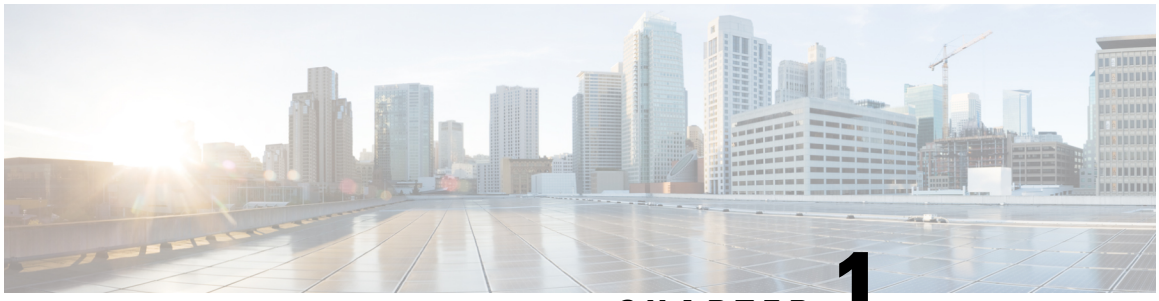
Migrating an ASA to an FDM-Managed Device Using Cisco Defense Orchestrator

First Published: 2019-06-17

Last Modified: 2020-05-06

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

CONTENTS



CHAPTER 1

Getting Started

Choose the Right Migration Process

There are two methods to migrate Adaptive Security Appliance (ASA) configurations to FDM-managed devices using Cisco Defense Orchestrator (CDO):

- CDO solution—If you intend to migrate your ASA configurations to FDM-managed devices and manage them with CDO and Firepower Device Manager, use the cloud-based process in CDO to migrate your ASA configurations.
- On-Premise solution (Firepower Device Manager)—If you intend to migrate your ASA configurations to FDM-managed devices, use the cloud-based process in CDO to migrate your ASA configurations. You can then use the Firepower Device Manager to manage your configuration.

This guide assumes that you have a basic understanding of CDO operations. To learn more, see the CDO Data Sheet.

About the Cisco Defense Orchestrator Migration Process

CDO can help you migrate your Adaptive Security Appliance (ASA) to an FDM-managed device. CDO provides the **ASA to FDM Migration** wizard to help you migrate your ASA's running configuration to an FDM template.

Note The *show-fdm* and *enable-asa-to-ftd-migration* feature flags must be enabled to view the **ASA to FDM Migration** option under **Tools & Services.** Contact TAC to activate the **ASA to FDM Migration** option if unavailable under **Tools & Services**.

You can migrate the following elements of ASA's running configuration to an FDM template using the **ASA to FDM Migration** wizard:

- Interfaces
- Routes
- Access Control Rules (ACLs)
- Network Address Translation (NAT) rules
- Network objects and network group objects

Note CDO does not support object names with reserved keywords. Rename the object names by adding a suffix "ftdmig" to it.

- Service objects and service group objects
- Site-to-Site VPN

CDO migrates only referenced objects. Objects in an access control list, which are defined but are not referenced to an access group are not migrated. Some of the common reasons CDO fails to migrate certain elements can be one or more of the following:

- ICMP access lists with no ICMP code
- TCP/UDP access lists with no access group configuration
- IP access lists not mapped to site-to-site VPN profiles
- Any network objects or groups referred to access lists that are not migrated
- Interfaces referred as shutdown

Note Any unreferenced object or object-groups in the configuration will also be dropped and marked as unused during the migration. See the **Migration Report** for information about elements that have not been migrated.

Once these elements of the ASA running configuration have been migrated to the FDM template, you can then apply the FDM template to a new FDM-managed device that is managed by CDO. The FDM-managed device adopts the configurations defined in the template, and so, the FDM-managed is now configured with some aspects of the ASA's running configuration.

Other elements of the ASA running configuration are not migrated using this process. Those other elements are represented in the FDM template by empty values. When the template is applied to the FDM-managed device, we apply values we migrated to the new device and ignore the empty values. Whatever other default values the new device has, it retains. Those other elements of the ASA running configuration that we did not migrate, will need to be recreated on the FDM-managed device outside the migration process.

License for the Migration Process

The FDM-managed device migration process is part of CDO and does not require any specific license other than the CDO license.

Guidelines and Limitations

Note Configurations that are not supported in CDO will be dropped during migration as **Unsupported** and will be reported in the **Migration Report**.

Feature or Function Name	What Can be Migrated	Restrictions or Limitations of Migration
Firewall Modes	Routed firewall mode	Transparent mode configurations cannot be migrated.

