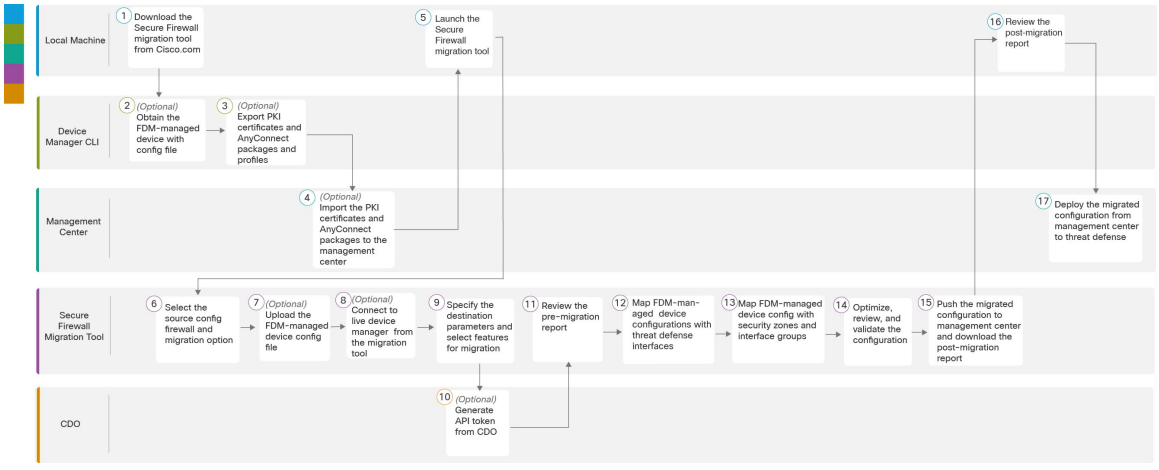


FDM-Managed Device to Threat Defense Workflow

- End-to-End Procedure, on page 1
- Prerequisites for Migration, on page 3
- Run the Migration, on page 11
- Uninstall the Secure Firewall Migration Tool, on page 38
- Sample Migration: FDM-managed device to Threat Defense 2100 , on page 39

End-to-End Procedure

The following flowchart illustrates the workflow for migrating an FDM-managed device 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	Device Manager CLI	(Optional) Obtain the FDM-managed device configuration file: To obtain the FDM-managed device config file from device manager CLI, see Obtain the FDM-Managed Device configuration file. If you intend to connect the FDM-managed device from Secure Firewall migration tool, skip to step 3.
3	Device Manager CLI	(Optional) Export PKI certificates and AnyConnect packages and profiles: This step is required only if you are planning to migrate site-to site VPN and RA VPN features from FDM-managed device to threat defense. To export the PKI certificates from device manager CLI, see Export PKI Certificate from and Import into Firewall Management Center, step 1. To export AnyConnect packages and profiles from device manager CLI, see Retrieve AnyConnect Packages and Profiles, step 1. If you are not planning to migrate site-to-site VPN and RA VPN, skip to step 7.
4	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 and Import into Firewall Management Center, step 2 and Retrieve AnyConnect Packages and Profiles, step 2.
5	Local Machine	Launch the Secure Firewall migration tool on your local machine, see Launch the Secure Firewall Migration Tool.
6	Secure Firewall Migration Tool	To select the source configuration firewall and migration option, See Select the Source Configuration Firewall and Migration Option
7	Secure Firewall Migration Tool	(Optional) Upload the FDM-managed device config file obtained from device manager CLI, see Upload the FDM-Managed Device Configuration File. If you are planning to connect to live FDM-managed device, skip to step 8.
8	Secure Firewall Migration Tool	You can connect to live device manager directly from the Secure Firewall migration tool. For more information, see Connect to the FDM-Managed Device 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	Security Cloud Control	(Optional) This step is optional and only required if you have selected cloud-delivered Firewall Management Center as destination management center. For detailed steps, see Specify Destination Parameters for the Secure Firewall Migration Tool, Step 1.
11	Secure Firewall Migration Tool	Navigate to where you downloaded the pre migration report and review the report. For detailed steps, see Review the Pre-Migration Report.
12	Secure Firewall Migration Tool	The Secure Firewall migration tool allows you to map the FDM-managed device configuration with threat defense interfaces. For detailed steps, see Map FDM-Managed Device Configurations with Secure Firewall Threat Defense Interfaces.

	Workspace	Steps
13	Secure Firewall Migration Tool	To ensure that the FDM-managed device configuration is migrated correctly, map the FDM-managed device interfaces to the appropriate threat defense interface objects, security zones and interface groups. For detailed steps, see Map FDM-Managed Device Interfaces to Security Zones and Interface Groups.
14	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 to be Migrated.
15	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.
16	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.
17	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 FDM-managed device 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.

If you want to use the cloud version of the Secure Firewall migration tool hosted on Security Cloud Control, skip to step 4.

Procedure

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 Firewall Threat Defense device download areas.

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

Ensure that you download the appropriate executable of the Secure Firewall migration tool for Windows or macOS machines.

