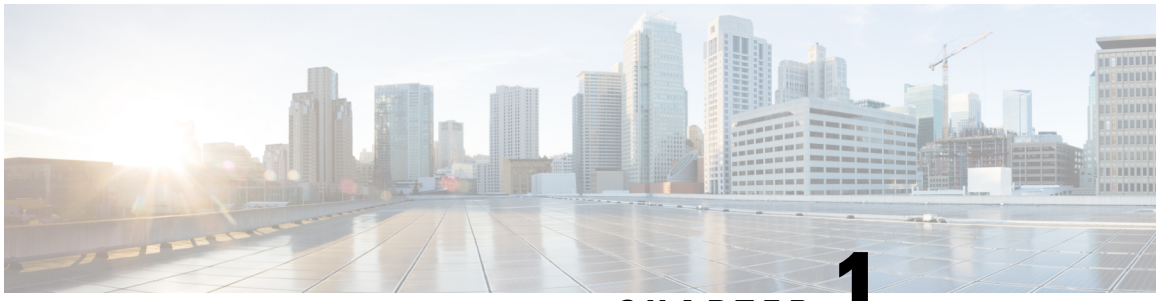
Cisco Secure Firewall Management Center Model Migration Guide

First Published: 2019-09-23

Last Modified: 2023-11-27

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

About Secure Firewall Management Center Model Migration

Secure Firewall Management Center allows you to migrate from one management center model to another management center model. After the migration, configurations and events from the source management center are available in the target management center.

From Version 7.2, Firepower Management Center (FMC) is rebranded as Secure Firewall Management Center (management center). Firepower Threat Defense (FTD) is rebranded as Secure Firewall Threat Defense (threat defense).

This chapter contains the following sections:

What's New in Management Center Model Migration

Feature	Version
Migrate Firepower Management Center 1000, 2500, or 4500 to Secure Firewall Management Center 1700, 2700, or 4700	7.4.x
Migrate Firepower Management Center 1600, 2600, or 4600 to Secure Firewall Management Center 1700, 2700, or 4700	7.4.x
Migrate Firepower Management Center 4600 to Secure Firewall Management Center Virtual 300 (FMCv300) for AWS	7.4.x

Supported Migration Paths

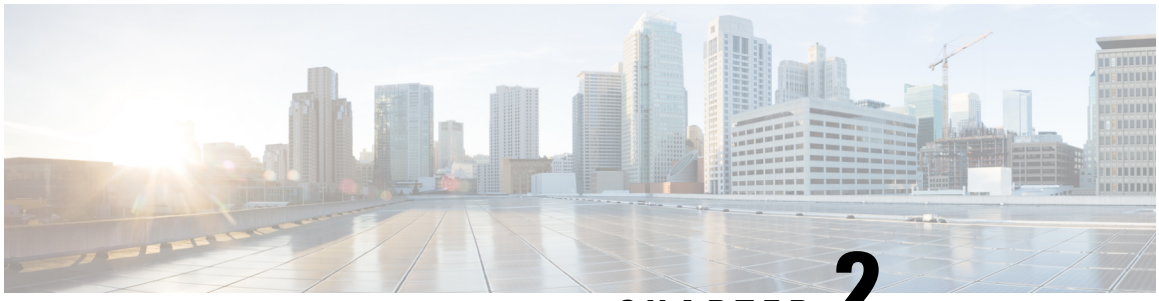
This guide describes the new features of the on-prem to on-prem model migration, which was first introduced in Management Center Version 6.5.

If you want to migrate Management Center 1000/2500/4500/1600/2600/4600 to a cloud-delivered Firewall Management Center (cdFMC), see the chapter Migrate On-Prem Management Center Managed Secure Firewall

Threat Defense to Cloud-Delivered Firewall Management Center in *Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator*.

The following table lists the supported target management center models that you can migrate to from your source (current) management center model.

