xml` and `Data.xml` must be uploaded to the management center from 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 Firewall Migration Manager in the **Review and Validate** > **Remote Access VPN** > **AnyConnect File** section.

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

3 FDM-managed device to Firewall Threat Defense Migration Workflow

Topics:

- FDM-managed device to Firewall Threat Defense migration workflow
- Migrate FDM-managed device using Firewall Migration Manager

Learn how to migrate your FDM-managed device configurations to Firewall Threat Defense using the Firewall Migration Manager. This workflow covers configuration gathering, parsing, mapping, and validating configurations to ensure a successful transition to your target device.

FDM-managed device to Firewall Threat Defense migration workflow

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

Summary

Firewall Migration Manager automates the FDM-managed device configuration migration by ensuring accurate parsing, validation, and deployment of FDM-managed device configurations to a Firewall Threat Defense device.

Workflow

These stages describe how the FDM-managed device to Firewall Threat Defense device migration works:

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

Migrate FDM-managed device using Firewall Migration Manager

Guides you through migration of FDM-managed device configuration files using Firewall Migration Manager.

Before you begin

- Download the latest version of Firewall Migration Manager from Cisco Software Download Center.
- Ensure that you review all the Migration Requirements on page 11.
- Obtain the FDM-managed device configuration File on page 21
- Export PKI certificate from Device Manager and import into Firewall Management Center on page 26
- Retrieve AnyConnect packages and profiles on page 27
- For large configuration files, disable system sleep settings before you start the migration.
- When you want to migrate using **Migrate Firewall Device Manager (Includes Device & Shared Configurations)** migration option, ensure you complete these requirements:
  - Ensure connectivity between FDM device and FMC to move the device from FDM to FMC using FDM.

- User should have the FDM credentials to fetch details.
- Ensure out-of-band access to FTD device is available to handle the accessibility issues during migration.
- If the FTD devices are in failover pair, failover needs to be disabled before proceeding with moving manager from FDM to FMC.
- FMC should be registered to Smart Licensing Server.

Procedure

1. In Firewall Migration Manager, from the left pane, click **Migration** ( ), and click **Start new migration** on the top-right of the window.

   The migration workflow is initiated. Alternatively, you can click **Lets Begin** in the home page to start the migration.

   There are three migration workflows. Separate project will be created for each workflow. For each project, you can give a unique project name.

   > **Note**
   >
   > Click on the **Edit** icon to provide a name for the migration project. Then, click **Apply**.

2. In **Select Firewalls**, from the **Select source** drop-down list, choose **Cisco Secure Firewall Device Manager (7.2+)**.
3. Select the migration option by which you wish to migrate the FDM-managed device.
   - Migrate Firewall Device Manager (Shared Configurations Only)

     This option allows the migration of shared configuration to FMC. This option should be used when you do not have FTD and when you want to do staged migrations so that the shared configurations are migrated initially, and the device configuration can be migrated at a later point of time. There is no downtime involved in this use case.
   - Migrate Firewall Device Manager (Includes Device & Shared Configurations)

     This option allows shared and device configuration to be migrated to the destination management center. As part of this migration, the source threat defense is moved from device manager to management center. After successful completion of migration, the management center continues to manage the threat defense device. Hence, the source and destination are the same threat defense device in this use case. There is a downtime involved in this use case as the threat defense device is moved to the management center.
   - Migrate Firewall Device Manager (Includes Device and Shared Configurations) to FTD Device (New Hardware)

     This option allows the FDM-managed device configuration to be migrated to the threat defense that is already registered with the destination management center. The configuration of the source FDM-managed device is migrated to the user selected destination threat defense registered to the destination management center. There is no downtime involved in this use case.

     To connect and extract configuration of the source FDM-managed device, refer to Connect to the FDM-managed device from Firewall Migration Manager on page 25
4. For **Select configuration extraction method**, click **Manual upload** to upload a configuration file.

> **Note**
>
> Manual upload will be supported for the below two options:
>
> - Migrate Firewall Device Manager (Shared Configurations Only)
> - Migrate Firewall Device Manager (Includes Device and Shared Configurations) to FTD Device (New Hardware)

5. Connect to Firewall Management Center and select a target device on page 34.
6. Map source configurations to the target device on page 36.
7. Review and validate the migration configuration on page 37.
8. Review the Firewall Migration Manager pre-migration report on page 40.
9. Review the Firewall Migration Manager post-migration report on page 41.