Step 4 If you are a Security Cloud Control user and want to use the migration tool hosted on it, log in to your Security Cloud Control tenant and on the left pane, navigate to **Administration** > **Migration** > **Firewall Migration Tool** to create your migration instance.

Obtain the FDM-Managed Device Configuration File

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

- Export the FDM-Managed Device Configuration File, on page 4
- Connect to the FDM-Managed Device from the Secure Firewall Migration Tool, on page 15

Export the FDM-Managed Device Configuration File

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

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

The export zip file might include the following:

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

Procedure

Step 1 Create the JSON object body for the export.

Example:

Following is an example of the JSON object.

```
"diskFileName": "string",
"encryptionKey": "*********",
"doNotEncrypt": false,
```

```
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": true,
  "entityIds": [
    "string"
  ],
  "jobName": "string",
  "type": "scheduleconfigexport"
}
```

The attributes are,

- **diskFileName**—(Optional) The name of the export zip file. If you do not specify a name, the system generates a name by default. Even if you specify a name, the system might append characters to the name to ensure uniqueness. The name has a maximum length of 60 characters.
- **encryptionKey**—An encryption key for the zip file. If you do not want to encrypt the file, skip this field, and specify **doNotEncrypt: true** instead. If you specify a key, use the key to open the zip file after you download it to your local machine. The exported configuration file exposes the secret keys, passwords, and other sensitive data in clear text (otherwise they cannot be imported). In this case you might want to apply an encryption key to protect sensitive data. The system uses AES 256 encryption.
- **doNotEncrypt**—(Optional) Whether the export file should be encrypted (false), or not encrypted (true). The default is false, which means you must specify a non-empty encryption key attribute. If you specify true, then the encryption key attribute is ignored.
- **configExportType**—You can select any of the following export types for exporting the configuration files:
  - FULL_EXPORT—Includes the entire configuration in the export file. **This is the default option and should be selected for migration.**
- **deployedObjectsOnly**—(Optional) Whether to include objects in the export file only if they have been deployed. The default is false, which means all pending changes are included in the export. Specify true to exclude pending changes.
- **entityIds**—A comma-separated list of the identities with a set of starting-point objects enclosed in [brackets]. The list is required for a PARTIAL_EXPORT job. Each item the list could be either a UUID value or an attribute-value pair matching patterns like "id=uuid-value", "type=object-type" or "name=object-name". For example, "type=networkobject"
  - The type can be a leaf entity, such as network object, or an alias of a set of leaf types. Some typical type aliases are: network (NetworkObject and NetworkObjectGroup), port (all TCP/UDP/ICMP port, protocol and group types), url (URL objects and groups), ikepolicy (IKE V1/V2 policies), ikeproposal (Ike V1/V2 proposals), identitysource (all identity sources), certificate (all certificate types), object (all object/group types that would be listed in the device manager on the Objects page), interface (all network interfaces, s2svpn (all site-to-site VPN related types), ravpn (all RA VPN related types), vpn (both s2svpn and ravpn).
  - All the objects and their outgoing referential descendants will be included in the PARTIAL_EXPORT output file. All the unexportable objects will be excluded from the output even if you specify their identities. Use the GET method for the appropriate resource types to obtain the UUIDs, types, or names for the target objects.

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

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

```
    "acc2e3cd-8c70-11e9-930a-1f12ee87b286"
    ]",
```

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

Step 2 Post the object.

Example:

The curl command would look like the following:

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

Step 3 Verify the response.

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

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

Step 4 Check the status of configuration export.

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

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

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

A successfully completed job diplays the following status:

```
{
  "version": "hdy62yf5xp3vf",
  "jobName": "Config Export",
  "jobDescription": null,
  "user": "admin",
```

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


Step 5 Download the export file.

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

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

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

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


```
{
  "items": [
    {
      "diskFileName": "export-config-2.zip",
      "dateModified": "2019-04-19 13:32:28Z",
      "sizeBytes": 10182,
      "id": "default",
      "type": "configimportexportfileinfo",
      "links": {
        "self": "https://10.89.5.38/api/fdm/latest/action/configfiles/default"
      }
    },
    {
      "diskFileName": "export-config-1.zip",
      "dateModified": "2019-04-19 13:14:56Z",
      "sizeBytes": 10083,
      "id": "default",
      "type": "configimportexportfileinfo",
      "links": {
        "self": "https://10.89.5.38/api/fdm/latest/action/configfiles/default"
      }
    }
  ],
```


Download the file using the diskFileName as the object ID.

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

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

Note

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

Export PKI Certificate from Device Manager and Import into Firewall Management Center

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

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

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

Procedure

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

Example:


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

```
    }
}
```

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

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 **VPN Tunnels** section.

Retrieve AnyConnect Packages and Profiles

Before you begin

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

- Remote Access VPN on the management center requires at least one AnyConnect package.
- If the configuration consists of a 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.xmland Data.xml must be added through the Secure Firewall migration tool.

Check the packages available on the device manager to download.

Procedure

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

You can use the **GET /object/anyconnectpackagefiles** API to view the packages on the device.

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

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

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

```
}
```

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

Step 2 Download the AnyConnect package.