Interface Configurations	• Physical interfaces
	• Subinterfaces
		• The FDM-managed device must have equal or more physical interfaces than the ASA interface configurations being migrated.
		• Subinterfaces (subinterface ID will always be set to the same number as the VLAN ID on migration)
		• The following interface configurations will not be migrated to FDM-managed device:
		  • Secondary VLANs on ASA interfaces
		  • Redundant Interface
		  • Bridge Group Interface
		  • Virtual Tunnel Interface

Feature or Function Name	What Can be Migrated	Restrictions or Limitations of Migration
EtherChanels	EtherChannels configured on physical interfaces. The member interfaces mapped to EtherChanels are retained during migration.	• Before migrating the configurations, you must create the equivalent number of EtherChannels on the FDM-managed device using CDO. See Add an EtherChannel Interface for an FDM-Managed Device. • Can only be migrated to configurations of Firepower 1000 or 2100 series hardware devices: 1010, 1120, 1140,1150, 2110, 2120, 2130, 2140. • You can migrate EtherChannel configurations from ASA 8.4+ to FDM-managed device running on software version 6.5+. • The EtherChannels created on the FDM-managed device before migration must be of the same type as the EtherChannel being migrated. CDO will only migrate Etherchannel to EtherChannel and physical interface to physical interface. • Member interfaces mapped to EtherChannels in the FDM template will not be available to users during Interface mapping step of the migration wizard. However, they are retained and migrated to their assigned EtherChannels.

Routing	Static routes	• When there are multiple static routes with the same network as destination, only one route with minimum metric value is migrated and others are dropped.
		• The following route features will not be migrated to FDM-managed device:
		  • Tunneled routes
		  • Null 0 interface routes
		  • Static routes with SLA track

Feature or Function Name	What Can be Migrated	Restrictions or Limitations of Migration
Access Control Rules (ACLs)	• Enabled Access Control Rules • Source and destination objects • CDO supports actions like Allow, Trust, and Block for FDM-managed device. During the migration, permit and deny actions in the source ASA configuration are handled and are mapped to the supported action for FDM-managed device on CDO. • CDO supports migration of ACLs attached to a policy, interface, or an access group without an IP protocol. • ACE with unencrypted L3 Tunnel protocols	The following ACL features will not be migrated to FDM-managed device: • CDO and Firepower Device manager do not support ACL with IPv4 and IPv6 mixed protocols • Logging severity-level information • Inactive or disabled rules • ACE with service object or service group having non-TCP, UDP, or ICMP protocols • ACE with non-TCP or UDP service objects • Non-TCP or UDP protocol in ACE with inline objects • ACEs with Time-range • Access list not mapped with access group
Network Address Translation (NAT) Rules	• Network Object (Auto) and twice (Manual) NAT or PAT • Static NAT • Dynamic NAT or PAT • Identity NAT • Source Port (service) Translation	The following NAT rules features will not be migrated to FDM-managed device: • PAT pool • Unidirectional • Inactive • With Twice NAT, the use of **destination** service objects for destination port (service) translation (including service objects that have both the source and destination) • Destination port translation • NAT46, NAT64 **Note** CDO does not support network object with 0.0.0.0/32.

Feature or Function Name	What Can be Migrated	Restrictions or Limitations of Migration
Service Objects and Service Group Objects	Service Objects and Nested Groups See Supported IP Protocols on CDO for the list of protocols used in services objects that CDO supports.	• The protocols, BCC-RCC-MON, and BBN-RCC-MON, are not supported. • Operators like less than, greater than, and not equal to, are not supported. • Object-group nesting
Network Objects and Network Group Objects	Network Objects and Network Group Objects	The following network object or network group are unsupported: • Discontinuous Mask Based • IP address starting with first octet ‘0’ in IPv4 address
ICMP Types	ICMP Types	The following ICMP types are unsupported: • ICMP–based service object entries with INVALID ICMP type or/and code • Service–type or ICMP–type object without code for ICMPv4 or ICMPv6 type • Any unassigned ICMP type (as per IANA) or Invalid ICMP type
Miscellaneous Unsupported Objects	-	The following miscellaneous objects are unsupported: • SGT–based Network Object-Group • User–based Network Object-Group

Feature or Function Name	What Can be Migrated	Restrictions or Limitations of Migration
Site-to-Site VPN	• Phase 1 and Phase 2 proposals for both IKEv1 and IKEv2 • Perfect Forward Secrecy (PFS) for both IKEv1 and IKEv2 • Crypto Access List with Nested Object-Group • Crypto Map with multiple peer IPs • Both IKEv1 and IKEv2 used for a tunnel in Crypto Map	The following Site-to-Site VPN features are not supported: • VPN-Filter • vpn-idle-timeout • isakmp keepalive threshold 10 retry 10 • Crypto Map VPNMAP 200 set security-association lifetime seconds 360 • set security-association lifetime kilobytes unlimited • set security-association lifetime seconds 3600 • Certificate Authentication • Dynamic Crypto Map • Route–based VPN (virtual tunnel interface)

For more information on Guidelines and Limitations, see Guidelines and Limitations for ASA Configurations and Guidelines and Limitations for FDM-managedDevices.