Connect to Firewall Management Center and select a target device

Connect to Firewall Management Center, and select a target device for the FDM-managed device migration.

Before you begin

1. Obtain the credentials of the target Firewall Management Center.
2. If you need to apply an intrusion policy or file policy to an access control list (ACL) in the **Review and Validate** page, create the policy in Firewall Management Center before migration.

   Firewall Migration Manager retrieves policies from the connected Firewall Management Center. Reusing an existing policy helps avoid performance issues and migration push failures that can occur when you create and assign a new policy to multiple ACLs.
3. Start the migration workflow.
4. Import the FDM-managed device configuration files.

Procedure

1. In **Target Information**, if you want to connect to on-premises FMC then choose a Firewall Management Center from the **Select target** drop-down list.

   To connect to cdFMC, choose **SCC – Firewall Manager** from the **Select target** drop-down list. Select a region and provide an API token. Then, continue with Step 6.
2. Enter the IP address, hostname, or FQDN of the Firewall Management Center and click **Connect**.

   You can only migrate to the devices available in the selected domain.
3. In the **Login to target FMC** dialog box, enter the username and password, and click **Login**.

   Firewall Migration Manager logs in to the Firewall Management Center and retrieves a list of managed devices.

4. **Note**

   When you select **Migrate Firewall Device Manager (Shared Configurations Only)** migration option, you need not select any device. The shared configurations will be migrated and the configurations include the details of access control lists, NAT, and objects. Click **Next** to proceed further.

   - Click **Select FTD** to choose a single Firewall Threat Defense device or an HA pair.

5. If you choose the **Select FTD** option, from the **Select FTD** drop-down list, choose a Firewall Threat Defense device.

   Choose a target device that meets these requirements:

   - The device must have at least the same number of physical or port-channel interfaces as the source configuration.
   - The container instance must have at least the same number of physical or port-channel interfaces and subinterfaces.
   - The device must use the same firewall mode as the FDM-managed device.

   Interface names do not need to match between the source and target devices.

   After you select a device, you can view device details such as IP address, device version, device model, mode (routed or transparent), and multi-instance state.

6. If you select **Migrate Firewall Device Manager (Includes Device & Shared Configurations)** migration option, after connecting to the target FMC, you need to provide the details of required FDM device in **FDM Device Onboarding Details** section.

   a) Select between **FTD is behind NAT Device**, **FMC is behind NAT Device**, **No NAT device**.

   b) Provide these details:

      - **Management Center / CDO Hostname**: All the details will be fetched from the target manager. You can modify the IP if required.
      - **Management Center / CDO Registration Key**: Unique registration key needs to be provided which will be used while moving the manager.
      - **NAT ID**: (Optional.) Required when threat defense or management center is behind NAT Device.
      - **Threat Defense Hostname**: Threat Defense IP/hostname is fetched from FDM-managed device configuration. User can modify the IP if required. Field will be ignored if **FTD is behind NAT Device**.
      - **DNS Server Group**: DNS Server group used for connectivity between device manager and management center.
      - **Management Center/ CDO Access Interface**: Choose between Data/Management interface to move the manager. Data interface is supported only if proper routes are configured through Data Interface.

   c) Verify the details and click **Save**.

   If the target FMC is cdFMC, then in **FDM Device Onboarding Details** section, click **Update Details** and provide the FTD device name which you want to onboard. Then, click **Save**. The details of the FTD device will be fetched from the cdFMC.

7. Click **Next**.

What to do next

Map source configurations to the target device on page 36

Map source configurations to the target device

Map source configurations to the target device by assigning interfaces, security zones, interface groups, and applications, with options for automatic or manual mapping and validation to ensure accurate migration.

Firewall Migration Manager retrieves a list of interfaces of the source and target device, and maps them according to their identities. For example, 'management-only' interfaces are mapped automatically and cannot be changed.

Before you begin

1. Start the migration workflow.
2. Import the FDM-managed device configuration files.
3. Connect to Firewall Management Center and select a target device on page 34

Procedure

1. In **Mappings**, click the **Interfaces** tab to map the source and target device interfaces.

   Note

   When you choose **Migrate Firewall Device Manager (Shared Configurations Only)** migration option, you need not map the interfaces.

   a) (Optional) Click **Auto Map** to automatically map the source and target device interfaces.

