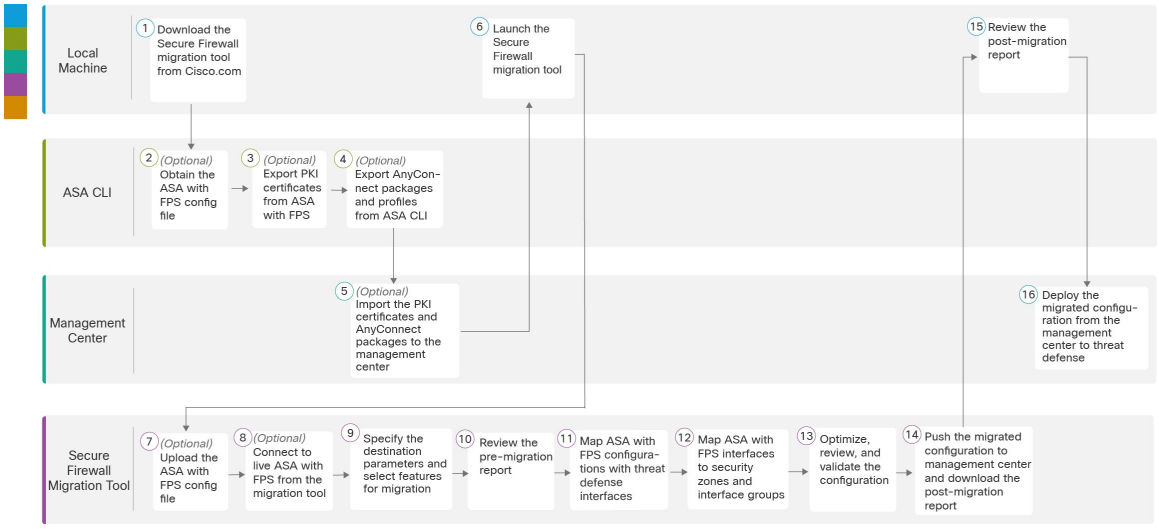
ASA with FPS to Threat Defense Migration Workflow

End-to-End Procedure

The following flowchart illustrates the workflow for migrating an ASA with FPS to threat defense using the Secure Firewall migration tool.



	Workspace	Steps
1	Local Machine	Download the latest version of Secure Firewall migration tool from Cisco.com. For detailed steps, see Download the Secure Firewall Migration Tool from Cisco.com.

	Workspace	Steps
2	ASA CLI	(Optional) Obtain the ASA with FPS configuration file: To obtain the ASA with FPS config file from ASA CLI, see Obtain the ASA with FPS Configuration File. If you intend to connect the ASA from Secure Firewall migration tool, skip to step 3.
3	ASA CLI	(Optional) Export PKI certificates from ASA CLI: This step is required only if you are planning to migrate site-to site VPN and RA VPN features from ASA to threat defense. To export the PKI certificates from ASA CLI, see Export PKI Certificate from ASA with FirePOWER Services and Import into Management Center. If you are not planning to migrate site-to-site VPN and RA VPN, skip to step 7.
4	ASA CLI	(Optional) Export AnyConnect packages and profiles from ASA CLI: This step is required only if you are planning to migrate RA VPN features from ASA with FPS to threat defense. To export AnyConnect packages and profiles from ASA CLI, see Retrieve AnyConnect Packages and Profiles. If you are not planning to migrate site-to-site VPN and RA VPN, skip to step 7.
5	Management Center	(Optional) Import the PKI certificates and Anyconnect packages to management center: To import the PKI certificates to management center, see Export PKI Certificate from ASA with FirePOWER Services and Import into Management Center and Retrieve AnyConnect Packages and Profiles.
6	Local Machine	Launch the Secure Firewall migration tool on your local machine, see Launch the Secure Firewall Migration Tool.
7	Secure Firewall Migration Tool	(Optional) Upload the ASA with FPS config file obtained from ASA CLI, see Upload the ASA with FPS Configuration File. If you are planning to connect to live ASA with FPS, skip to step 8.
8	Secure Firewall Migration Tool	You can connect to live ASA with FPS directly from the Secure Firewall migration tool. For more information, see Connect to the ASA from the Secure Firewall Migration Tool.
9	Secure Firewall Migration Tool	During this step, you can specify the destination parameters for the migration. For detailed steps, see Specify Destination Parameters for the Secure Firewall Migration Tool.
10	Secure Firewall Migration Tool	Navigate to where you downloaded the postmigration report and review the report. For detailed steps, see Review the Pre-Migration Report.
11	Secure Firewall Migration Tool	The Secure Firewall migration tool allows you to map the ASA with FPS configuration with threat defense interfaces. For detailed steps, see Map ASA with FPS Configurations with Secure Firewall Device Manager Threat Defense Interfaces.
12	Secure Firewall Migration Tool	To ensure that the ASA with FPS configuration is migrated correctly, map the ASA with FPS interfaces to the appropriate threat defense interface objects, security zones and interface groups. For detailed steps, see Map ASA with FPS Configurations with Secure Firewall Device Manager Threat Defense Interfaces.

	Workspace	Steps
13	Secure Firewall Migration Tool	Optimize and review the configuration carefully and validate that it is correct and matches how you want to configure the threat defense device. For detailed steps, see Optimize, Review and Validate the Configuration.
14	Secure Firewall Migration Tool	This step in the migration process sends the migrated configuration to management center and allows you to download the post-migration report. For detailed steps, see Push the Migrated Configuration to Management Center.
15	Local Machine	Navigate to where you downloaded the post migration report and review the report. For detailed steps, see Review the Post-Migration Report and Complete the Migration.
16	Management Center	Deploy the migrated configuration from the management center to threat defense. For detailed steps, see Review the Post-Migration Report and Complete the Migration.

Prerequisites for Migration

Before you migrate your ASA with FPS configuration, execute the following activities:

Download the Secure Firewall Migration Tool from Cisco.com

Before you begin

You must have a Windows 10 64-bit or macOS version 10.13 or higher machine with an internet connectivity to Cisco.com.

Step 1 On your computer, create a folder for the Secure Firewall migration tool.

We recommend that you do not store any other files in this folder. When you launch the Secure Firewall migration tool, it places the logs, resources, and all other files in this folder.

Note Whenever you download the latest version of the Secure Firewall migration tool, ensure, you create a new folder and not use the existing folder.

Step 2 Browse to https://software.cisco.com/download/home/286306503/type and click **Firewall Migration Tool**.

The above link takes you to the Secure Firewall migration tool under Firewall NGFW Virtual. You can also download the Secure Firewall migration tool from the threat defense device download areas.

Step 3 Download the most recent version of the Secure Firewall migration tool into the folder that you created.

Download the appropriate executable of the Secure Firewall migration tool for Windows or macOS machines.

Obtain the ASA with FPS Configuration File

You can use one of the following methods to obtain an ASA with FPS configuration file:

- Export the ASA with FPS Configuration File, on page 4
- Connect to the ASA from the Secure Firewall Migration Tool, on page 10

Export the ASA with FPS Configuration File

This task is required only if you want to manually upload an ASA with FPS configuration file. If you want to connect to an ASA with FPS from the Secure Firewall migration tool, skip to Connect to the ASA from the Secure Firewall Migration Tool, on page 10.