Maximum Managed Devices	Source Model	Target Model							
		FMC 1600	FMC 2600	FMC 4600	Management Center 1700	Management Center 2700	Management Center 4700	FMCv300 (VMware)	FMCv300 (AWS)
2	FMCv2 (VMware)	Yes	Yes	Yes	—	—	—	Yes	—
10	FMCv10 (VMware)	Yes	Yes	Yes	—	—	—	Yes	—
25	FMCv25 (VMware)	Yes	Yes	Yes	—	—	—	Yes	—
50	FMC 1000	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—
50	FMC 1600	—	Yes	Yes	Yes	Yes	Yes	Yes	—
250	FMC 2000	—	Yes	Yes	—	—	—	Yes	—
300	FMC 2500	—	Yes	Yes	—	Yes	Yes	Yes	—
300	FMC 2600	—	—	Yes	—	Yes	Yes	Yes	—
300	FMCv300 (VMware)	—	Yes	Yes	—	—	—	—	—
750	FMC 4000	—	—	Yes	—	—	—	—	—
750	FMC 4500	—	—	Yes	—	—	Yes	—	—
750	FMC 4600	—	—	—	—	—	Yes	—	Yes
50	Management Center 1700	—	—	—	Yes	Yes	Yes	—	—
300	Management Center 2700	—	—	—	—	Yes	Yes	—	—
1000	Management Center 4700	—	—	—	—	—	Yes	—	—



CHAPTER 2

Migrate Your Management Center from the Source Model to the Target Model

This chapter provides information about the prerequisites and the workflow for the management center model migration.

Prepare for Migration

General Prerequisites

- See Supported Migration Paths, on page 1 to determine which target model you can migrate to from your source model.
- Management center model migration supports all management center licensing modes, including evaluation, connected, and Specific License Reservation (SLR).
- Ensure that the target management center has the same number of interfaces as your source management center.
- Verify that the target management center version matches the source management center version (including patch,Vulnerability Database [VDB], Lightweight Security Package [LSP], and Snort Rule Update [SRU]). To verify, in each management center choose **Help** > **About**.
- Verify that all the pending deployments are completed successfully.
- Configure the backup file in the source management center:

  1. Choose **System** (⚙) > **Backup/Restore**.
  2. Click the **Backup Mangement** tab and click **Firewall Mangement Backup**.
  3. Check the following check boxes:
     - **Back Up Configuration**

- **Backup Events**
- **Backup Threat Intelligence Director**

- Confirm that you have the correct number of threat defense entitlements in Cisco Smart Software Manager (CSSM).
- If a management center migrates to a higher platform and manages more threat defense devices, you must acquire the required licenses for the additional threat defense devices.
- If the source management center is Unified Capabilities Approved Products List (UCAPL) compliant or Common Criteria (CC) compliant, after migration, the target management center will also be UCAPL or CC compliant.
- For management center HA migrations:
  - If the target management centers are in HA, you must pause the synchronization in the target management centers before the migration.
  - Ensure that you meet all the HA requirements. For more information, see:
    - For versions 6.5 to 7.1, see the Requirements for Firepower Management Center High Availability topic in the *Firepower Management Center Configuration Guide*.
    - For Version 7.2 and later, see the Requirements for Management Center High Availability topic in the *Cisco Secure Firewall Management Center Administration Guide*.
- After migration, you must deregister the licenses from the source management center and register the licenses in the target management center.
- After migration, if you want to manage a different group of threat defense devices in the source management center:
  - Ensure that source management center cannot reach the stale threat defense devices.
  - Delete the stale devices that are now managed by the target management center.

Note If the source management center can reach the stale devices, these devices will be deregistered from the target management center.

Prerequisites for Migrating Management Center 1000, 2500, or 4500 to Management Center 1700, 2700, or 4700

1. Ensure that Management Center 1000, 2500, or 4500 and all the corresponding managed threat defense devices are Version 7.0.x.

   We recommend that you use Version 7.0.5.

2. Upgrade Management Center 1000, 2500, or 4500 from Version 7.0.x to 7.4.x. This upgrade is only for migration.

   You can download the upgrade package from here: Special Release. Unzip (but do not untar) the upgrade package before uploading it to the on-prem management center.

For more information about the upgrade, see the *Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*

Prerequisites for Management Center 1600, 2600, or 4600 to Management Center 1700, 2700, or 4700

- Upgrade Management Center 1600, 2600, or 4600 to 7.4.x. For more information about upgrade, see *Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center*.
- Ensure that the source management center manages only threat defense devices with Version 7.0.x.

Prerequisites for Migrating Management Center 4600 to Management Center Virtual 300 (FMCv300) for AWS

- Note that Management Center Virtual 300 has lower limits than Management Center 4600. We recommend that you refer to the following table before you migrate.