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

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

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

Note
The AnyConnect profiles are automatically retrieved from the device manager by the Secure Firewall migration tool. This step is only required if you want to manually upload the AnyConnect profile.

You can use the **GET /object/anyconnectclientprofiles** to check the available profiles on the device manager.

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

The following response will be displayed:

```
  "items": [

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

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

Step 4 Download the AnyConnect profile.

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

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

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

a. Dap.xmland 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 Security Cloud Control, skip to Upload the FDM Configuration Bundle .

Note When you launch the desktop version of 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.

Procedure

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.

  Note
  Ensure you disable any popup blockers in your browser because they might hinder login popus from appearing.

  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 premigration 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, 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 FDM-managed device configuration to your computer, proceed to Upload the FDM-managed device Configuration File.

Using the Demo Mode in the Secure 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**.

The demo mode provides an opportunity to perform 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, demo FTD devices, or Multicloud Defense.

Caution Choosing **Demo Mode** erases existing migration workflows, if any. 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. You cannot push the configurations to the demo target devices you selected because this is only a demo mode. 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.

Select the Source Configuration and Device Manager Migration Option

Procedure

Step 1 Select the **Source Firewall Vendor** from the drop-down list and click **Start Migration**.

Step 2 Select the migration option by which you wish to migrate the FDM-managed device.

Following are the available options:

- **Migrate Firepower Device Manager (Shared Configurations only)**

  This option allows the migration of shared configuration from the device manager to the destination management center. This option should be used for staged migrations so that the shared configurations are migrated initially, and the device configuration can be migrated at a later point of time. There is no downtime involved in this use case.

- **Migrate Firepower Device Manager (Includes Device and Shared configurations)**

  This option allows shared and device configuration to be migrated to the destination management center. As part of this migration, the source threat defense is moved from device manager to management center. After successful completion of migration, the management center continues to manage the threat defense device. Hence, the source and destination are the same threat defense device in this use case. There is a downtime involved in this use case as the threat defense device is moved to the management center.

  For migrating your configuration using this option, perform the following as a part of pre-migration activity:

  a. Log in to the device manager and navigate to **Objects** section.

  b. Click on **Identity Sources** and select **AD Realm** from **Preset filters**.

  c. Under **Actions**, click on **Edit** ( ) for the specific realm that has the encryption type as **LDAPS** or **STARTTLS**.

  d. In the **Directory Server Configuration**, click the **drop-down** arrow next to the name of the server.

  e. Under **Encryption Section**, change the encryption type to **NONE** and click **OK**.

  f. Deploy the changes.

  Note
  Once the configuration is migrated to the management center, you can revert the encryption type of AD realm in the management center to LDAPS or STARTTLS. For detailed steps, see Review the Post-Migration Report and Complete the Migration, Step 4 (b).

- **Migrate Firepower Device Manager (Includes Device and Shared Configurations) to FTD Device (New Hardware)**

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

Upload the FDM Configuration bundle

Before you begin

Export the configuration bundle as `.zip`from the source device manager.

Note Manual upload will be supported for the below two options:

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

Procedure

Step 1 On the **Extract FDM Information** screen, in the **Manual Upload** section, click **Upload**, to upload an FDM-managed configuration bundle. If the configuration bundle is encrypted, provide with the key on the text box for the Secure Firewall migration tool to decrypt the bundle.

Step 2 Browse to where the FDM-managed device configuration file is located and click **Open**.

The Secure Firewall migration tool uploads the configuration bundle. For large configuration files, this step takes a longer time. The console provides a line-by-line log view of the progress, including the FDM-managed device configuration 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

Step 3 Click **Start Parsing**.

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

Step 4 Review the summary of the elements in the uploaded configuration file that the Secure Firewall migration tool detected and parsed.

Step 5 Click **Next** to select the target parameters.

What to do next

SpecifyDestination Parameters for the Secure Firewall migration tool

Connect to the FDM-Managed Device from the Secure Firewall Migration Tool

Before you begin

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

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

Procedure

Step 1 On the **ExtractFDM Information** screen, in the **Connect to FDM** section, click **Connect** to connect to the FDM-managed device that you want to migrate

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

a. In the **FDM IP Address/Hostname** field, enter the management IP address or hostname of the FDM. Click **Login**.

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

c. Click **Login**.

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

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

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

Step 3 Review the summary of the elements that the Secure Firewall migration tool detected and parsed, from the FDM-managed device.

Step 4 Click **Next**, to select the target parameters.

What to do next

SpecifyDestination Parameters for the Secure Firewall migration tool