Supported IP Protocols on CDO

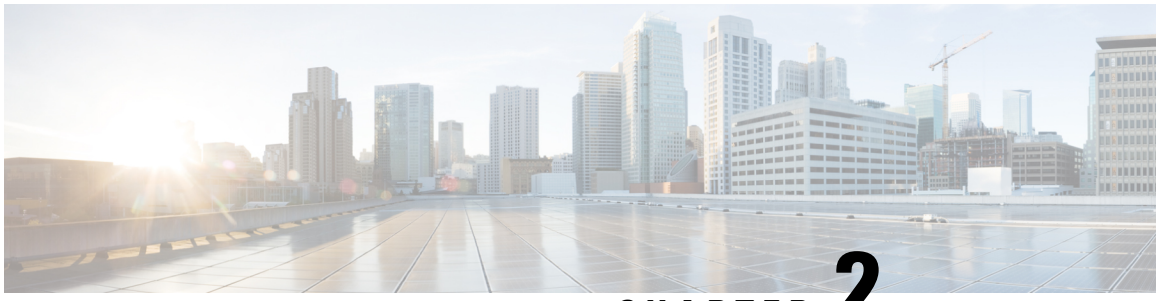
The IP Protocols that CDO supports in service objects are as follows:

IP Protocols in Service Objects			
1= ICMP	34 = THREEPC	73 = CPHB	106= QNX
2 = IGMP	35 = IDPR	74 = WSN	107 = AN
3 = GGP	36 = XTP	75 = PVP	108 = IPCOMP
5 = ST2	37 = DDP	76 = BRSATMON	109= SNP
6 = TCP	38 = IDPRCMTP	78 = WBMON	110 = COMPAQPEER
7 = CBT	39 = TPPLUSPLUS	77 = SUNND	111 = IPXINIP
8 = EGP	40 = IL	79 = WBEXPAK	112 = VRRP
9 = IGP	42 = SDRP	80 = ISOIP	113= PGM
10 = BBNRCCMON	45 = IDRP	81 = VMTP	115 = L2TP
11 = NVP2	46 = RSVP	82 = SECUREVMTP	116 = DDX
12 = PUP	48 = MHRP	83 = VINES	117= IATP
13 = ARGUS	49 = BNA	84 = TTP	118 = ST
14 = EMCON	50 = ESP	85 = NSFNETIGP	119= SRP
15=XNET	51 = AH	86 = DGP	120= UTI
16 = CHAOS	52 = INLSP	87 = TCF	121= SMP
17 = UDP	53 = SWIPE	88 = EIGRP	122= SM
18 = MUX	54 = NARP	89 = OSPFIGP	123= PTP
19 = DCNMEAS	55 = MOBILE	90 = SPRITERPC	124= ISIS
20 = HMP	56 = TLSP	91 = LARP	125 = FIRE
21 = PRM	57 = SKIP	92 = MTP	126 = CRTP
22 = XNSIDP	58= IPv6-ICMP	93 = AX25	127 = CRUDP
23 = TRUNK1	59 = IPv6NONXT	94 = IPIP	128 = SSCOPMCE
24 = TRUNK2	62 = CFTP	95 = MICP	129 = IPLT
25 = LEAF1	64 = SATEXPAK	96 = SCCSP	130= SPS
26 = LEAF2	65 = KRYPTOLAN	97 = ETHERIP	131= PIPE
27 = RDP	66 = RVD	98 = ENCAP	132 = SCTP
28 = IRTP	67 = IPPC	100 = GMTP	133 = FC
29 = ISOTP4	69 = SATMON	101 = IFMPP	254 = DIVERT
30 = NETBLT	70 = VISA	102= PNNI	
31 = MFENSP	71 = IPCV	103= PIM	
32 = MERITINP	72 = CPNX	104 = ARIS	
33 = SEP		105= SCPS	

Best Practices

Follow these best practices when using CDO to migrate an ASA configuration to an FDM template:

- Ensure you fetch the running configuration from an ASA device using **show run** command in a model device migration.
- Review the migration reports for skipped, unsupported, and partially supported configurations.
- After migration, verify the migrated rules and objects in the FDM template before deploying it to an FDM-managed device.
- Optimize your ASA policies before migrating them to the FDM template.
- We recommend that you deploy the migrated ASA configuration to the FDM-managed device that does not have an existing configuration.