Table 1: Compatibility Check for Migrating Management Center 4600 to Management Center Virtual 300 for AWS

Performance and Functionality	Management Center 4600 (Current Configuration)	Management Center Virtual 300 (Maximum Limit)
Overall size (Event Storage Space)	3.2 TB	2 TB
Total devices	750	300
Maximum IPS events	300 million	60 million
Memory	128 GB	64 GB
CPU	Two Intel Xeon 4214 processors	32 vCPUs
Maximum network map size (hosts/users)	600,000/600,000	150,000/150,000
Maximum event rate (events per second)	20,000 eps	12,000 eps

- Ensure that the source Management Center 4600 and the target Management Center Virtual 300 for AWS are Version 7.4.x.
- Ensure that Management Center Virtual 300 for AWS has a license.
- From Version 7.4.x, after migration, you must update the following parameters:
  - IP address of the target management center
  - Manager details in all the managed threat defense devices. For more information, see Update the Management Center IP Address or Hostname on the Threat Defense Device, on page 12.

Limitations for Migrating Management Center 1000/2500/4500/1600/2600/4600 to Management Center 1700/2700/4700

- For the migration, you can upgrade Management Center 1000, 2500, or 4500 only from Version 7.0.x to 7.4.x. Upgrades from 7.0.x to 7.1.x, 7.2.x, or 7.3.x are not available.

- You cannot use Management Center 1000, 2500, or 4500 with Version 7.4.x to manage threat defense devices. Upgrades from 7.0.x to 7.4.x support only migration to Management Center 1700, 2700, or 4700.
- You cannot migrate Management Center 1000, 2500, 4500, 1600, 2600, or 4600 that manage the following types of devices:
  - Any threat defense device earlier than Version 7.0.x.
  - NGIPSv or FirePOWER services.

Standalone Management Center Model Migration Workflow

The following flowchart illustrates the workflow for migrating a source management center to a target management center.

Note Ensure that you meet the prerequisites described in Prepare for Migration, on page 3.