Note Do not hand code or make changes to the ASA with FPS configuration after you export the file. These changes will not be migrated to threat defense, and they create errors in the migration or cause the migration to fail. For example, opening and saving the configuration file in terminal can add white space or blank lines that the Secure Firewall migration tool cannot parse.

Ensure that the exported ASA with FPS configuration file does not contain the "--More--" keyword as text, as this can cause the migration to fail.

ASA with FPS configuration file migration into the Secure Firewall migration tool is a two-step process:

- You can import the ASA configuration file using the manual method or live-connect method.
- You must import the FPS configuration file by connecting to the Firewall Management Center that manages the FPS, and by selecting the required source ACL policy that must be migrated.

Step 1 Use the **show running-config** command for the ASA device or context that you are migrating and copy the configuration from there. See View the Running Configuration.

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

Note For a multi context ASA with FPS, you can use the **show tech-support** command to obtain the configuration for all the contexts in a single file.

Step 2 Save the configuration as either `.cfg` or `.txt`.

You cannot upload the ASA with FPS configuration to the Secure Firewall migration tool if it has a different extension.

Step 3 Transfer the ASA with FPS configuration file to your computer where you downloaded the Secure Firewall migration tool.

Export PKI Certificate from ASA with FirePOWER Services and Import into Management Center

Before you begin

The Secure Firewall migration tool supports migration of Certificate-based VPN into the management center.

ASA with FirePOWER Services uses the trustpoint model for storing certificates in the configuration. A trustpoint is a container in which certificates are stored. ASA with FirePOWER Services trustpoint can store up to two certificates.

The ASA with FirePOWER Services trustpoint or certificates in the ASA with FirePOWER Services configuration file contains hash values. Hence, you cannot directly import them into a management center.

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

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

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

Step 2 Import the PKI certificate into a management center (**Object Management PKI Objects)**.

For more information, see Firewall Management Center Configuration Guide.

The manually created PKI objects can now be used in the Secure Firewall migration tool in the **Review and Validate Page** under the **Trustpoint** section in **Remote Access VPN**.

Retrieve AnyConnect Packages and Profiles

AnyConnect profiles are optional and can be uploaded through the management center or Secure Firewall migration tool.

Before you begin

- Remote Access VPN on the management center requires at least one AnyConnect package.
- If the configuration consists of Hostscan and External Browser package, you must upload these packages.
- All packages must be added to the management center as part of the pre-migration activity.
- Dap.xml and Data.xml must be added through the Secure Firewall migration tool.

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

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

```
ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <----- Example of copying Dap.xml
ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Example of copying Data.xml
ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Example of copying Anyconnect Profile.
```

Step 2 Import the downloaded packages to management center (**Object Management** > **VPN** > **AnyConnect File**).

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

b. AnyConnect profiles can be uploaded directly to the management center or through the Secure Firewall migration tool in the **Review and Validate** > **Remote Access VPN** > **AnyConnect File** section.

The manually uploaded files can now be used in the Secure Firewall migration tool.

Run the Migration

Launch the Secure Firewall Migration Tool

This task is applicable only if you are using the desktop version of the Secure Firewall migration tool. If you are using the cloud version of the migration tool hosted on CDO, skip to .

Note When you launch the Secure Firewall migration tool a console opens in a separate window. As you go through the migration, the console displays the progress of the current step in the Secure Firewall migration tool. If you do not see the console on your screen, it is most likely to be behind the Secure Firewall migration tool.

Before you begin

- Download the Secure Firewall Migration Tool from Cisco.com
- Review and verify the requirements in the Supported Target Management Center for Migration section.
- Ensure that your computer has a recent version of the Google Chrome browser to run the Secure Firewall migration tool. For information on how to set Google Chrome as your default browser, see Set Chrome as your default web browser.
- If you are planning to migrate a large configuration file, configure sleep settings so the system doesn't go to sleep during a migration push.

Step 1 On your computer, navigate to the folder where you downloaded the Secure Firewall migration tool.

Step 2 Do one of the following:

- On your Windows machine, double-click the Secure Firewall migration tool executable to launch it in a Google Chrome browser.

  If prompted, click **Yes** to allow the Secure Firewall migration tool to make changes to your system.

The Secure Firewall migration tool creates and stores all related files in the folder where it resides, including the log and resources folders.

- On your Mac move, the Secure Firewall migration tool `*.command` file to the desired folder, launch the Terminal application, browse to the folder where the Secure Firewall migration tool is installed and run the following commands:

```
# chmod 750 Firewall_Migration_Tool-version_number.command
# ./Firewall_Migration_Tool-version_number.command
```

The Secure Firewall migration tool creates and stores all related files in the folder where it resides, including the log and resources folders.

Tip When you try to open the Secure Firewall migration tool, you get a warning dialog because the Secure Firewall migration tool is not registered with Apple by an identified developer. For information on opening an application from an unidentified developer, see Open an app from an unidentified developer.

Note Use MAC terminal zip method.

Step 3 On the **End User License Agreement** page, click **I agree to share data with Cisco Success Network** if you want to share telemetry information with Cisco, else click **I'll do later**.

When you agree to send statistics to Cisco Success Network, you are prompted to log in using your Cisco.com account. Local credentials are used to log in to the Secure Firewall migration tool if you choose not to send statistics to Cisco Success Network.

Step 4 On the Secure Firewall migration tool's login page, do one of the following:

- To share statistics with Cisco Success Network, click the **Login with CCO** link to log in to your Cisco.com account using your single sign-on credentials. If you do not have a Cisco.com account, create it on the Cisco.com login page.

  Proceed to step 8, if you have used your Cisco.com account to log in.

- If you have deployed your firewall in an air-gapped network that does not have internet access, contact Cisco TAC to receive a build that works with administrator credentials. Note that this build does not send usage statistics to Cisco, and TAC can provide you the credentials.

Step 5 On the **Reset Password** page, enter the old password, your new password, and confirm the new password.

The new password must have 8 characters or more and must include upper and lowercase letters, numbers, and special characters.

Step 6 Click **Reset**.

Step 7 Log in with the new password.

Note If you have forgotten the password, delete all the existing data from the <*migration_tool_folder*> and reinstall the Secure Firewall migration tool.

Step 8 Review the pre-migration checklist and make sure you have completed all the items listed.

If you have not completed one or more of the items in the checklist, do not continue until you have done so.

Step 9 Click **New Migration**.

Step 10 On the **Software Update Check** screen, if you are not sure you are running the most recent version of the Secure Firewall migration tool, click the link to verify the version on Cisco.com.

Step 11 Click **Proceed**.