CHAPTER 2

Migrating ASA to an FDM-Managed Device Workflow

How to Implement the Migration Process

	Do This
Step 1	Prepare for Migration, on page 11 • Onboard an ASA Device • Optimize Your ASA Policies Before You Migrate • Add EtherChannel Configurations to FDM-Managed Device Before Migrating, on page 13

Step 2	Run the Migration, on page 13
	• Select the Device to Migrate
	• (Optional) Update the Migration Name
	• Parsing the ASA Configuration
	• Apply Migration
	  • Apply Migration Now
	  • Apply Migration Later

Step 3	View the Migration Actions
Step 4	Deploy the Configuration, on page 22

Prepare for Migration

To prepare your devices for migration, ensure that:

- You have a CDO tenant and you can log into it. See Initial Login for more information.
- You have onboarded to your tenant the ASA device or ASA configuration file that you want to migrate to an FDM-managed device.

  Your ASA's running configuration file must be less than 4.5 MB and 22,000 lines. See Confirming ASA Running Configuration Size.
- You have onboard an FDM-managed device to CDO if you want to migrate the ASA configuration to the device directly after the migration process, or if you want to migrate EtherChannel configurations to the FDM-managed device. See Onboard an FTD device for more information.
- The devices must be in **synced** state.

  This ensures that the running configuration on the device and the running configuration that is stored in CDO are the same.
- Your ASA is running software version 8.4 or later.

To know more about device support summary, unsupported devices, hardware and software specifics, see Software and Hardware Supported by CDO.

Onboard an ASA Device

Click (+) from the **Inventory** page.

The **Onboarding** page displays where you can onboard the device.

How to Onboard an ASA Device

Perform the following to onboard an ASA device with any of these options:

- Onboard a live ASA device.
- Import configuration for offline management:
  - Enter the **Device Name** and chose the **Device Type** as ASA.
  - Click **Browse** to choose the ASA Configuration file that is a *.TXT* or a *.CFG* file.
  - Click **Upload**.

Optimize Your ASA Policies Before You Migrate

Now that you have all your ASAs onboarded, start using CDO to identify and correct problems with network objects, optimize your existing policies, review your VPN connections, and upgrade your ASAs to the newest releases.

Resolve Network Object Issues

Start to optimize the security policies on your ASAs by resolving issues with network policy objects.

- Unused objects—CDO identifies network policy objects that exist in a device configuration but are not referenced by another object, an access-list, or a NAT rule. Find these unused objects and delete them.
- Duplicate objects—Duplicate objects are two or more objects on the same device with different names but the same values. These objects are usually created accidentally, serve similar purposes, and are used

by different policies. Look for opportunities to standardize names while recognizing that some duplicates may exist for legitimate reasons.

- Inconsistent objects—Inconsistent objects are objects on two or more devices with the same name but different values. Sometimes users create objects in different configurations with same name and content but over time the values of these objects diverge which creates the inconsistency. Consider standardizing the values in these objects or renaming one to identify it as a different object.

Fix Shadow Rules

Now that you have resolved your network object issues, review network policies for shadow rules and fix them. A shadow rule is marked by a half-moon badge on the network policies page. It is a rule in a policy that will never trigger because a rule with higher priority in the policy acts on all the packets before they reach the shadowed rule. If there is a shadowed rule that will never be hit, remove it, or edit the policy to bring that rule "into the light."

Add EtherChannel Configurations to FDM-Managed Device Before Migrating

Before you begin

Review this information:

- Prepare for Migration, on page 11
- The Guidelines and Limitations, on page 3 for migrating EtherChannels.

Procedure

Step 1 Before migrating the EtherChannel configurations, you must create the equivalent number of EtherChannels on the FDM-managed device that you are migrating from ASA. You can use CDO to create the EtherChannels. See Add an EtherChannel Interface for an FDM-Managed Device for instructions.

The minimum configuration for an EtherChannel is an EtherChannel ID and at least one EtherChannel member.

Step 2 Deploy the changes to your FDM-managed device.

What to do next

Continue to Run the Migration, on page 13.

Run the Migration

Select the Device to Migrate

You can select the ASA device for migration using any of the following methods:

- Launch the FDM Migration Wizard and Select the Device.
- Select the Device and Launch the FDM Migration Wizard

Launch the FDM Migration Wizard and Select the Device

Procedure

Step 1 Log into your CDO tenant.