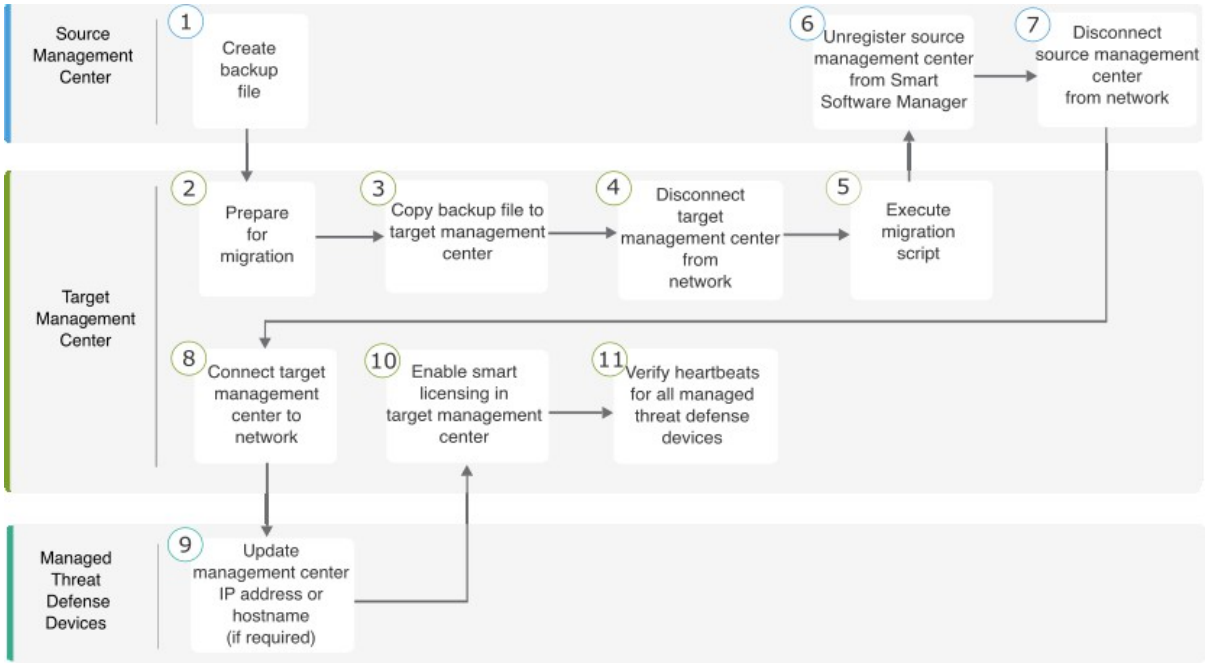


Table 2: Standalone Management Center Model Migration Workflow

Step	Task	More Info
1	Create a backup file in the source management center.	For versions 6.5 to 7.1, see the Back Up the FMC topic in the *Firepower Management Center Configuration Guide*. For Version 7.2 and later, see the Back Up the Management Center topic in the *Cisco Secure Firewall Management Center Administration Guide*.
2	Prepare for migration.	See Prepare for Migration, on page 3.
3	Copy the generated backup file to the target management center.	For versions 6.5 to 7.1, see the Restore an FMC from Backup topic in the *Firepower Management Center Configuration Guide*. For Version 7.2 and later, see the Restore Management Center from Backup topic in the *Cisco Secure Firewall Management Center Administration Guide*.
4	Disconnect the target management center from the network.	Physically disconnect the target management center from the network.
5	Execute the migration script in the target management center.	See How to Use the Management Center Model Migration Script, on page 11.
6	Unregister your source management center from Cisco Smart Software Manager (CSSM).	For versions 6.5 to 7.1, see the Deregister a Firepower Management Center from the Cisco Smart Software Manager topic in the *Firepower Management Center Configuration Guide*. For Version 7.2 and later, see the Deregister the Management Center topic in the *Cisco Secure Firewall Management Center Administration Guide*.
7	Disconnect the source management center from the network.	Physically disconnect the source management center from the network.
8	Connect the target management center to your network.	After a successful migration, the target management center gets the IP address of the source management center. If required, you can assign a new IP address to the target management center. If you change the management center IP address after migration, you must do the following: • Update the Management Center IP Address or Hostname on the Threat Defense Device, on page 12. • Update the NAT configuration between the management center and its managed devices.
9	Update the manager details on all the managed threat defense devices, if required.	See Update the Management Center IP Address or Hostname on the Threat Defense Device, on page 12.

Step	Task	More Info
10	Enable smart licensing in the target management center.	For versions 6.5 to 7.1, see the License Requirements for Firepower Management Center topic in the *Firepower Management Center Configuration Guide*. For Version 7.2 and later, see the Configure Smart Licensing topic in the *Cisco Secure Firewall Management Center Administration Guide*.
11	Verify the heartbeats for all the threat defense devices managed by the target management center. Verify that the data is migrated successfully to the target management center.	Log in to the target management center. Verify that all the configurations are restored and basic management center operations such as policy editing, deployment, and scheduled jobs work as expected.

Management Center High-Availability Model Migration Workflow

You can migrate your management center HA setup by executing the migration script on the target primary management center and secondary management center.

The following flowchart illustrates the workflow for migrating your management center HA setup from the source models to the target models.

Note Ensure that you meet the prerequisites described in Prepare for Migration, on page 3.