What to do next

You can proceed to the following step:

- If you have exported ASA with FPS configuration to your computer, proceed to Upload the ASA with FPS Configuration File.
- If you want to extract information from an ASA with FPS using the Secure Firewall migration tool, proceed to Connect to the ASA from the Secure Firewall Migration Tool, on page 10

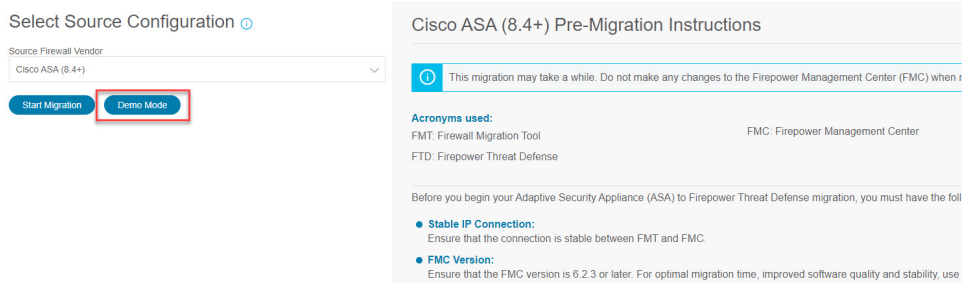
Using the Demo Mode in Firewall Migration Tool

When you launch the Secure Firewall Migration tool and are on the **Select Source Configuration** page, you can choose to start performing a migration using **Start Migration** or enter the **Demo Mode**.

Note This feature is applicable only if you are using the desktop version of Secure Firewall migration tool.

The demo mode provides an opportunity to try performing a demo migration using dummy devices, and visualize how an actual migration flow would look like. The migration tool triggers the demo mode based on the selection you make in the **Source Firewall Vendor** drop-down; you can also upload a configuration file or connect to a live device and continue with the migration. You can proceed performing the demo migration by selecting demo source and target devices such as demo FMC and demo FTD devices.

Caution Choosing **Demo Mode** erases any existing migration workflows. If you use the demo mode while you have an active migration in **Resume Migration**, your active migration is lost and needs to be restarted from first, after you use the demo mode.



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

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

Upload the ASA with FPS Configuration File

Before you begin

Export the configuration file as `.cfg` or `.txt` from the source ASA with FPS device.

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

Step 1 On the **Extract Cisco ASA (9.2.2+) with FPS Information** screen in the **Manual Upload** section, click **Upload** to upload the ASA with FPS Configuration file.

Step 2 Browse to where the ASA with FPS configuration file is located and click **Open**.

The Secure Firewall migration tool uploads the configuration file. For large configuration files, this step takes a longer time. The console provides a line by line log view of the progress, including the ASA with FPS configuration line that is being parsed. If you do not see the console, you can find it in a separate window behind the Secure Firewall migration tool. The **Context Selection** section identifies if the uploaded configuration corresponds to the multi-context .

Step 3 In the **Firewall Management Center IP Address/Hostname** field, enter the relevant details:

- Single context ASA with FPS—Management IP address or hostname
- Multi-context ASA with FPS—IP address of the admin context or hostname

Step 4 Click **Connect**.

Enter the following details in the **Firewall Management Center Login** screen.

- Username
- Password
- Click **Login** to connect to Firewall Management Center.

Step 5 The **Select FPS Device** drop-down, shows a list of FPS devices that is attached to the particular management center. Each device shows the device name with the associated ACL Policy.

Step 6 Review the **Context Selection** section and select the ASA with FPS context that you want to migrate.

Step 7 Click **Proceed**.

The access rules is fetched from the device.

Step 8 Click **Start Parsing**.

The **Parsed Summary** section displays the parsing status.

Step 9 Review the summary of the elements in the uploaded configuration file that the Secure Firewall migration tool detected and parsed.

Step 10 Click **Next** to select the target parameters.

What to do next

Specify Destination Parameters for the Secure Firewall Migration Tool, on page 11

Connect to the ASA from the Secure Firewall Migration Tool

The Secure Firewall migration tool can connect to an device that you want to migrate and extract the required configuration information.

Before you begin

- Download and launch the Secure Firewall migration tool.
- For single context ASA, obtain the management IP address, administrator credentials, and the enable password.
- For multi-context mode ASA, obtain the IP address of the **admin** context, administrator credentials, and the enable password.

Note If ASA is not configured with **Enable Password**, you can leave the field blank on the Secure Firewall migration tool.

Step 1 On the **Extract Cisco ASA (9.2.2+) with FPS Information** screen, in the **Connect to ASA** section, click **Connect** to connect to the ASA device that you want to migrate.

Step 2 On the **ASA Login** screen, enter the following information:

a. In the **ASA IP Address/Hostname** field, enter the management IP address or hostname (for single context ASA) or IP address of the admin context or hostname (for a multi-context ASA).

b. In the **Username**, **Password**, and **Enable Password** fields enter the appropriate administrator login credentials.

Note If ASA is not configured with an **Enable password**, you can leave the field blank on the Secure Firewall migration tool.

c. Click **Login**.

When the Secure Firewall migration tool connects to the ASA, it displays a successfully connected to the ASA message. For a multi-context ASA, the Secure Firewall migration tool identifies and lists the contexts.

Step 3 Select the context that you want to migrate from the **Context** drop-down list.

Step 4 (Optional) Select **Collect Hitcounts**.

When checked, this tool computes the number of times an ASA rule was used and the last time the rule was used since ASA uptime or last ASA restart and displays this information on the **Review and Validate** page. This allows you to evaluate the efficacy and relevance of the rule before migration.

Step 5 Click **Start Extraction**.

The Secure Firewall migration tool connects to the ASA and starts extracting configuration information. When the extraction completes successfully, the **Context Selection** section identifies if the uploaded configuration corresponds to a single-context or multi-context ASA.

Step 6 Review the **Context Selection** section and select the ASA context that you want to migrate.

Step 7 In the **Firewall Management Center IP Address/Hostname** field, enter the relevant details:

- Single context ASA with FPS—Management IP address or hostname
- Multi-context ASA with FPS—IP address of the admin context or hostname

Step 8 Click **Connect**.

Enter the following details in the **Firewall Management Center Login** screen:

- Username
- Password
- Click **Login** to connect to Firewall Management Center.

Step 9 The **Select FPS Device** drop-down, shows a list of FPS devices that is attached to the particular management center. Each device shows the device name with the associated ACL Policy.

Step 10 Click **Proceed**.

The access rules is fetched from the device.

Step 11 The **Parsed Summary** section displays the parsing status. The Secure Firewall migration tool parses the configuration file and disconnects from the ASA.

Step 12 Review the summary of the elements that the Secure Firewall migration tool detected and parsed in the uploaded configuration file.

Step 13 Click **Next** to select the target parameters.

What to do next

Specify Destination Parameters for the Secure Firewall Migration Tool, on page 11

Specify Destination Parameters for the Secure Firewall Migration Tool

Before you begin

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

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

Step 1 On the **Select Target** screen, in the **Firewall Management** section, do the following:

a) Click the **On-Prem FMC** radio button.
b) Enter the IP address or Fully-Qualified Domain Name (FQDN) for the management center.
c) In the **Domain** drop-down list, select the domain to which you are migrating.

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

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

Step 2 In the **Firewall Management Center Login** dialog box, enter the username and password of the dedicated account for the Secure Firewall migration tool, and click **Login**.