Step 2 In the navigation bar, click **Tools & Services**.

Step 3 Under **Tools & Services**, select **ASA to FDM Migration**.

Note The *show-fdm* and *enable-asa-to-ftd-migration* feature flags must be enabled to view the **ASA to FDM Migration** option under **Tools & Services.** Contact TAC to activate the **ASA to FDM Migration** option if unavailable under **Tools & Services**.

Step 4 In the FDM Migration page, click (+) to add an ASA device or to upload config file you want to migrate to the FDM-managed device.

Step 5 Upload the ASA config file or select the device from the drop-down list.

If there have been previous migrations of this device, you will see the resulting migrations from the selected device.

For more information on filtering, see About Migrations Filters.

If this is a new migration, click **Start a new migration for (device name)**.

Select the Device and Launch the FDM Migration Wizard

Procedure

Step 1 Log into your CDO tenant.

Step 2 In the navigation bar, click **Inventory**.

Step 3 Click the **Devices** tab to locate your device.

Step 4 Click the **ASA** tab and select the ASA device or model you want to migrate to the FDM-managed device.

The device details of the selected ASA device like the location, model, serial, and so on, are displayed in the **Device Details** pane.

Step 5 In the **Device Actions** pane, click **Migrate to FDM**.

If there have been previous migrations of this device, you will see the resulting migrations from the selected device.

For more information on filtering, see About Migrations Filters.

If this is a new migration, click **Start a new migration for (device name)**.

Step 6 (Optional) If you want to select a different ASA device or a model to migrate to the FDM template, see About Migrations Filters.

(Optional) Update the Migration Name

Migration name is auto-generated based on the device name and the timestamp.

Procedure

Step 1 In the **FDM Migration** screen, you can also update the migration name or retain the default name. CDO allows you to search the migration list with the migration name.

Note The FDM template name will be the same as the migration name by default.

Step 2 Click **Next** to trigger the migration.

(Optional) Preserve the Running Configuration

Note This is applicable only when you chose live ASA from the **Inventory** page.

In **Preserve Running Configuration**, the Migration tool allows you to save CDO's copy of the ASA's running configuration as an configuration file. This model device configuration is used for migration thus not affecting the live ASA.

The following options are available for migrating a CDO's copy of the ASA's running configuration to FDM-managed device:

- Create an configuration file from the CDO's copy of the ASA's running device

Note Allows you to retain a snapshot (model device) of the ASA configuration at the point of initiating the migration. When you are required to make the configuration changes for migration purposes, you can use the configuration file without affecting/interrupting the CDO's copy of the ASA's running configuration.

- Migrate the configuration directly from the device

Note The source configuration for the migration is a CDO's copy of the ASA's running configuration. The migration tool considers only the configuration from the time the migration starts. Any changes to that CDO's copy of the ASA's running configuration later, will not be reflected in the resulting migration. The additional migration attempts from the changed CDO's copy of the ASA's running configuration might result in different FDM-managed device configurations.

Procedure

Step 1 Enter the model device name under **Model Device Name** field.

Step 2 Perform one of these actions:

a) Click **Next**.

The model device is created and triggers the migration for that device.

b) Click **Skip** to trigger the migration on the live ASA.

Parsing the ASA Configuration

Note Depending on the size of the configuration files and the number of other devices or services, it may take a while for the configuration to get parsed. For more information, see Confirming ASA Running Configuration Size.

The parsing of the migration continues until it succeeds or fails. The migration process gathers ASA information, parses it, creates an FDM template and enables this FDM template to be applied to a device in CDO. For more information on FDM templates, see Templates. During the parsing phase, the migration process generates a **Migration Report** and a **Migration Log** that identify:

- ASA configuration items that are fully migrated, partially migrated, unsupported for migration, and ignored for migration.
- ASA configuration lines with errors, listing the ASA CLIs that the migration process cannot recognize; this blocks migration.

Note Management interface and Static routes that are associated with the management interface are not migrated.

Fix the Migration Errors

When there is a migration error, you can review the **Review Migration Report** and **Review Migration Log** in the **FDM Migration** screen.

Select **Download Report** and **Download Log** from the **FDM Migration** screen to download the migration report and logs.

Reports and logs must be able to print the lines in the ASA configuration that caused the parsing failure. Navigate to the ASA device that you have chosen for migration, update the ASA configuration, and then restart the new migration.

If the parse is successful but the FDM template creation fails, navigate to **Template** > **Workflows** or **Migration** > **Workflows** to identify any failures and address the issues.