   A **Confirm Auto-Creation** pop-up window is displayed. If you click **Auto create**, Firewall Migration Manager automatically maps FDM-managed device interfaces to existing security zones and interface groups in Firewall Management Center with matching names. If no match is found, Firewall Migration Manager creates a new security zone and interface group in Firewall Management Center using the interface name.

   b) To manually map the interfaces, from the **FTD interface** drop-down list, choose the interface.

   Note

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

   c) Review, validate and edit the mapping, if required.

2. Click the **Security zones** tab to map the source security zones with the Firewall Management Center security zones and interface groups.

   In Firewall Management Center, access control policies and NAT policies use interface objects. These interface objects are grouped into:

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

a) (Optional) Click **Auto Map** to automatically map the source and target device security zones.
b) To manually map the security zones, configure:
   - From the **FMC Security Zones** drop-down list, choose a security zone.
c) To add a new security zone .

> **Note**
>
> When you choose **Migrate Firewall Device Manager (Shared Configurations Only)** migration option, you need to click **Add Zones**.

d) Click the **Security zones (SZ)** tab and in the **Add new security zone** field, enter the security zone name and click **Add**.
e) Click **Save & Close**.

3. Click the **Applications** tab to map the source and target device applications automatically.

   If the Firewall Migration Manager unable to map the applications, you must manually choose the application from the **Target application/Ports** field.

   Click **Validate mappings** to validate the applications.

4. Click **Next**.

What to do next

Review and validate the migration configuration on page 37

Review and validate the migration configuration

Review and validate the migrated FDM-mangaed device configuration before deployment.

Before you push the migrated FDM-mangaed device configuration to the Firewall Management Center, review the configuration carefully and resolve any conflicts. Firewall Migration Manager identifies issues and allows remediation. 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.

Procedure

---

1. In the left pane of the Firewall Migration Manager click **Review**.

   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.

2. Click **Download Pre-Migration Report** to review the pre-migration report.

   For more information, refer to Review the Firewall Migration Manager pre-migration report on page 40.

3. Review access control configurations.
   a. Click **Access Control** in the **Shared configurations** area
   b. Check mappings for each entry and verify them.

c. If you do not want to migrate specific access control list policies, deselect them and from the **Bulk actions** drop-down list, click **Do not migrate**.

Rules not chosen for migration will be grayed out.

d. In the **Edit rule** dialog box, update the existing data or add new data.

To add an object to source or destination:

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

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

e. To apply a Firewall Management Center file policy to one or more access control policies, select the policies and choose **Actions** > **File Policy**.

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

g. To apply a Firewall Management Center IPS policy to one or more access control policies, select the policies and choose **Actions** > **IPS Policy**.

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

h. To update the logging options for an access control rule,select the rule 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**, 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.

i. To change actions for migrated access control rules in the Access Control table, select the rules, and choose **Actions** > **Rule Action**.

In the **Rule Action** dialog from the **Actions** drop-down, you can click the **ACP** tab.

4. Click these tabs and review the configuration items:
   - Interfaces
   - Routes (Static)
   - Access Control
   - NAT
   - Objects (Network objects, Port objects, URL objects, and objects)
   - Site-to-Site VPN

> **Note**
>
> For VPN configurations, review VPN filter configurations and extended access list objects.
>
> To exclude specific NAT rules or route interfaces from migration, deselect as needed, choose **Actions** > **Do not migrate**, and click **Save**. Excluded rules are grayed out.

a. (Optional) To rename network or port objects, in the **Network Objects** or the **Port Objects** tab, select the object and choose **Actions** > **Rename**.

   Access rules and NAT policies referencing renamed objects are updated accordingly.

b. Review routes from the **Routes** section. Select routes you do not want to migrate, and choose **Actions** > **Do not migrate**.

5. Review and validate site-to-site VPN tunnels:

   In the **Site-to-Site VPN Tunnels** section, review the VPN tunnel data from the source firewall such as **Source Interface**, **VPN Type**, and **IKEv1** and **IKEv2** configurations and provide preshared key values as needed.

6. Optional: Click **Download** to download details for each configuration item in the grid.
7. Resolve migration issues listed in the **Actions** area. Click **Remediate** to resolve the issues.

   For example, to avoid conflicts with existing Firewall Management Center objects, add a suffixe to object names. Select the object and choose **Actions** > **Add suffix** to apply the default suffix, or enter a suffix manually.

   When errors are resolved, a tick mark appears next to each error.

> **Note**
>
> Ensure that all issues are resolved before proceeding with migration.

8. Validate the configuration.

a. After you complete your review, click **Validate**. The **Begin migration** dialog box appears with the validated configurations.

b. Confirm migration by checking the confirmation box and click **Begin Migration**.

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

c. Click **Next**.

9. Review migration results.

   After a successful migration, a summary and a link to the post-migration report appears.

a. Click **Download report** to download and save the post-migration report. A copy is also saved in the Resources folder.

b. If migration fails, review the post-migration report, log file, and unparsed file to troubleshoot the failure.

What to do next

Review the post-migration report.

Review the Firewall Migration Manager pre-migration report

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

Before migration, it's important to thoroughly review the pre-migration report. This report shows errors, unreferenced configurations, ignored configuration lines, and rules that were not migrated completely.

Incomplete rules can affect the source setup, block authorized traffic, or allow unintended traffic. After migration, refine rules and policies in Firewall Management Center to optimize traffic handling and system performance.

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.

   This report contains:

   - **Overall Summary**–Lists the supported configurations from the source device that can be migrated successfully to Firewall Management Center.

     While connecting to a live FDM-managed device, the summary includes the hit count information, the number of times a rule was encountered and its timestamp information.

   - **Unsupported Configuration**–Displays details of FDM-managed device configurations that are not migrated. 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**–Displays details of unsupported configuration by Firewall Management Center, or not parsed by Firewall Migration Manager because they are irrelevant to the target device. Review these and verify whether each feature is supported in Firewall Management Center. If required, configure the features manually in Firewall Management Center.

   - **Unreferenced Configuration**–Displays the details of FDM-managed device configurations defined in the source configuration but are not used in any access-group, prefix list, VPN, or policy. These items will not be migrated. Decide whether to remove them from the source or manually add them to the target device.

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

What to do next

After the migration, review and adjust migrated configurations as needed to optimize performance and ensure compliance.

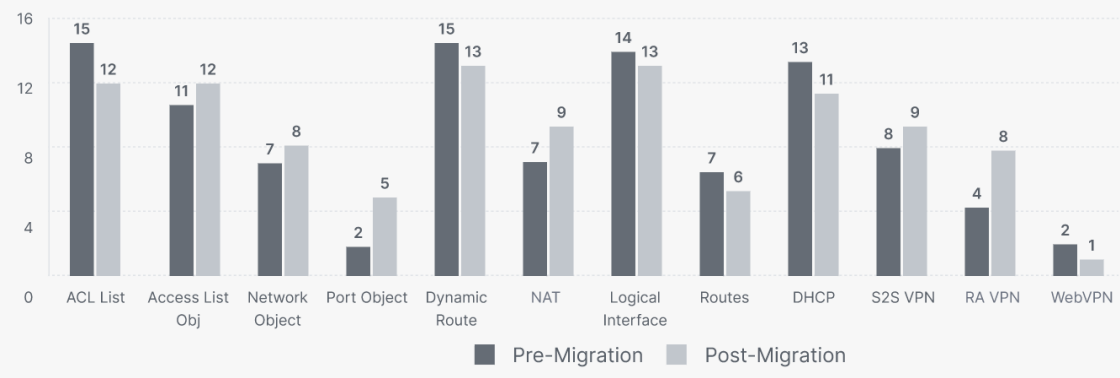
Review the Firewall Migration Manager post-migration report

Review the post-migration report to understand how your FDM-managed device configuration was migrated and identify any configurations that require manual migration.

The post-migration report provides details about the source and target devices such as policies, interface and zone mapping, ACL rules, ACL optimization, and the overall optimization performed on the configuration. It also provides details about partially migrated configurations and errors that occurred during migration. The report also offers guidance on resolving the errors.

Procedure

1. Open the **Post-migration report**.
2. Review the post-migration report:
   - **Summary Overview**–View comparison charts showing pre-migration and post-migration states.



   - **Device Details**–View summary of source and target devices.
   - **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.
     - **Interface-to-Interface Mapping**–Displays the successfully migrated interfaces and the mappings between the source and target device interfaces.

       Note

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

     - Source **Interface Names to Security Zones and Interface Groups**–Displays the successfully migrated logical interfaces and how you mapped them to security zones and interface groups in a Firewall Threat Defense device. Confirm these mappings.

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

- **Object & ACL Anomalies**
  - **Object Conflict Handling**–Displays objects that were split or renamed to avoid conflicts in the Firewall Management Center.
  - **ACL Category Conflict Handling**–Displays the category names that were trimmed to fit Firewall Management Center naming limits.
  - **Optimization**–Displays objects renamed to avoid conflicts, or reused where an identical object already existed in Firewall Management Center.
  - **Reused Objects**–Displays objects that the Firewall Migration Manager reused because they already existed in Firewall Management Center with an identical configuration.
  - **Access Control Rules, NAT, and Routes You Chose Not to Migrate**–Displays the rules that you chose not to migrate with the Firewall Migration Manager. Review these rules that were disabled by the Firewall Migration Manager and were not migrated. If required, you can configure these rules manually.
- **Migration Issues**
  - **Partially Migrated Configuration**–Displays partially migrated rules, including rules with unsupported advanced options. Review these rules, verify whether the advanced options are supported in Firewall Management Center, and if so, configure these options manually.
  - **Policy Rules Failing Zone Lookup**–Displays rules that could not resolve a source or destination zone during migration.
  - **Expanded Access Control Rules**–Displays access control policy rules that were expanded from a single FDM-managed device point rule into multiple Firewall Threat Defense rules during migration.
- **Action Taken on Features**
  - **Action Taken on Converted Features**–Displays VPN policies and deprecated settings that were automatically adjusted during migration.
  - **Actions Taken on Access Control Rules**
    - **Access Rules You Chose Not to Migrate**–Displays access control rules that you chose not to migrate with the Firewall Migration Manager. Review these rules. If required, configure these rules manually.
    - **Access Rules with Rule Action Change**–Displays 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 rules. If required, configure these rules manually.
    - **Access Control Rules that have IPS Policy and Variable Set Applied**–Displays all access control policy rules that have IPS policies. Review these rules carefully and determine whether the feature is supported in a Firewall Threat Defense device.
    - **Access Control Rules that have File Policy Applied**–Displays all access control policy rules that have File Policy applied. Review these rules carefully and determine whether the feature is supported in a Firewall Threat Defense device.

- **Access Control Rules that have Rule 'Log' Setting Change**–Displays the access control rules that had **Log setting** changed using the Firewall Migration Manager. The Log Setting values are: False, Event Viewer, Syslog. Review these rules. If required, configure these rules manually.
- **Access Control Rules that have failed Zone-lookup**–Displays access control rules that fail the route-lookup operation. 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**–Displays tunnel rules that are migrated as a prefilter tunnel rule during migration.

- **Errors & Failures**–Items that failed to migrate to Firewall Management Center.

  Error report may indicate an incorrect migrated configuration or a conflict within the Firewall Management Center caused by existing configurations or unsupported features. Review each error and apply the suggested remedies. Verify the corrections before proceeding or resuming the configuration push to the target Firewall Management Center.

> **Note**
>
> - Unsupported rules are not migrated to prevent unwanted traffic from passing through the Firewall Threat Defense device. Configure a rule in Firewall Management Center to block this traffic by the Firewall Threat Defense.
> - If you need to apply an intrusion policy or file policy to an access control list (ACL) on the **Review and Validate** page, create the policy in Firewall Management Center before migration.
>
>   Firewall Migration Manager retrieves policies from the connected Firewall Management Center. Reuse the same policy to avoid performance issues and possible push failures when assigning policies to multiple targets.

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

3. In Firewall Management Center, perform these actions:
   a) Review the migrated configuration for the Firewall Threat Defense device to confirm that all expected rules and other configuration items, including the following, were migrated:
      - Interfaces
      - Routes (Static)
      - Access Control
      - NAT
      - Objects (Network objects, Port objects, URL objects, and objects)
      - Site-to-Site VPN

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

      For information on how to configure these items and rules, refer to Firewall Management Center Configuration Guides.

4. After your review and manual configurations are complete, 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 source device configuration.