The Secure Firewall migration tool logs in to the management center and retrieves a list of threat defense devices that are managed by that management center. You can view the progress of this step in the console.

Step 3 On the **Select Target** screen, in the **Choose Threat Defense** section, you can either select a threat defense device that you want to migrate to, or if you do not have a threat defense device, you can migrate the shared policies (Access Control Lists, NAT, and Objects) of the ASA with FPS configuration to the management center.

Step 4 In the **Choose Threat Defense** section, do one of the following:

- Click the **Select Firewall Threat Defense Device** drop-down list and check the device where you want to migrate the ASA with FPS configuration.

  The devices in the selected management center domain are listed by **IP Address** and **Name**.

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

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

Table 1: ASA with FPS Firewall Features and Supported Management Center or Threat Defense Versions

Firewall Features	Supported Management Center or Threat Defense Version
ASA with FPS with remote deployment	6.7 or later
Crypto Map Site-to-Site VPN	6.6 or later
Virtual Tunnel Interface (VTI) and Route-based (VTI)	6.7 or later
ASA with FPS deployment	6.5 or later
Dynamic-Route Objects and BGP	7.1 or later
Remote Access VPN	• Management Center 7.2 or later • Threat Defense 7.0 or later.
EIGRP	• Management Center 7.2 or later • Threat Defense 7.0 or later.

Note To migrate Site-to-Site VPN, VTI, and Route-based (VTI) interfaces, threat defense must be configured on management center.

- For ASA 5505, the device-specific configs (Interface and routes) and shared policies (NAT, ACLs, and Objects) can be migrated only when the supported target threat defense platform is Firewall 1010 with management center version 6.5 or later.

  Note
  - If the target threat defense is not FPR-1010 or the target management center is earlier than 6.5, ASA 5505 migration support is applicable for shared policies only. Device specifics will not be migrated.
  - You can select only FPR-1010 in the **Select Device** drop-down list as the source config is ASA 5505.
  - ASA-SM migration support is for shared policies only. Device specifics will not be migrated.

- Click **Proceed without FTD** to migrate the configuration to the management center.

  When you proceed without threat defense, the Secure Firewall migration tool will not push any configurations or the policies to threat defense. Thus, interfaces and routes, and site-to-site VPN which are threat defense device-specific configurations will not be migrated and need to be manually configured on management center. However, all the other supported configurations (shared policies and objects) such as NAT, ACLs, and port objects will be migrated. Remote Access VPN is a shared policy and can be migrated even without threat defense.

Step 5 Click **Proceed**.

Depending on the destination that you are migrating to, the Secure Firewall migration tool allows you to select the features that you want to migrate.

Step 6 Click the **Select Features** section to review and select the features that you want to migrate to the destination.

- If you are migrating to a destination threat defense device, the Secure Firewall migration tool automatically selects the features available for migration from the ASA with FPS configuration in the **Device Configuration** and **Shared Configuration** sections. You can further modify the default selection, according to your requirements.
- If you are migrating to a management center, the Secure Firewall migration tool automatically selects the features available for migration from the ASA with FPS configuration in the **Shared Configuration** section. You can further modify the default selection, according to your requirements.

  Note The **Device Configuration** section is not available when you have not selected a destination threat defense device to migrate to.

  Note The **Device Configuration** section is not available when you have selected **Migrate Firepower Device Manager (Shared Configurations Only)**.

- The Secure Firewall migration tool supports the following for access control during migration:
  - Populate Destination Security Zones—Enables mapping of destination zones for the ACL during migration.

    Route-lookup logic is limited to Static Routes and Connected Routes, and PBR, Dynamic Routes, and NAT are not considered. Interface network configuration is used to derive the connected route information.

    Based on the nature of Source and Destination network object-groups, this operation may result in rule explosion.

  - Migrate unencrypted tunnels rules (ASA) as prefilter policy—Mapping of ASA encapsulated tunnel protocol rule to Prefilter tunnel rules and has the following advantages:
    - Tailor Deep Inspection—For encapsulated traffic and to improve performance with fastpathing.
    - Improve Performance—You can fastpath or block any other connections that benefit from early handling.

    The Secure Firewall migration tool identifies the encapsulated tunnel traffic rules in source configuration and migrates them as Prefilter tunnel rules. You can verify the migrated tunnel rule under the Prefilter policy. The Prefilter policy is associated with the migrated access control policy on management center.

    The protocols which are migrated as Prefilter tunnel rules are following:
    - GRE (47)
    - IPv4 encapsulation (4)
    - IPv6 encapsulation (41)
    - Teredo Tunneling (UDP:3544)

    Note If you do not opt to select the prefilter option, all the tunneled traffic rules will be migrated as unsupported rules.

    The ACL tunnel rules (GRE and IPnIP) in the ASA with FPS configuration are currently migrated as bidirectional by default. You can now specify the Rule direction for the destination as bidirectional or unidirectional in the access control state option.

- The Secure Firewall migration tool supports the following interfaces and objects for VPN Tunnel migration:
  - Policy-based (Crypto Map)—If the target management center and threat defense is version 6.6 or later.
  - Route-based (VTI)—If the target management center and threat defense is version 6.7 or later.

- The Secure Firewall migration tool supports migration of Remote Access VPN if the target management center is 7.2 or later. Remote Access VPN is a shared policy that can be migrated without threat defense. If migration is selected with threat defense, the threat defense version should be 7.0 or later.
- (Optional) In the **Optimization** section, select **Migrate only referenced objects** to migrate only those objects that are referenced in an access control policy and a NAT policy.

  Note When you select this option, unreferenced objects in the ASA with FPS configuration will not be migrated. This optimizes migration time and cleans out unused objects from the configuration.

- (Optional) In the **Optimization** section, select **Object group search** for optimal memory utilization by access policy on threat defense.
- (Optional) In the **Inline Grouping** section, the Secure Firewall migration tool allows you to clear the access rules of the pre-defined network and service object names that start with CSM or DM. If you uncheck this option, the pre-defined object names will be retained during migration. For more information, see Inline Grouping.

  Note By default, the option of Inline Grouping is enabled.

Step 7 Click **Proceed**.

Step 8 Click **Start Conversion** to initiate the conversion.

Step 9 In the **Rule Conversion/ Process Config** section, click **Start Conversion** to initiate the conversion.

Step 10 Review the summary of the elements that the Secure Firewall migration tool converted.

To check whether your configuration file is successfully uploaded and parsed, download and verify the **Pre-Migration Report** before you continue with the migration.

Step 11 Click **Download Report** and save the **Pre-Migration Report**.

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

What to do next

Review the Pre-Migration Report, on page 16

Inline Grouping

Object Grouping by ASDM and CSM Managed ASA

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

Note To change the behavior of the object grouping from **Tools** > **Preferences**, choose **Auto-expand network and service objects with specified prefix** rule table preference.