Specify Destination Parameters for the Secure Firewall Migration Tool

Before you begin

If you are using the cloud version of the migration tool hosted on Security Cloud Control, skip to Step 3.

- Obtain the IP address for the Firewall Management Center for On-Prem Firewall Management Center.
- (Optional) Add the target threat defense device to the management center if the selected flow is **Migrate Firepower Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware)** to the Firewall 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 Firewall Management Center before migration. Use the same policy, as the Secure Firewall migration tool fetches the policy from the connected Firewall Management Center. Creating a new policy and assigning it to multiple access control lists may degrade the performance and may also result in a push failure.

Procedure

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

- For migrating to an On-Prem Firewall Management Center, 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 have selected **Migrate Firepower Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware)**, you can only migrate to the threat defense devices available in the selected domain.

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

- For migrating to a Cloud-delivered Firewall Management Center, do the following:

a) Click the **Cloud-delivered FMC** radio button.
b) Choose the region and paste the Security Cloud Control API token. For generating the API token. from Security Cloud Control, follow the below steps:

   1. Log in to Security Cloud Control.
   2. From the top-right corner, navigate to **Preferences** > **General Preferences** and copy the API Token from **My Tokens** section.

c) 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 Firewall Management Center and retrieves a list of Firewall Threat Defense devices that are managed by that Firewall Management Center. You can view the progress of this step in the console.

Step 3 Click **Proceed**.

If you have selected **Migrate Firepower Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware)**, you can only migrate to the threat defense devices available in the selected domain.

If you have selected **Migrate Firepower Device Manager (Shared Configurations Only)**

The threat defense section of the management center is not populated in this work flow, only shared policies (Access Control Lists, NAT, and Objects) are pushed to Firewall Management Center. You can choose to include or skip the shared policies that needs to be pushed to the management center.

If you have selected **Migrate Firepower Device Manager (Includes Device & Shared Configurations)**

The threat defense that is moved to the management center is the same device that is being managed by device manager. The threat defense part of the management center is not populated in this case.

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

- Click the **Select FTD Device** drop-down list and check the device where you want to migrate the FDM-managed device configuration.

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

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.

- Click **Proceed without FTD** to migrate the configuration to the Firewall Management Center.

  When you proceed without Firewall Threat Defense, the Secure Firewall migration tool will not push any configurations or the policies to Firewall Threat Defense. Thus, interfaces and routes, and site-to-site VPN which are Firewall Threat Defense device-specific configurations will not be migrated and need to be manually configured on Firewall 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 Firewall Threat Defense device, the Secure Firewall migration tool automatically selects the features available for migration from the FDM-managed device 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 Firewall Management Center, the Secure Firewall migration tool automatically selects the features available for migration from the FDM-managed device configuration in the **Device Configuration**, **Shared Configuration**, and **Optimization** sections. You can further modify the default selection, according to your requirements.

  Note
  The **Device Configuration** section is not available if 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, whereas 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.

  - • 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 Firewall 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 FDM-managed device 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 Firewall Management Center and Firewall Threat Defense is version 6.6 or later.
  - Route-based (VTI)—If the target Firewall Management Center and Firewall 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 FDM-managed device 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 Firewall Threat Defense.
- If you have platform settings, file, and malware policies on your source FDM-managed device, the migration tool displays them on the **Select Features** page as **Platform Settings** under Shared Configuration and **File and Malware Policy** under Device Configuration. Note that these checkboxes are selected by default.

Step 7 Click **Proceed**.

Step 8 In the **Rule Conversion/ Process Config** section, click **Start Conversion** to initiate the conversion.

Step 9 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 10 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.

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.

Procedure

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

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

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

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

- **Overall Summary**—The method used to extract the FDM-managed device configuration information or connecting to a live FDM-managed device configuration.

  A summary of the supported FDM-managed device configuration elements that can be successfully migrated to Firewall Threat Defense or Multicloud Defense and specific features selected for migration.

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

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

- **Ignored Configuration**—Details of FDM-managed device configuration elements that are ignored because they are not supported by the Firewall 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 Firewall Management Center, and if not supported, plan to configure the features manually.

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

Step 3 (Optional) If the **Pre-Migration Report** recommends corrective actions, complete the corrections in the interface, export the FDM-managed device configuration file again, and upload the updated configuration file before proceeding.

Step 4 After your FDM-managed device 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 FDM-managed device Interfaces with Firepower Threat Defense Interfaces