Reparse After Fixing the Migration Errors

You can reparse the ASA configuration after fixing the migration errors. Perform the following:

- In the **FDM Migration** screen, click **Go to Configuration**.
- Go to the specific configuration and make the configuration changes that caused the conversion failure.
- Once you make the updates for the correct configuration, click **Re-parse the configuration** to trigger the migration against the changed configuration.

Note The **Re-parse the configuration** option is applicable only when you have updated the configuration file and for the configuration with parsing errors only.

Apply Migration

To apply the migration, you can choose one of these options:

- Apply Migration Now
- Apply Migration Later

As per the CDO apply template feature, the FDM template that is created during migration deploys the changes on the device, only to the following: Interfaces, NAT, ACLs, Objects, and Routes.

The DHCP and Data DNS settings are restored to default, as the interface information would have changed during the migration.

The Other settings like VPN, HA, and so on, remain the same on the device.

Apply Migration Now

Note Before applying the migration on a device, check whether the device is in **synced** state.

You can apply the FDM template to any device, review the device template, and deploy to the device later by selecting the FDM-managed device.

Procedure

Step 1 Select **Apply Migration Now**.

a) From the **Select FTD Device** drop-down list, select the FDM-managed device for which you want to apply the FDM device template.

The device state must be "**Synced**" with "**Online**" connectivity.

b) Click **Select** to select the FDM-managed device.

Step 2 Click **Next**.

Step 3 In the **Map Interfaces** row, the Migration tool retrieves a list of **Template Interfaces** and the **Devices Interfaces** on the FDM-managed device. By default, the Firewall Migration Tool maps the interfaces in ASA and the FDM-managed device according to their interface identities. Click **Continue**.

For more information on mapping ASA Interfaces with FDM-managed devices, see Map ASA Interfaces with Firewall Threat Defense Interfaces.

Step 4 Review the FDM template information to be applied to the FDM-managed device, and then click **Apply Template**.

Step 5 In the **Done** row, you can do the following:

You have successfully applied the migrated configuration to the selected FDM-managed device.

- Click **Remove model device used for migration** check box.

  Selecting the check box removes the model device that is created from live ASA. This will also remove the model device, deletes the migration logs and the files that are associated with the migration.

  Note This check box is displayed only when the live ASA is selected from the **Inventory** page and only if the user has created the model device.

- Click the **Save migrated configuration as a template** check box.

  Note This check box is displayed only when the FDM template is applied successfully and is checked by default.

  If the check box is unchecked, the FDM template is not saved.

  If you encounter any error while applying the FDM template, navigate to **Device** > **Workflows** to view the errors and address the issues.

  Note You can access these FDM templates from the **Devices & Services** page. For more information on the FDM templates, see Templates.

  Note After the FDM template is saved successfully, you can perform the following actions:

Take one of these actions:

- Click **Preview and Deploy** to deploy the configuration.

  You can verify the list of objects that will be deployed in the **Preview and Deploy** page.

- Click **Go to Devices** that provides you an option to deploy the configuration.

(Optional) Post-Migration Tasks

- Navigate to the FDM template to review the migration results.
- Optimize the configurations using CDO capabilities.
- Deploy the FDM template to the device.

Support for FDM-Managed Device with Management Access Interface Migration

Note The Apply Template feature is not supported for a target device that has management access interface. Modify the FDM template manually before applying it on the target FDM-managed device.

When you apply any migrated FDM template on a target device that has management access interface configured, the apply template feature fails due to mismatch in the mapped interfaces. On the target FDM-managed device, the management access interface configuration and the corresponding static routes must be preserved to ensure the connectivity with CDO. Therefore, to avoid connectivity failures, you must manually configure the management access interfaces along with required static routes by following these steps, and then apply the FDM template. This section provides the procedure that you must follow to ensure successful migration.

If there are multiple management access interfaces and the interfaces are configured incorrectly or unused, you must update the target FDM-managed device to maintain only the relevant management access interface configured, so that the unused interfaces can be used for the migrated configuration.

Procedure

Step 1 Update the physical interface in the template by modifying the IP address and subnet mask of the data interfaces so that it is the same as that of the management access interface.

Note The management access interface of the Target FDM-managed device must be mapped with the management access interface in the FDM template. The IP address and subnet mask of the FDM template must be the same as that of the target FDM-managed device.

a) Navigate to the **Inventory** page.
b) Click the **Template** tab.
c) Click the **Threat Defense** tab and select the FDM device template.
d) Choose **Interface** from the **Management** pane.
e) Click **Edit** in the **Editing Physical Interface** dialog box.
f) Enter the **IP Address** and the **Subnet Mask**.
g) Click **Save**.