The following is the configuration snippet extracted using the **show run** command on ASA managed by ASDM.

```
object network host1
 host 10.1.1.100
object network fqdn_obj1
 fqdn abc.cisco.com
object-group network DM_INLINE_NETWORK_1
 network-object 10.21.44.189 255.255.255.255
 network-object 10.21.44.190 255.255.255.255
object-group network DM_INLINE_NETWORK_2
 network-object 10.21.44.191 255.255.255.255
 network-object object host1
 network-object object fqdn_obj1


access-list CSM_DM_ACL extended permit tcp object-group DM_INLINE_NETWORK_1 object-group
DM_INLINE_NETWORK_2
```

In the above example, access-list CSM_DM_ACL on ASDM UI does not show DM_INLINE group as rule's Source and Destination network instead displays contents of DM_INLINE group.

Inline Grouping—ASDM/CSM

The Inline Grouping functionality of the Secure Firewall migration tool allows you to parse **show running-configuration** of ASDM or CSM managed ASA devices. It provides an option to preserve the same UI representation of the access-list rules as on ASDM or CSM. If opted out, migrated rules will refer to DM_INLINE groups as recorded in ASA **show running-configuration**.

Note The source ASA configuration file input to the Secure Firewall migration tool would still be **show run** or **show tech** collected from ASA or via live connection to ASA device (SSH). The Secure Firewall migration tool does not support any other form of configuration files or methods.

The following figures show how the Source and Destination Network fields of ACE or RULE change based on the enabling or disabling the inline grouping option respectively.

Figure 1: With Inline Grouping—ASDM/CSM Enabled

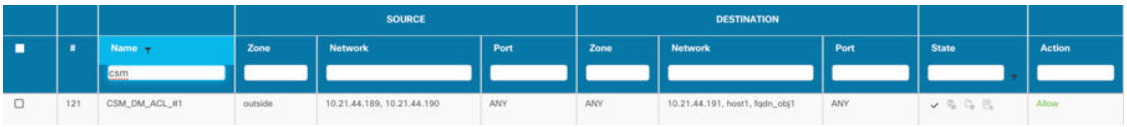


Figure 2: With Inline Grouping—ASDM/CSM Disabled

Review the Pre-Migration Report

If you have missed to download the Pre-Migration Reports during migration, use the following link to download:

Pre-Migration Report Download Endpoint—http://localhost:8888/api/downloads/pre_migration_summary_html_format

Note You can download the reports only when the Secure Firewall migration tool is running.

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

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

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

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

- **Overall Summary**—The method used to extract the ASA with FPS configuration information or manual upload for ASA with FPS.

  If connecting to a live ASA, the firewall mode detected on the ASA with FPS, and for multiple context mode, the context you chose for migration.

  A summary of the supported ASA with FPS configuration elements that can be successfully migrated to threat defense and specific ASA with FPS features selected for migration.

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

- **Configuration Lines with Errors**—Details of ASA with FPS configuration elements that cannot be successfully migrated because the Secure Firewall migration tool could not parse them. Correct these errors on the ASA with FPS configuration, export a new configuration file, and then upload the new configuration file to the Secure Firewall migration tool before proceeding.

- **Partially Supported Configuration**—Details of ASA with FPS configuration elements that can be only partially migrated. These configuration elements include rules and objects with advanced options where the rule or the object can be migrated without the advanced options. Review these lines, verify whether the advanced options are supported in management center, and if so, plan to configure those options manually after you complete the migration with the Secure Firewall migration tool.

- **Unsupported Configuration**—Details of ASA with FPS configuration elements that cannot be migrated because the Secure Firewall migration tool does not support migration of those features. Review these lines, verify whether each feature is supported in management center, and if so, plan to configure the features manually after you complete the migration with the Secure Firewall migration tool.

- **Ignored Configuration**—Details of ASA with FPS configuration elements that are ignored because they are not supported by the management center or the Secure Firewall migration tool. The Secure Firewall migration tool does not parse these lines. Review these lines, verify whether each feature is supported in management center, and if so, plan to configure the features manually.

For more information about supported features in management center and threat defense, see Management Center Configuration Guide.

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

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

What to do next

Map ASA with FPS Configurations with Secure Firewall Device Manager Threat Defense Interfaces

Map ASA with FPS Configurations with Secure Firewall Device Manager Threat Defense Interfaces

The threat defense device must have an equal or greater number of physical and port channel interfaces than those used by ASA with FPS configuration. These interfaces do not have to have the same names on both devices. You can choose how you want to map the interfaces.

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

The mapping of ASA with FPS interface to the threat defense interface differs based on the threat defense device type:

- If the target threat defense is of native type:
  - The threat defense must have equal or a greater number of used ASA with FPS interfaces or port channel (PC) data interfaces (excluding management-only and subinterfaces in the ASA with FPS configuration). If the number is less, add the required type of interface on the target threat defense.
  - Subinterfaces are created by the secure Firewall migration tool based on physical interface or port channel mapping.
- If the target threat defense is of container type:
  - The threat defense must have equal or a greater number of used ASA with FPS interfaces, physical subinterfaces, port channel, or port channel subinterfaces (excluding management-only in ASA with FPS configuration). If the number is less, add the required type of interface on the target threat defense. For example, if the number of physical interfaces and physical subinterface on the target threat defense is 100 less than that of ASA with FPS then you can create the additional physical or physical subinterfaces on the target threat defense.
  - Subinterfaces are not created by the Secure Firewall migration tool. Only interface mapping is allowed between physical interfaces, port channel, or subinterfaces.

Before you begin

Make sure you have connected to the management center and chosen the destination as threat defense. For more information, see Specify Destination Parameters for the Secure Firewall Migration Tool, on page 11.

Note This step is not applicable if you are migrating to a management center without a threat defense device.

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

You cannot change the mapping of the management interfaces. If a threat defense interface has already been assigned to an ASA with FPS interface, you cannot choose that interface from the drop-down list. All assigned interfaces are greyed out and unavailable.

You do not need to map subinterfaces. The Secure Firewall migration tool maps subinterfaces on the threat defense device for all subinterfaces in the ASA with FPS configuration.

Step 2 When you have mapped each ASA with FPS interface to a threat defense interface, click **Next**.

What to do next

Map the ASA with FPS interfaces to the appropriate threat defense interface objects, security zones, and interface groups. For more information, see Map ASA with FPS Interfaces to Security Zones and Interface Groups.

Map ASA with FPS Interfaces to Security Zones and Interface Groups

Note If your ASA with FPS configuration does not include Access Lists and NAT rules or if you choose not to migrate these policies, you can skip this step and proceed to Optimize, Review and Validate the Configuration, on page 20.

To ensure that the ASA with FPS configuration is migrated correctly, map the interfaces to the appropriate threat defense interface objects, security zones. In an ASA with FPS configuration, access control policies and NAT policies use interface names (nameif). In management center, those policies use interface objects. In addition, management center policies group interface objects into the following:

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

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

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

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

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

Step 3 You can manually map or auto-create the security zones and interface groups.