Map FDM-Managed Device Configurations with Firewall Threat Defense Interfaces

The Firewall Threat Defense device must have an equal or greater number of physical and port channel interfaces than those used by FDM-managed device 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 Firewall Threat Defense device. By default, the Secure Firewall migration tool maps the interfaces in FDM-managed device and the Firewall Threat Defense device according to their interface identities. For example, the 'management-only' interface on the FDM-managed device interface is automatically mapped to the 'management-only' interface on the Firewall Threat Defense device and is unchangeable.

The mapping of FDM-managed device interface to the Firewall Threat Defense interface differs based on the Firewall Threat Defense device type:

- If the target Firewall Threat Defense is of native type:
  - The Firewall Threat Defense must have equal or a greater number of used FDM-managed device interfaces or port channel (PC) data interfaces (excluding management-only and subinterfaces in the FDM-managed device configuration). If the number is less, add the required type of interface on the target Firewall Threat Defense.
  - Subinterfaces are created by the secure Firewall migration tool based on physical interface or port channel mapping.
- If the target Firewall Threat Defense is of container type:
  - The Firewall Threat Defense must have equal or a greater number of used FDM-managed device interfaces, physical subinterfaces, port channel, or port channel subinterfaces (excluding management-only in FDM-managed device configuration). If the number is less, add the required type of interface on the target Firewall Threat Defense. For example, if the number of physical interfaces and physical subinterface on the target Firewall Threat Defense is 100 less than that of FDM-managed device then you can create the additional physical or physical subinterfaces on the target Firewall 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 Firewall Management Center and chosen the destination as Firewall Threat Defense. For more information, see Specify Destination Parameters for the Secure Firewall Migration Tool, on page 16.

Note This step is not applicable if you are migrating using **Migrate Firepower Device Manager (Shared Configurations Only)**

This step is an information-only step for **Migrate Firepower Device Manager (Includes Device & Shared Configurations)**.

Procedure

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 interface.

You cannot change the mapping of the management interfaces. If a Firewall Threat Defense interface has already been assigned to an FDM-managed device 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 Firewall Threat Defense device for all subinterfaces in the FDM-managed device configuration.

Step 2 When you have mapped each FDM-managed device interface to a Firewall Threat Defense interface, click **Next**.

Map FDM-Managed Device Interfaces to Security Zones Interface Groups

Note If your FDM-managed device 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 to be migrated, on page 23

To ensure that the FDM-managed device configuration is migrated correctly, map the FDM-managed device interfaces to the appropriate Firewall Threat Defense interface objects, security zones. In an FDM-managed device configuration, access control policies and NAT policies use interface names (nameif). In Firewall Management Center, those policies use interface objects. In addition, Firewall Management Center policies group interface objects into the following:

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

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 Firewall Management Center allows it. For more information about security zones and interface groups in Firewall Management Center, see Security Zones and Interface Groups in *Cisco Secure Firewall Management Center Device Configuration Guide*.

Procedure

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 Firewall Management Center, or that is available in FDM-managed device 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**.

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 FDM-managed device 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 FDM-managed device interface. For example, if the FDM-managed device 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 to be migrated

For FDM-managed device configuration, the configuration is validated in different ways and will depend on the migration flow selected. The configuration validation for different options are as follows:

- **Migrate Firepower Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware)**—Both device and shared configuration are reviewed and validated in a single flow.
- **Migrate Firepower Device Manager (Shared Configurations Only)**— Only Shared configuration is reviewed and validated.
- **Migrate Firepower Device Manager (Includes Device & Shared Configurations)**—Shared and device Configuration is validated in Separate flow

Optimize, Review and Validate Shared Configuration

Before you push the migrated FDM configuration to management center, optimize and review the configuration carefully and validate that it is correct and matches how you want to configure the threat defense device. A flashing tab indicates that you must take the next course of action.



Note If you close the Secure Firewall migration tool at the **Optimize, Review and Validate Configuration** screen, it saves your progress and allows you to resume the migration later. If you close the Secure Firewall migration tool before this screen, your progress is not saved. If there is a failure after parsing, relaunching the Secure Firewall migration tool resumes from the **Interface Mapping** screen.

Here, the Secure Firewall migration tool fetches the Intrusion Prevention System (IPS) Policies and File Policies which are already present on the Firewall Management Center and allows you to associate those to the Access Control Rules you are migrating.

A file policy is a set of configurations that the system uses to perform Advanced Malware Protection for networks and file control, as part of your overall access control configuration. This association ensures that before the system passes a file in traffic that matches an access control rule's conditions, it first inspects the file.

Similarly, you can use an IPS policy as the system's last line of defense before traffic is allowed to proceed to its destination. Intrusion policies govern how the system inspects traffic for security violations and, in inline deployments, can block or alter malicious traffic. Whenever the system uses an intrusion policy to evaluate traffic, it uses an associated variable set. Most variables in a set represent values commonly used in intrusion rules to identify source and destination IP addresses and ports. You can also use variables in intrusion policies to represent IP addresses in rule suppression and dynamic rule states.

To search for specific configuration items on a tab, enter the item name in the field at the top of the column. The table rows are filtered to display only items that match the search term.

If you close the Secure Firewall migration tool at the **Optimize, Review and Validate Configuration** screen, it saves your progress and allows you to resume the migration later. If you close the before this screen, your progress is not saved. If there is a failure after parsing, relaunching the Secure Firewall migration tool resumes from the **Interface Mapping** screen.

Secure Firewall Migration Tool ACL Optimization Overview

The Secure Firewall migration tool provides support to identify and segregate ACLs that can be optimized (disabled or deleted) from the firewall rule base without impacting the network functionality.

The ACL optimization supports the following ACL types:

- Redundant ACL—When two ACLs have the same set of configurations and rules, then removing the non-base ACL will not impact the network. For example, if any two rule allows FTP and IP traffic on the same network with no rules that are defined for denying access, the first rule can be deleted.
- Shadow ACL—The first ACL completely shadows the configurations of the second ACL. If two rules have similar traffic, the second rule is not applied to any traffic as it appears later in the access list. If the two rules specify different actions for traffic, you can either move the shadowed rule or edit any one of the rules to implement the required policy. For example, the base rule may deny the IP traffic, and the shadowed rule may allow FTP traffic for a given source or destination.

- Disable ACL—The ACL that has been explicitly turned off in the firewall's configuration. The rules exist in the configuration file, but the Secure Firewall Migration Tool ignores them when processing traffic.

The Secure Firewall migration tool uses the following parameters while comparing rules for ACL optimization:



Note Optimization is available for the FDM-managed device only for ACP rule action.

- The source ACLs are expanded into the corresponding ACEs (inline values), and then compared for the following parameters:
  - Source and Destination Zones
  - Source and Destination Network
  - Source and Destination Port

Object Optimization

The following objects are considered for Object optimization during the migration process:

- Unreferenced objects—You can choose not to migrate unreferenced objects at the beginning of the migration.
- Duplicate objects—If an object already exists on Firewall Management Center, instead of creating a duplicate object, the policy is reused.

Procedure

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 FDM-managed device configuration file. For example, if an FDM-managed device 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) To edit an access control list policy, select the row by checking the check box for the policy, and choose **Actions** > **Edit**.

Edit Rule dialog box appears. You can update existing data or add new data in the chosen policy.

To add an object to source or destination:

1. Choose the object from the left pane by checking the check box for it.
2. Click the **Add Source** or **Add Destination** button under **Selected Sources** or **Selected Destination and Applications** column to move the object to the respective location.

You can also delete the existing object from the source or destination by clicking the delete icon.

All rules that are not applicable are grayed out in the table.

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

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

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

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

f) 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 Firewall Management Center from the **Syslog** drop-down menu.

g) 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. This list also includes malware and file policies associated with the ACLs, which you can choose to not migrate, apply, or modify.
- 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.

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 Firewall 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.

h) In the **Intrusion Policy**, all intrusion policies and the corresponding base policy, custom /overridden rules present, intrusion mode and reference in ACP is shown. It also shows Snort Engine and NAP Policy for Snort 3.

Snort 2 Policies with overridden rules are ignored due to API Limitation on the management center.

An intrusion policy with default setting is reused on management center.

A new policy is created with policy name _ <FDM Hostname> for an intrusion policy with overriden rules/custom rules for Snort 3 or intrusion mode detection for Snort3/Snort2

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**
- **SNMP**
  - **SNMPv1/v2**
  - **SNMPv3**
- **DHCP**
  - **DHCP Server**

- **DHCP Relay**
- **DDNS**

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 **Site-to-Site VPN Tunnels** section, the VPN tunnels from the source firewall configurations are listed. Review the VPN tunnel data such as **Source Interface**, **VPN Type**, and **IKEv1** and **IKEv2** configurations for each row and ensure that you provide the preshared key values for all the rows.

For configurations containing several site-to-site VPN tunnel configurations, to update the preshared keys for multiple entries at once, follow the steps below:

- Select the site-to-site VPN configuration entries for which you want to update the preshared keys.
- Click download () to export the table to an editable Excel sheet.
- Enter the preshared keys in the respective columns against each VPN configuration and save the file. For VPN configurations containing both IKEv1 and IKEv2 versions of IKE, ensure you enter two values in the column separated by a comma.
- Click upload (). The migration tool reads the entries in the Excel and automatically adds them to the corresponding preshared key columns of the VPN configurations.

  Note
  To update a preshared key that was missed to be updated as part of the bulk update, use the default method of selecting the entry and choosing **Actions** > **Update Pre-Shared Key** or export the Excel, update the key, and import it.

Step 6 In the **Remote Access VPN** section, all objects corresponding to Remote Access VPN are migrated from FDM-managed device 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 FDM-managed 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 FDM-managed device. 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 FDM-managed device. 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 FDM-managed device 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.

  ```
  ciscoFDM#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 Firewall 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, FDM-managed device supports IP and hostname or domain, but the management center supports only hostname or domain. If FDM-managed device config contains hostname or domain, it is retrieved and displayed. If FDM-managed device 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 FDM-managed device config), **AD Primary Domain** is a mandatory field to be configured on a management center. This field is not configured separately on FDM-managed device and extracted from the LDAP-base-dn config on FDM-managed device.

  ```
  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=FDM,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 FDM-managed device 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 FDM-managed device 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 overridden SAML trustpoint configuration is available in source FDM-managed device, it can be selected in **Override SAML** option.

  For information on exporting PKI certificates from FDM-managed device, see Export PKI Certificate from Device Manager and Import into Management Center.
- **Certificate Maps**—Certificate maps are displayed here.

Step 7 Under the **SNMP** tab, you can review, validate, and work with the following tabs:

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

SNMPV1/V2:

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

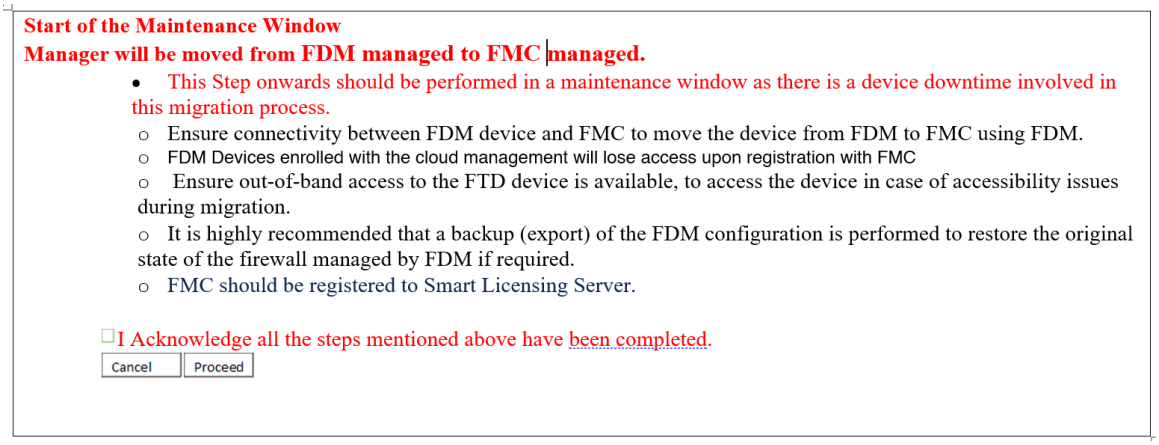
SNMPV3:

- **User Name**: The username for SNMP host
- **Authentication Password**: Click **Actions** to provide the authentication password for the user
- **Encryption Password**: Click **Actions** to provide the privacy password for the user

- **Validation State**: The user's validation state that will be created in the target management center

Start Maintenance and Move Manager

Once the shared configuration is pushed, you need to accept a popup to go to the maintenance window.



In the **Move Manager** page, following details should be provided:

- Select between **FTD is behind NAT Device, FMC is behind NAT Device, No Device is behind NAT (Default Setting)**
- **Management Center**/Security Cloud Control **Hostname or IP Address**: All the details will be fetched from the target manager. You can modify the IP if required.

Note Fields will be ignored if **FMC is behind NAT Device**.

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

Once you select **Move Manager**, the Secure Firewall migration tool triggers moving the manager from device manager to management center. After moving the manager the device will not be accessible from the device manager.

Optimize Review and Validate the Device Configuration to be migrated

Procedure

Step 1 Select the following tabs and review the configuration items:

- **Interfaces**
- **Routes**
- **Site-to-Site VPN Tunnels**

  For configurations containing several site-to-site VPN tunnel configurations, to update the preshared keys for multiple entries at once, follow the steps below:

  - Select the site-to-site VPN configuration entries for which you want to update the preshared keys.
  - Click download () to export the table to an editable Excel sheet.
  - Enter the preshared keys in the respective columns against each VPN configuration and save the file. For VPN configurations containing both IKEv1 and IKEv2 versions of IKE, ensure you enter two values in the column separated by a comma.
  - Click upload (). The migration tool reads the entries in the Excel and automatically adds them to the corresponding preshared key columns of the VPN configurations.

    Note
    To update a preshared key that was missed to be updated as part of the bulk update, use the default method of selecting the entry and choosing **Actions** > **Update Pre-Shared Key** or export the Excel, update the key, and import it.

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 2 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

Step 3 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 4 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 **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 Firewall 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 5 The **Optimize Your Configuration** dialog box displays a check mark next to each optimized attribute and identifies attributes that need optimization. Click **Proceed** to start the optimization. You can skip optimization, but it is recommended to optimize the attributes before proceeding with migration.

Step 6 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.

Push the Migrated Configuration to Firewall Management Center

You cannot push the migrated FDM-managed device configuration to Firewall 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 Firewall Management Center. It does not deploy the configuration to the Firewall Threat Defense device. However, any existing configuration on the Firewall 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 Firewall Management Center.

Procedure

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

Step 2 Click **Push Configuration** to send the migrated FDM-managed device configuration to Firewall 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.

Note
When the Secure Firewall Migration tool identifies duplicate object attributes, a dialog box appears and prompts you to correct the duplicate values. You can proceed with migration only after renaming the duplicate attributes.

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 Firewall Management Center in the console.

Note
If there are configurations with errors when a bulk configuration push is being done, the migration tool throws a warning, prompting you to abort the migration to fix the error manually or to continue the migration leaving out the incorrect configurations. You can choose to view the configurations that have errors and then select **Continue with migration** or **Abort**. If you abort the migration, you can download the troubleshooting bundle and share it with Cisco TAC for analysis.

If you continue the migration, the migration tool will treat the migration as a partial success migration. You can download the postmigration report to view the list of configurations that were not migrated because of the push error.

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 to be migrated, on page 23

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.

Procedure

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 FDM-managed device configuration was migrated:

- **Migration Summary**—A summary of the configuration that was successfully migrated from FDM-managed device to Firewall Threat Defense, including information about the FDM-managed device interface, Firewall Management Center hostname and domain, target Firewall Threat Defense device (if applicable), and the successfully migrated configuration elements.

You can also view a comparison chart that illustrates the difference between the count of pre-migration and post-migration states.

- **FDM Migration Path** —Shows the option which was selected between the three migration flows:
  - **Migrate Firepower Device Manager (Shared Configurations Only)**
  - **Migrate Firepower Device Manager (Includes Device & Shared Configurations)**
  - **Migrate Firepower Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware)**
- **Selective Policy Migration**—Details of the specific FDM-managed device feature selected for migration are available within three categories - Device Configuration Features, Shared Configuration Features, and Optimization.
- **FDM-managed device Interface to Threat Defense Interface Mapping**—Details of the successfully migrated interfaces and how you mapped the interfaces on the FDM-managed device configuration to the interfaces on the Firewall Threat Defense device. Confirm that these mappings match your expectations.

  Note
  This section is not applicable for migrations without a destination Firewall Threat Defense device or if **Interfaces** are **not** selected for migration.
- **Source Interface Names to Threat Defense Security Zones and Interface Groups**—Details of the successfully migrated FDM-managed device logical interfaces and name and how you mapped them to security zones and interface groups in Firewall Threat Defense. Confirm that these mappings match your expectations.

  Note
  This section is not applicable if **Access Control Lists** and **NAT** are **not** selected for migration.
- **Object Conflict Handling**—Details of the FDM-managed device objects that were identified as having conflicts with existing objects in Firewall Management Center. If the objects have the same name and configuration, the Secure Firewall migration tool reused the Firewall 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 FDM-managed device rules that were only partially migrated, including rules with advanced options where the rule could be migrated without the advanced options. Review these lines, verify whether the advanced options are supported in Firewall Management Center, and if so, configure these options manually.
- **Unsupported Configuration**—Details of FDM-managed device 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 Firewall Threat Defense. If so, configure those features manually in Firewall Management Center.
- **Expanded Access Control Policy Rules**—Details of FDM-managed device access control policy rules that were expanded from a single FDM-managed device Point rule into multiple Firewall Threat Defense rules during migration.
- **Actions Taken on Access Control Rules**

- **Access Rules You Chose Not to Migrate**—Details of the FDM-managed device 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 FDM-managed device access control policy rules that have IPS Policy applied. Review these rules carefully and determine whether the feature is supported in Firewall Threat Defense.
- **Access Control Rules that have File Policy Applied**—Details of all FDM-managed device access control policy rules that have File Policy applied. Review these rules carefully and determine whether the feature is supported in Firewall Threat Defense.
- **Access Control Rules that have Rule 'Log' Setting Change**—Details of the FDM-managed device 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.
- **Errors/Failure on Migrated Configuration**—Details on error causing the migration failure while pushing the migrated configuration elements. The error reported below could be related to the incorrect migrated configuration or else conflict on management center due to some existing configuration or unsupported feature. Review these errors and verify before proceeding or resuming the configuration push to the target management center.

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

Note
If 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 Firewall Management Center and Firewall Threat Defense, see Management Center Configuration Guide, Version 6.2.3.

Step 3 Open the **Pre-Migration Report** and make a note of any FDM-managed device configuration items that you must migrate manually on the Firewall Threat Defense device.

Step 4 In Firewall Management Center, do the following:

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

- Access control lists (ACL)
- Network Address Translation rules
- Port and network objects
- Routes

- Interfaces
- IP SLA objects
- Object Group Search
- Time-based objects
- 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

If you have changed the encryption of AD realm before migration, follow the below steps to revert the encryption type to LDAPS or STARTTLS:

1. Navigate to **Integration** section and click **Other Integrations**.
2. Select **Realms** and click **Edit** ( ) next to the specific realm to change the encryption type.
3. Click **Directory** and change the encryption type to **LDAPS** or **STARTTLS**.
4. Save and deploy the changes.

Step 5 After you have completed your review, deploy the migrated configuration from Firewall Management Center to the Firewall Threat Defense device.

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

The Secure Firewall migration tool assigns the policies to the Firewall Threat Defense device. Verify that the changes are reflected in the running configuration. To help you to identify the policies that are migrated, the description of those policies includes the hostname of the FDM-managed device configuration.

Uninstall the Secure Firewall Migration Tool

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

Before you begin

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

Procedure

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: FDM-managed device 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, on page 40

Pre-Maintenance Window Tasks

Before you begin

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

Procedure

Step 1 Obtain the FDM-managed configuration or connect to FDM-managed device to fetch the configuration.

Step 2 Review the FDM-managed device 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 Firewall Management Center.

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

Step 5 (Optional) If your source FDM-managed device 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 Firewall Management Center.

For more information, see Specify Destination Parameters for the Secure Firewall Migration Tool, on page 16.

Step 8 Map the FDM-managed device interfaces with the Firewall Threat Defense interfaces.

Note
The Secure Firewall migration tool allows you to map an FDM-managed device interface type to the Firewall Threat Defense interface type.

For example, you can map a port channel in FDM-managed device to a physical interface in Firewall Threat Defense.

For more information, see Map the FDM-managed device Interfaces with 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 FDM-managed device logical interfaces to the security zones.

For more information, see Map FDM-managed device Logical 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 Firewall Management Center.

Step 11 Review the Post Migration report, manually setup and deploy other configurations to the Firewall Threat Defense and complete the migration.

For more information, see Optimize, Review and Validate the Configuration to be migrated, on page 23.

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 39.

Procedure

Step 1 Connect to the FDM-managed device through the SSH console and switch to the interface configuration mode.

Step 2 Shutdown the FDM-managed device interfaces using the **shutdown** command.

Step 3 (Optional) Access the Firewall 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 FDM-managed device 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 Firewall Management Center for your Firepower 2100 device.