Step 2 Add the data interface as management access interface in the template settings:

a) Navigate to the **Inventory** page.
b) Click the **Template** tab.
c) Click the **Threat Defense** tab and select the FDM device template.
d) Navigate to **Settings** on the right side of the **Management** pane.
e) In the **Data Interface** pane, click **+** to add an interface as management access interface.

Note Ensure that the data interface has a name, state, and the IP address.

f) Click **Save**.

Step 3 Add or update the static routes with the interfaces associated on the device. When you map the management access interface to an additional interface, set the routing configuration for the selected FDM-managed device.

For more information to add or update the static routes, see Configure Static for Threat Devices.

Apply Migration Later

Procedure

Step 1 Select **Apply Migration Later**.

A migration template is saved. You can save the created template and apply the template to the FDM-managed device later.

Note You can access the FDM templates from the **Inventory** page.

Once the FDM template is saved successfully, you can perform the following actions:

- Navigate to the FDM template to review the migration results.
- Optimize the FDM template using CDO capabilities.
- Navigate to the destination FDM-managed device and select the FDM template that has to be applied.
- Deploy the FDM template to the device.

Step 2 Click **Done**.

The **Inventory** page is displayed with the preselected FDM template.

CDO allows you to perform all the template-related actions like review policies, configurations, and so on.

Step 3 When you are ready to apply the FDM template:

a. Select the target FDM-managed device from the **Inventory** page.

b. Click **Apply Template** from the **Device Actions** pane.

The **Apply Device Configuration** screen is displayed.

c. Select the FDM template that you want to apply on the device.

d. Click **Apply**.

Note The Management Interface IP that is running on the device remains unchanged.

View the Migration Actions

The **Migration Table** screen displays the following:

- The Migration Name. By default, CDO generates the migration name that is based on the device name. You can also customize this name. See (Optional) Update the Migration Name.
- The timestamp of the last migration activity performed on the device.
- Displays the migration state of the device. For more information on the migration states, see Migration States and Description.
- Allows you to perform various actions like rename, download log, and so on. For more information on the actions, see Actions and Descriptions.

Table 1: Migration States and Description

Migration States	Description
Parsing	Migration in progress.
Parse Error	The parsing is complete, with errors.
Conversion Error	The conversion is complete with errors.
Template Created	The migration is complete. The FDM template is successfully created, but with validation errors.

For more information on fixing the migration errors, see Fix the Migration Errors.

Table 2: Actions and Description

Action	Description
Resume	Resumes from the step where the migration process stopped. For example, if the migration is complete, then the process resumes from applying the FDM template.
Rename	Rename the migration name.
Workflows	Displays the workflow screen.
Download Log	Allows you to download the log files in the TXT format. This is a parsing log.
Download Report	Allows you to download the report details in the HTML format.
Configuration	Allows you to view the ASA configuration against which the migration was performed.
Remove	Removes the migration and its associated files like the log files.

About Migrations Filters:

If you want to select a different ASA device or a model to migrate to the FDM template, use any of the following options:

- Filter by Device
- Filter by Clear option

Filter by Device

You can use many different filters on the **Migrations** page to find objects you are looking for. The migrations filter allows you to filter by device, state, and time range.

Table 3: Filter Attributes and the Descriptions

Filter Attribute	Description
Filter by Device	Allows you to select a specific device for migration.
State	• Error—Displays the migration list that is based on the parsing errors. • Done—Displays the migration list that is based on the FDM template that is successfully created.
Time Range	Start, End—Displays the list of devices based on the selected start and end dates of migration.

Filter by Clear option

1. Click **Clear** to clear the filter bar.
2. Click the (+) icon.
3. Select a device from the list or search for it by name and select it.
4. Click **Select**.

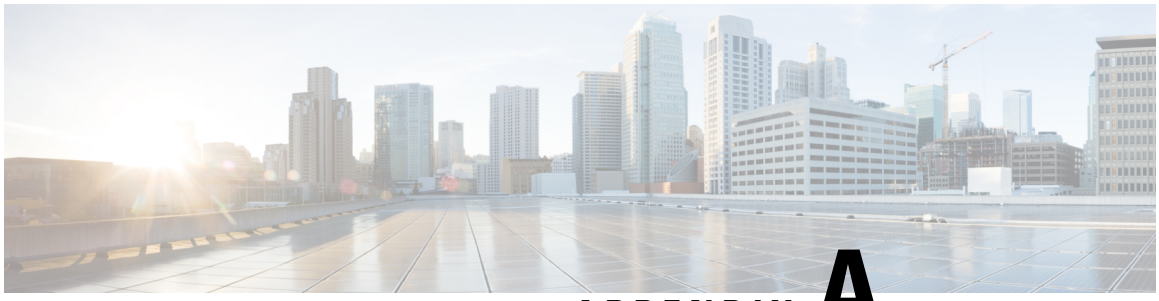
   The **FDM Migration** screen is displayed.

Deploy the Configuration

The final step is to deploy the configuration changes you made to the device.

For more information, see Deploy the Device Configuration.

See Managing FDM Devices with Cisco Defense Orchestrator and Managing FMC with Cisco Defense Orchestrator to learn about how CDO can manage the different aspects of an FDM-managed device and its security policies.



APPENDIX A

Telemetry

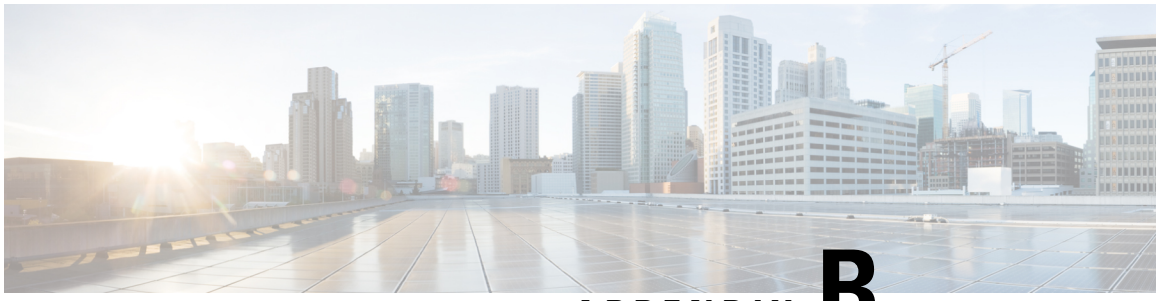
Cisco Success Network

Note CDO does not manage the Cisco Success Network settings. The device manager user interface manages the settings and provides the telemetry information.

Cisco Success Network is user-enabled cloud service. When you enable Cisco Success Network, a secure connection is established between the device and the Cisco Cloud to stream usage information and statistics.

For more information, see Cisco Success Network-Telemetry Data.

Telemetry



APPENDIX B

Frequently Asked Questions

Troubleshooting FAQs

Q. Why does it take a longer time to parse?

A. If the ASA configuration file size is large, then it takes longer time to parse. Your ASA's running configuration file must be less than 4.5 MB and 22,000 lines. For more information, see Confirming ASA Running Configuration Size.

Q. What must I do when I find parsing errors during migration?

A. Refer to the **Review Migration Report** and **Review Migration Logs** for the error details.

Q. I am encountering parsing errors during migration. How do I fix them?

A. Navigate to the **Migration** page, click **Download Logs**, for the specific device and fix the errors.

Q. I get conversion errors during FDM template generation. What must I do?

A. Navigate to the **Migration** page, click **Workflows** for the specific device to view the errors.

Q. What to do when an FDM template is created with errors?

A. If your FDM template is created with validation errors, you can search for the FDM template in the **Inventory** page. Click **Workflows** from the **Devices Actions** pane where you can view the error details.

Q. CDO fails to write to the change log. Why?

A. When you onboard an ASA to CDO, CDO stores copy of the ASA's running configuration file in its database. Generally, if that running configuration file is too large (4.5 MB or larger), or it contains too many lines (approximately 22,000 lines), or there are too many access-list entries for a single access group, CDO will not be able to predictably manage that device. For more information, see Confirming ASA Running Configuration Size.

You can also contact your Cisco account team for help to safely reduce the size of your configuration file without disrupting your security policies.

Q. Does CDO validate the syntax of the ASA configuration file before it migrates?

A. No. CDO does not validate the syntax of the ASA configuration file before it migrates it to an FDM template. If you are trying to migrate an ASA model that you have onboarded to CDO, and the migration

fails, review the migration report and review the migration log in the FDM migration screen. You may need to verify the syntax of the configuration file.

Q. Why weren't some of my access lists and network objects migrated?

A. CDO migrates only referenced objects. Objects in an access control list, which are defined but are not referenced to an access group are not migrated. In addition, some of the common reasons CDO fails to migrate certain elements can be one or more of the following:

- ICMP access lists with no ICMP code
- TCP/UDP access lists with no access group configuration
- IP access lists not mapped to site-to-site VPN profiles
- Any network objects or groups referred to access lists that are not migrated
- Interfaces referred as shutdown

See the **Migration Report** for more information about elements that have not been migrated.