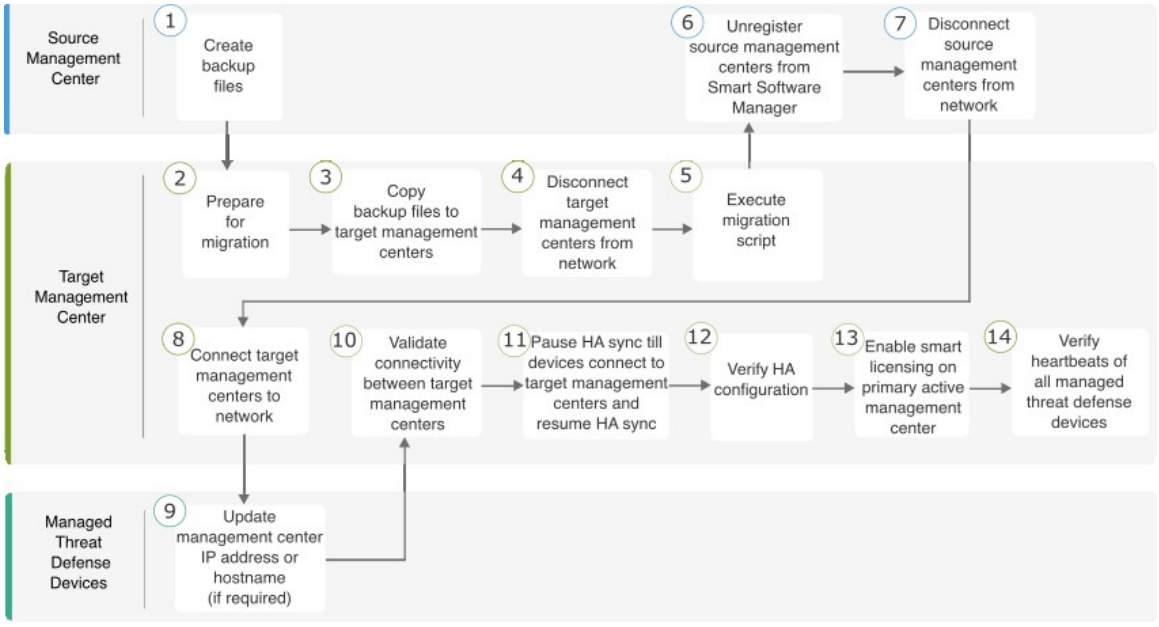


Table 3: Firewall Management Center High-Availability Model Migration Workflow

Step	Task	More Info
1	Create a backup file in each of the source management centers. The backup pauses the HA synchronization.	For versions 6.5 to 7.1, see the Back Up the FMC topic in the *Firepower Management Center Configuration Guide* For Version 7.2 and later, see the Back Up the Management Center topic in the *Cisco Secure Firewall Management Center Administration Guide*.
2	Set up the target management centers.	See Prepare for Migration, on page 3.
3	Copy the generated backup files to the target management centers. Ensure that you do the following: • Copy the backup file from the source primary management center to the target primary management center. • Copy the backup file from the source secondary management center to the target secondary management center.	For versions 6.5 to 7.1, see the Restore an FMC from Backup topic in the *Firepower Management Center Configuration Guide*. For Version 7.2 and later, see the Restore Management Center from Backup topic in the *Cisco Secure Firewall Management Center Administration Guide*.
4	Disconnect target management centers from the network. **Note** If the target management centers are in HA, before the migration, you must pause the synchronization on the target management centers.	Physically disconnect the target management centers from the network.
5	Execute the migration script in the target management centers.	How to Use the Management Center Model Migration Script, on page 11
6	Unregister your source management centers from the Cisco Smart Software Manager (CSSM).	For versions 6.5 to 7.1, see the Deregister a Firepower Management Center from the Cisco Smart Software Manager topic in the *Firepower Management Center Configuration Guide*. For Version 7.2 and later, see the Deregister the Management Center topic in the *Cisco Secure Firewall Management Center Administration Guide*.
7	Disconnect source management centers from the network.	Physically disconnect the source management centers from the network.

Step	Task	More Info
8	Connect the target management centers to the network.	After a successful migration, the target management centers get the IP addresses of the source management centers. If required, you can assign new IP addresses. If you change the management center IP address after migration, you must do the following: • Update the Management Center IP Address or Hostname on the Threat Defense Device, on page 12. • Update the NAT configuration between the management center and its managed devices.
9	Update the manager details on all the managed threat defense devices, if required.	See Update the Management Center IP Address or Hostname on the Threat Defense Device, on page 12.
10	Validate connectivity between the target management centers.	For versions 6.5 to 7.1, see the Viewing Firepower Management Center High Availability Status topic in the *Firepower Management Center Configuration Guide*. For Version 7.2 and later, see the Viewing Management Center High Availability Status topic in the *Cisco Secure Firewall Management Center Administration Guide*.
11	Pause HA synchronization till the threat defenses connect to the target management centers and resume the HA synchronization.	For versions 6.5 to 7.1, see the Pausing Communication Between Paired Firepower Management Centers and Restarting Communication Between Paired Firepower Management Centers topics in the *Firepower Management Center Configuration Guide*. For Version 7.2 and later, see the Pausing Communication Between Paired Management Centers and Restarting Communication Between Paired Management Centers topics in the *Cisco Secure Firewall Management Center Administration Guide*.
12	Verify that the HA configuration of the management centers is healthy and that there are no alerts.	For versions 6.5 to 7.1, see the Viewing Firepower Management Center High Availability Status topic in the *Firepower Management Center Configuration Guide*. For Version 7.2 and later, see the Viewing Management Center High Availability Status topic in the *Cisco Secure Firewall Management Center Administration Guide*.