Step 4 To map the security zones and interface groups manually, perform the following:

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

For ASA with FPS Migration:

- Security Zone type ASA to Security Zone type Routed/Switched (threat defense supported) is supported for migration.
- Because, management center only accepts unique security zone names, new threat defense supported Security Zone cannot have the same name as that of the source ASA with FPS zones.
- For all ASA type zones from the selected ASA with FPS that exists in source management center, a new threat defense (Routed/Switched) zone is created in Secure Firewall migration tool under the **Zone Mapping** page. Unlike in ASA to management center migration, in ASA with FPS scenarios, security zones are fetched from FPS policy and are not created based on the threat defense Logical name (ASA nameif).
- The Interface Groups will be migrated using the threat defense logical name, and hence there will be no impact on NAT.

The **FPS Zones** column, displays the security zones that is mapped to the ASA logical interface.

Note This column displays only the selected ASA with FPS device zones and list them against their respective interfaces.

If one ASA with FPS zone is attached to more than one interface of the same ASA with FPS device, split the zone into two threat defense supported zones.

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

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

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

Step 5 When you have mapped all interfaces to the appropriate security zones and interface groups, click **Next**.

Optimize, Review and Validate the Configuration

Step 1 (Optional) On the screen, click **Optimize ACL** to run the optimization code, and perform the following:

a) To download the identified ACL optimization rules, click **Download**.
b) Select rules and choose **Actions** > **Migrate as disabled** or **Do not migrate** and apply one of the actions.
c) Click **Save**.
The migration operation changes from **Do not migrate** to **disabled** or vice-versa.

You can perform bulk selection of rules, using the following options

- Migrate—To migrate with default state.
- Do not Migrate—To ignore the migration of ACLs.
- Migrate as disabled—To migrate ACLs with ***State*** field set to ***Disable***.
- Migrate as enabled—To migrate ACLs will with ***State*** field set to ***Enable***.

Step 2 On the Optimize, **Review and Validate Configuration** screen, click **Access Control Rules** and do the following:

a) For each entry in the table, review the mappings and verify that they are correct.

A migrated Access Policy Rule uses the ACL name as prefix and appends the ACL rule number to it to make it easier to map back to the ASA with FPS configuration file. For example, if an ASA with FPS ACL is named "inside_access," then the first rule (or ACE) line in the ACL will be named as "inside_access_#1." If a rule must be expanded because of TCP or UDP combinations, an extended service object, or some other reason, the Secure Firewall migration tool adds a numbered suffix to the name. For example, if the allow rule is expanded into two rules for migration, they are named "inside_access _#1-1" and " inside_access_#1-2".

For any rule that includes an unsupported object, the Secure Firewall migration tool appends an "_UNSUPPORTED" suffix to the name.

b) If you do not want to migrate one or more access control list policies, check the box for the appropriate rows, choose **Actions** > **Do not migrate**, and then click **Save**.

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

c) If you want to apply a management center file policy to one or more access control policies, check the box for the appropriate rows, choose **Actions** > **File Policy**.

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

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

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

e) If you want to change the logging options for an access control rule which has logging enabled, check the box for the appropriate row and choose **Actions** > **Log**.

In the **Log** dialog, you can enable logging events either at the beginning or end of a connection or both. If you enable logging, you must opt to send the connection events either to the **Event Viewer** or to the **Syslog** or both. When you opt to send connection events to a syslog server, you can choose the syslog policies that are already configured on the management center from the **Syslog** drop-down menu.

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

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

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

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

ACL Rule Category—The Secure Firewall migration tool preserves the Rule sections in the CSM managed ASA configuration and migrates them as ACL categories on management center.

Policy capacity and limit warning—The Secure Firewall migration tool compares the total ACE count for the migrated rules with the supported ACE limit on the target platform.

Based on the comparison result, the Secure Firewall migration tool displays a visible indicator and a warning message if the total count of migrated ACE exceeds threshold or if it approaches the threshold of the supported limit of target device.

You can optimize or decide not to migrate if the rules exceed the ACE Count column. You can also complete the migration and use this information to optimize the rules after a push on the management center before deployment.

Note The Secure Firewall migration tool does not block any migration despite the warning.

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

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

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

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

- **NAT Rules**
- **Objects (Access List Objects, Network Objects, Port Objects, VPN Objects, and Dynamic-Route Objects)**
- **Interfaces**
- **Routes**
- **Site-to-Site VPN Tunnels**
- **Remote Access VPN**

Access List objects displays Standard and Extended ACL used in BGP, EIGRP, and RA VPN.

If you do not want to migrate one or more NAT rules or Route Interfaces, check the box for the appropriate rows, choose **Actions** > **Do not migrate**, and then click **Save**.

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

Step 4 (Optional) While reviewing your configuration, you can rename one or more network, port, or VPN objects in the **Network Objects** tab or the **Port Objects** tab, or the **VPN Objects** by choosing **Actions** > **Rename**.

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

Step 5 In the **Dynamic-Route Objects** section, all the supported objects that are migrated are displayed:

- Policy-List
- Prefix-List
- Route-Map
- Community List
- AS-Path
- Access-List

Step 6 In the **Routes** section, the following routes are displayed:

- Static—Displays all IPv4 and IPv6 static routes.
- BGP—Displays all the BGP routes.
- EIGRP—Displays all the EIGRP routes.

  For EIGRP, authentication keys are obtained if the `more system:running` configuration is uploaded and the keys are unencrypted. If the key is encrypted in the source configuration, you can manually provide the key under the interface section in EIGRP. You can select the authentication type (encrypted, unencrypted, auth, or none) and provide the key accordingly.
- ECMP—Displays all the ECMP zones.

  Note The only action which can be performed in this section is renaming the ECMP zones.
- PBR—Displays all the PBR routes.

Step 7 In the **Remote Access VPN** section, all objects corresponding to Remote Access VPN are migrated from ASA to management center and are displayed:

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

  As part of pre-migration activity, upload all AnyConnect packages to the management center. You can upload AnyConnect profiles directly to the management center or from the Secure Firewall migration tool.

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

  Dap.xml must be the correct file retrieved from ASA. Validations are performed on dap.xml that are available in the configuration file. You must upload and select all the required files for validation. Failure to update will be marked as incomplete and the Secure Firewall migration tool does not proceed with validation.
- **AAA**—Authentication servers of Radius, LDAP, AD, LDAP, SAML, and Local Realm type are displayed. Update the keys for all AAA servers. From Secure Firewall migration tool 3.0, the pre-shared keys are retrieved automatically for a Live Connect ASA. You can also upload the source configuration with the hidden keys using **more system: running-config** file. To retrieve the AAA authentication key in clear text format, follow the below steps:

  Note These steps should be performed outside the Secure Firewall migration tool.

  a. Connect to the ASA through the SSH console.

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

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

```
ciscoASA#more system:running-config

!

aaa-server Test-RADIUS (inside) host 2.2.2.2

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

aaa-server Test-LDAP (inside) host 3.3.3.3

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

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

Note If the password for the local user is encrypted, you can internally check for the password or configure a new one on the Secure Firewall migration tool.

- LDAPS requires domain on management center. You must update domain for encryption type LDAPS.
- Unique AD Primary Domain is required on management center for an AD server. If a unique domain is identified, it will be displayed on the Secure Firewall migration tool. If conflict is found, you must enter a unique AD primary domain to push the objects successfully.

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

  For AAA server with type AD (server-type is Microsoft in ASA config), **AD Primary Domain** is a mandatory field to be configured on a management center. This field is not configured separately on ASA and extracted from the LDAP-base-dn config on ASA.

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

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

  LDAP-base-dn example file:

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

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

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

  AD Primary Domain is fwsecurity.cisco.com.

  AD Primary Domain is retrieved automatically and displayed on the Secure Firewall migration tool.

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

- **Address Pool**—All IPv4 and IPv6 pools are displayed here.
- **Group-Policy**—This section shows group policies with client profiles, management profiles, client modules, and group policies without profiles. If the profile was added in the AnyConnect file section, it is displayed as pre-selected. You can select or remove the user profile, management profile, and client module profile.
- **Connection Profile**—All connection profiles/tunnel groups are displayed here.
- **Trustpoint**—Trustpoint or PKI object migration from ASA to management center is part of the pre-migration activity and is required for successful migration of RA VPN. Map the trustpoint for Global SSL, IKEv2, and interface in the **Remote Access Interface** section to proceed with the next steps of migration. Global SSL and IKEv2 Trustpoint are mandatory if the LDAPS protocol is enabled. If a SAML object exists, trustpoint for SAML IDP and SP can be mapped in the SAML section. SP Certificate is optional. Trustpoint can also be overridden for a specific tunnel-group. If the overriden SAML trustpoint configuration is available in source ASA, it can be selected in **Override SAML** option.

  For information on exporting PKI certificates from ASA, see Export PKI Certificate from ASA with FirePOWER Services and Import into Management Center.
- **Certificate Maps**—Certificate maps are displayed here.

Step 8 (Optional) To download the details for each configuration item in the grid, click **Download**.

Step 9 After you have completed your review, click **Validate**.

During validation, the Secure Firewall migration tool connects to management center, reviews the existing objects, and compares those objects to the list of objects to be migrated. If an object already exists in management center, the Secure Firewall migration tool does the following:

- If the object has the same name and configuration, the Secure Firewall migration tool reuses the existing object and does not create a new object in management center.
- If the object has the same name but a different configuration, the Secure Firewall migration tool reports an object conflict.

You can view the validation progress in the console.

Step 10 When the validation is complete, if the **Validation Status** dialog box shows one or more object conflicts, do the following:

a) Click **Resolve Conflicts**.

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

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

For example, you might be prompted to add a suffix to the object name to avoid a conflict with the existing management center object. You can accept the default suffix or replace it with one of your own.

e) Click **Resolve**.
f) When you have resolved all object conflicts on a tab, click **Save**.
g) Click **Validate** to revalidate the configuration and confirm that you have resolved all object conflicts.

Step 11 When the validation is complete and the **Validation Status** dialog box displays the message **Successfully Validated**, continue with Push the Migrated Configuration to Management Center, on page 26.

Push the Migrated Configuration to Management Center

You cannot push the migrated ASA with FPS configuration to management center if you have not successfully validated the configuration and resolved all object conflicts.

This step in the migration process sends the migrated configuration to management center. It does not deploy the configuration to the threat defense device. However, any existing configuration on the threat defense is erased during this step.

Note Do not make any configuration changes or deploy to any device while the Secure Firewall migration tool is sending the migrated configuration to management center.

Step 1 In the **Validation Status** dialog box, review the validation summary.

Step 2 Click **Push Configuration** to send the migrated ASA with FPS configuration to management center.

The new optimization functionality in the Secure Firewall migration tool allows you to fetch the migration results quickly using the Search filters.

The Secure Firewall migration tool also provides support to optimize CSV download and to apply the actions per page view or on all rules.

The Secure Firewall migration tool displays a summary of the progress of the migration. You can view detailed, line-by-line progress of which the components that are being pushed to management center in the console.

Step 3 After the migration is complete, click **Download Report** to download and save the post-migration report.

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

Step 4 If your migration failed, review the post-migration report, log file, and unparsed file carefully to understand what caused the failure.

You can also contact the support team for troubleshooting.

Migration Failure Support

If the migration is unsuccessful, contact Support.

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

The Help support page appears.

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

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

c. Click **Download**.

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

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

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

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

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

Review the Post-Migration Report and Complete the Migration

The Post-migration report provides details on ACL count under various categories, ACL optimization, and the overall view of optimization performed on the configuration file. For more information, see Optimize, Review and Validate the Configuration, on page 20

Review and verify the objects:

- **Category**
  - Total ACL rules (Source Configuration)
  - Total ACL rules considered for Optimization. For example, Redundant, Shadow, and so on.
- ACL Count for optimization gives the total number of ACL rules counted before and after Optimization.

If you have missed to download the Post-Migration Reports during migration, use the following link to download:

Post-Migration Report Download Endpoint—http://localhost:8888/api/downloads/post_migration_summary_html_format

Note You can download the reports only when the Secure Firewall migration tool is running.

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

Step 2 Open the post-migration report and carefully review its contents to understand how your ASA with FPS configuration was migrated:

- **Migration Summary**—A summary of the configuration that was successfully migrated from ASA with FPS to threat defense, including information about the interface, management center hostname and domain, target threat defense device (if applicable), and the successfully migrated configuration elements.
- **Selective Policy Migration**—Details of the specific ASA with FPS feature selected for migration are available within three categories - Device Configuration Features, Shared Configuration Features, and Optimization.
- **ASA with FPS Interface to Threat Defense Interface Mapping**—Details of the successfully migrated interfaces and how you mapped the interfaces on the ASA with FPS configuration to the interfaces on the threat defense device. Confirm that these mappings match your expectations.

  Note This section is not applicable for migrations without a destination threat defense device or if **Interfaces** are **not** selected for migration.

- **Source Interface Names to Threat Defense Security Zones and Interface Groups**—Details of the successfully migrated ASA with FPS logical interfaces and name and how you mapped them to security zones and interface groups in threat defense. Confirm that these mappings match your expectations.

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

- **Object Conflict Handling**—Details of the ASA with FPS objects that were identified as having conflicts with existing objects in management center. If the objects have the same name and configuration, the Secure Firewall migration tool reused the management center object. If the objects have the same name but a different configuration, you renamed those objects. Review these objects carefully and verify that the conflicts were appropriately resolved.
- **Access Control Rules, NAT, and Routes You Chose Not to Migrate**—Details of the rules that you choose not to migrate with the Secure Firewall migration tool. Review these rules that were disabled by the Secure Firewall migration tool and were not migrated. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.
- **Partially Migrated Configuration**—Details of the ASA with FPS rules that were only partially migrated, including rules with advanced options where the rule could be migrated without the advanced options. Review these lines, verify whether the advanced options are supported in management center, and if so, configure these options manually.
- **Unsupported Configuration**—Details of ASA with FPS configuration elements that were not migrated because the Secure Firewall migration tool does not support migration of those features. Review these lines, verify whether each feature is supported in threat defense. If so, configure those features manually in management center.
- **Expanded Access Control Policy Rules**—Details of ASA with FPS access control policy rules that were expanded from a single Point rule into multiple threat defense rules during migration.
- **Actions Taken on Access Control Rules**
  - **Access Rules You Chose Not to Migrate**—Details of the ASA with FPS access control rules that you choose not to migrate with the Secure Firewall migration tool. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.
  - **Access Rules with Rule Action Change**—Details of all Access Control Policy Rules that had ‘Rule Action’ changed using the Secure Firewall migration tool. The Rule Action values are - Allow, Trust, Monitor, Block, Block with reset. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.
  - **Access Control Rules that have IPS Policy and Variable Set Applied**—Details of all ASA with FPS access control policy rules that have IPS Policy applied. Review these rules carefully and determine whether the feature is supported in threat defense.
  - **Access Control Rules that have File Policy Applied**—Details of all ASA with FPS access control policy rules that have File Policy applied. Review these rules carefully and determine whether the feature is supported in threat defense.
  - **Access Control Rules that have Rule ‘Log’ Setting Change**—Details of the ASA with FPS access control rules that had ‘Log setting' changed using the Secure Firewall migration tool. The Log Setting values are - False, Event Viewer, Syslog. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.
  - **Access Control Rules that have failed Zone-lookup**—Details of the ASA with FPS access control rules that fail the Route-lookup operation and that is populated in the **Post-Migration Report**. The Secure Firewall migration tool performs the route-lookup operation based on the route (static and connected) information in the source configuration to populate the destination security zones in the access rules.

- **Access Control Rules for Tunneled Protocols**—Details of Tunnel rules that are migrated as a prefilter tunnel rule during migration.

Note An unsupported rule that was not migrated causes issues with unwanted traffic getting through your firewall. We recommend that you configure a rule in management center to ensure that this traffic is blocked by threat defense.

Note If it requires you to apply IPS or file policy to ACL in the **Review and Validate** page, you are highly recommended to create a policy on the management center before migration. Use the same policy, as the Secure Firewall migration tool fetches the policy from the connected management center. Creating a new policy and assigning it to multiple policies may degrade the performance and may also result in a push failure.

For more information about supported features in management center and threat defense, see Management Center Configuration Guide, Version 6.2.3.

Step 3 Open the **Pre-Migration Report** and make a note of any ASA with FPS configuration items that you must migrate manually on the threat defense device.

Step 4 In management center, do the following:

a) Review the migrated configuration for the threat defense device to confirm that all expected rules and other configuration items, including the following, were migrated:

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

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

For information on how to configure these items and rules, see the Management Center Configuration Guide. The following are examples of configuration items that require manual configuration:

- Platform settings, including SSH and HTTPS access, as described in Platform Settings for Threat Defense
- Syslog settings, as described in Configure Syslog
- Dynamic routing, as described in Routing Overview for Threat Defense
- Service policies, as described in FlexConfig Policies
- VPN configuration, as described in Threat Defense VPN

- Connection log settings, as described in Connection Logging

Step 5 After you have completed your review, deploy the migrated configuration from management center to the threat defense device.

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

The Secure Firewall migration tool assigns the policies to the threat defense device. Verify that the changes are reflected in the running configuration. To help you to identify the policies that are migrated, the description of those policies includes the hostname of the ASA with FPS configuration.

Uninstall the Secure Firewall Migration Tool

All components are stored in the same folder as the Secure Firewall migration tool.

Step 1 Navigate to the folder where you placed the Secure Firewall migration tool.

Step 2 If you want to save the logs, cut or copy and paste the `log` folder to a different location.

Step 3 If you want to save the pre-migration reports and the post-migration reports, cut or copy and paste the `resources` folder to a different location.

Step 4 Delete the folder where you placed the Secure Firewall migration tool.

Tip The log file is associated with the console window. If the console window for the Secure Firewall migration tool is open, the log file and the folder cannot be deleted.

Sample Migration: ASA with FPS to Threat Defense 2100

Note Create a test plan that you can run on the target device after you complete the migration.

- Pre-Maintenance Window Tasks
- Maintenance Window Tasks

Pre-Maintenance Window Tasks

Before you begin

Make sure you have installed and deployed a management center. For more information, see the appropriate Management Center Hardware Installation Guide and the appropriate Management Center Getting Started Guide.

Step 1 Use the **show running-config** command for the ASA with FPS device or context that you are migrating and save a copy of the ASA with FPS configuration. See View the Running Configuration.

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

Note For a multi context ASA with FPS, you can use the **show tech-support** command to obtain the configuration for all the contexts in a single file.

Step 2 Review the ASA with FPS configuration file.

Step 3 Deploy the Firepower 2100 series device in your network, connect the interfaces and power on the appliance.

For more information, see Cisco Threat Defense for the 2100 Series Using Management Center Quick Start Guide.

Step 4 Register the Firepower 2100 series device to be managed by the management center.

For more information, see Add Devices to the Management Center.

Step 5 (Optional) If your source ASA with FPS configuration has port channels, create port channels (EtherChannels) on the target Firepower 2100 series device.

For more information, see Configure EtherChannels and Redundant Interfaces.

Step 6 Download and run the most recent version of the Secure Firewall migration tool from https://software.cisco.com/download/home/286306503/type.

For more information, see Download the Secure Firewall Migration Tool from Cisco.com, on page 3.

Step 7 When you launch the Secure Firewall migration tool, and specify destination parameters, make sure that you select the Firepower 2100 series device that you registered to the management center.

For more information, see Specify Destination Parameters for the Secure Firewall Migration Tool, on page 11.

Step 8 Map the ASA with FPS interfaces with the threat defense interfaces.

Note The Secure Firewall migration tool allows you to map an ASA with FPS interface type to the threat defense interface type.

For example, you can map a port channel in ASA with FPS to a physical interface in threat defense.

For more information, see Map ASA with FPS Configurations with Secure Firewall Device Manager Threat Defense Interfaces.

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

For more information, see Map ASA with FPS Interfaces to Security Zones and Interface Groups.

Step 10 Follow the instructions of this guide to sequentially review and validate the configuration to be migrated, and then push the configuration to the management center.

Step 11 Review the Post Migration report, manually setup and deploy other configurations to the threat defense and complete the migration.

For more information, see Review the Post-Migration Report and Complete the Migration, on page 27.

Step 12 Test the Firepower 2100 series device using the test plan that you would have created while planning for migration.

Maintenance Window Tasks

Before you begin

Make sure you have completed all the tasks that must be performed before the maintenance window. See Pre-Maintenance Window Tasks, on page 30.

Step 1 Connect to the ASA with FPS through the SSH console and switch to the interface configuration mode.

Step 2 Shutdown the ASA with FPS interfaces using the **shutdown** command.

Step 3 (Optional) Access the management center and configure dynamic routing for the Firepower 2100 series device.

For more information, see Dynamic Routing.

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

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

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

Step 7 If you are assigning a new IP address to the Firepower 2100 series device and not reusing the IP address assigned to the ASA with FPS perform the following steps:

a. Update any static routes which refer to the IP address, so that they now point to the Firepower 2100 series device IP address.

b. If you are using routing protocols, ensure that neighbors see the Firepower 2100 series device IP address as the next hop for expected destinations.

Step 8 Run a comprehensive test plan and monitor logs within the managing management center for your Firepower 2100 device.