Step	Task	More Info
13	Register smart licensing in the target primary active management center.	For versions 6.5 to 7.1, see the License Requirements for Firepower Management Center topic in the Firepower Management Center Configuration Guide. For Version 7.2 and later, see the Configure Smart Licensing topic in the *Cisco Secure Firewall Management Center Administration Guide*.
14	Verify the heartbeats for all the threat defense devices managed by the target management center. Verify that the data is migrated successfully to the target management centers.	Log in to the target management center. Verify that all the configurations are restored and basic management center operations such as policy editing, deployment, and scheduled jobs work as expected.

How to Use the Management Center Model Migration Script

Perform the following procedure to use the migration script. Note that this procedure is only one part of the management center model migration. See Standalone Management Center Model Migration Workflow, on page 6 or Management Center High-Availability Model Migration Workflow, on page 8 for details about the full model migration workflow.

Procedure

Step 1 Log in to the target management center CLI.

Step 2 Run the **expert** command to switch to expert mode.

Step 3 Execute the migration command:

/var/sf/backup/sf-migration.pl *backup_file_path*

Example:

```
root@firepower:# /var/sf/bin/sf-migration.pl /var/sf/backup/100localbackup-2023-05-20examp.tar
```

Note that when the migration process is completed, the system reboots.

What to do next

Return to Standalone Management Center Model Migration Workflow, on page 6 or Management Center High-Availability Model Migration Workflow, on page 8 and complete all the remaining steps.

Update the Management Center IP Address or Hostname on the Threat Defense Device

After migration, if the network configuration of the target management center is different from that of the source management center, you must update the IP address or hostname of the management center on each threat defense device.

Procedure

Step 1 From the threat defense CLI, get the unique identifier for the management center using the **show managers** command:

Example:

```
> show managers
Type                      : Manager
Host                      : xx.xx.x.x
Display name              : xx.xx.x.x
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration and analytics
```

Step 2 Update the management center IP address or hostname using the **configure manager** command:

configure manager edit *fmc_uuid* **hostname** *fmc_ipaddress*

Example:

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname xx.xx.x.x
Updating hostname from xx.xx.x.x to xx.xx.x.x
Manager hostname updated.
```

Step 3 Update the management center display name using the **configure manager** command:

configure manager edit *fmc_uuid* **displayname** *fmc_ipaddress*

Example:

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 displayname xx.xx.x.x
Updating displayname from xx.xx.x.x to xx.xx.x.x
Manager displayname updated.
```

Step 4 Verify the updated management center configuration using the **show managers** command again.

Troubleshooting Management Center Model Migration

Table 4: Management Center Model Migration Error Messages

Error Message	Recommended Action
`Migration data size is greater than the storage space of the target management center.`	Increase the size of the target management center.

Error Message	Recommended Action
`Interface count mismatch.`	The source and target management centers must have the same number of interfaces. See Prepare for Migration, on page 3.
`No migration path exists from the Secure Firewall Management Center 4500 to Secure Firewall Management Center 2700.`	See Supported Migration Paths, on page 1.
`No migration path exists from the Secure Firewall Management Center 4600 to the Secure Firewall Management Center for VMware 300.`	You can migrate a Secure Firewall Management Center 4600 to only a Management Center Virtual 300 (FMCv300) for AWS or Secure Firewall Management Center 4700. See Supported Migration Paths, on page 1.
`No migration path exists from the Secure Firewall Management Center 4600 to Secure Firewall Management Center for Azure 300.`	
`Device count is more than 300.`	1. Reduce the device count in the source management center (Secure Firewall Management Center 4600). 2. Create a backup file in the source management center before migrating to the target management center (Management Center Virtual 300 [FMCv300] for AWS). See Prepare for Migration, on page 3.

Model Migration of Management Center 1000/2500/4500 or 1600/2600/4600 to Management Center 1700/2700/4700

For model migration of management center 1000/2500/4500 or 1600/2600/4600 to management center 1700/2700/4700:

If the migration does not function to your expectations and you want to switch back, note that Version 7.4 is unsupported for general operations on the 1000/2500/4500 and 1600/2600/4600 devices. To return the old management center to a supported version, you must reimage back to Version 7.0.x, and restore from backup.

For more information about reimaging the management center to Version 7.0.x, see the Getting Started Guide for your management center:

- For management center 1000/2500/4500, see Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide.
- For management center 1600/2600/4600, see Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide.