Getting Started with the Secure Firewall Migration Tool

About the Secure Firewall Migration Tool

This guide contains information on how you can download the Secure Firewall migration tool and complete the migration. In addition, it provides you troubleshooting tips to help you resolve migration issues that you may encounter.

The sample migration procedure (Sample Migration: FDM-managed device to Threat defense 2100) included in this book helps to facilitate understanding of the migration process.

The Secure Firewall migration tool converts supported FDM-managed device configurations to a supported Secure Firewall Threat Defense platform. The Secure Firewall migration tool allows you to automatically migrate the supported FDM-managed device features and policies to threat defense. You must manually migrate all unsupported features.

The Secure Firewall migration tool gathers FDM-managed device information, parses it, and finally pushes it to the Secure Firewall Management Center. During the parsing phase, the Secure Firewall migration tool generates a **Pre-Migration Report** that identifies the following:

- FDM-managed device configuration items that are fully migrated, partially migrated, unsupported for migration, and ignored for migration.
- FDM-managed device configuration lines with errors that lists the FDM-managed device components which the Secure Firewall migration tool cannot recognize; this blocks the migration.

Console

The console opens when you launch the Secure Firewall migration tool. The console provides detailed information about the progress of each step in the Secure Firewall migration tool. The contents of the console are also written to the Secure Firewall migration tool log file.

The console must stay open while the Secure Firewall migration tool is open and running.

Important When you exit the Secure Firewall migration tool by closing the browser on which the web interface is running, the console continues to run in the background. To completely exit the Secure Firewall migration tool, exit the console by pressing the Command key + C on the keyboard.

Logs

The Secure Firewall migration tool creates a log of each migration. The logs include details of what occurs at each step of the migration and can help you determine the cause if a migration fails.

You can find the log files for the Secure Firewall migration tool in the following location: `<migration_tool_folder>\logs`

Resources

The Secure Firewall migration tool saves a copy of the **Pre-Migration Reports**, **Post-Migration Reports**, FDM-managed device configs, and logs in the **Resources** folder.

You can find the **Resources** folder in the following location: *<migration_tool_folder>\resources*

Unparsed File

You can find the unparsed file in the following location:

<migration_tool_folder>\resources

Search in the Secure Firewall Migration Tool

You can search for items in the tables that are displayed in the Secure Firewall migration tool, such as those on the **Optimize, Review and Validate** page.

To search for an item in any column or row of the table, click the **Search** () above the table and enter the search term in the field. The Secure Firewall migration tool filters the table rows and displays only those that contain the search term.

To search for an item in a single column, enter the search term in the **Search** field that is provided in the column heading. The Secure Firewall migration tool filters the table rows and displays only those that match the search term.

Ports

The Secure Firewall migration tool supports telemetry when run on one of these 12 ports: ports 8321-8331 and port 8888. By default, Secure Firewall migration tool uses port 8888. To change the port, update port information in the *app_config* file. After updating, ensure to relaunch the Secure Firewall migration tool for the port change to take effect. You can find the *app_config* file in the following location: *<migration_tool_folder>\app_config.txt*.

Note We recommend that you use ports 8321-8331 and port 8888, as telemetry is only supported on these ports. If you enable Cisco Success Network, you cannot use any other port for the Secure Firewall migration tool.

Notifications Center

All the notifications, including success messages, error messages, and warnings that pop up during a migration are captured in the notifications center and are categorized as **Successes**, **Warnings**, and **Errors**. You can click the 

icon on the top right corner any time during the migration and see the various notifications that popped up, along with the time they popped up in the tool.

Cisco Success Network

Cisco Success Network is a user-enabled cloud service. When you enable Cisco Success Network, a secure connection is established between the Secure Firewall migration tool and the Cisco cloud to stream usage information and statistics. Streaming telemetry provides a mechanism to select data of interest from the Secure Firewall migration tool and to transmit it in a structured format to remote management stations for the following benefits:

- To inform you of available unused features that can improve the effectiveness of the product in your network.
- To inform you of additional technical support services and monitoring that is available for your product.
- To help Cisco improve our products.

The Secure Firewall migration tool establishes and maintains the secure connection and allows you to enroll in the Cisco Success Network. You can turn off this connection at any time by disabling the Cisco Success Network, which disconnects the device from the Cisco Success Network cloud.

What's New in the Secure Firewall Migration Tool

Version	Supported Features
7.0.1	

Version	Supported Features
	This release includes the following new features and enhancements: • You can now migrate configurations from your Cisco firewalls such as ASA and FDM-managed devices and third-party firewalls to Cisco Secure Firewall 1200 Series devices. See: Cisco Secure Firewall 1200 Series • You can now update the preshared keys for more than one site-to-site VPN tunnel configuration at once. Export the site-to-site VPN table in the **Optimize, Review and Validate Configuration** page to an Excel sheet, specify the preshared keys in the respective cells, and upload the sheet back. The migration tool reads the preshared keys from the Excel and updates the table. See: Optimize, Review, and Validate the Configuration Supported migrations: All • You can now choose to ignore migration-hindering, incorrect configurations and still continue the final push of a migration. Previously, the whole migration failed even if a single object's push failed because of errors. You also now have the control to abort the migration manually to fix the error and retry migration. See: Push the Migrated Configuration to Management Center Supported migrations: All • The Secure Firewall migration tool now detects existing site-to-site VPN configurations in the target threat defense device and prompts you to choose if you want them deleted, without having to log in to the management center. You could choose **No** and manually delete them from the management center to continue with the migration. See: Optimize, Review, and Validate the Configuration Supported migrations: All • If you have an existing hub and spoke topology configured on one of the threat defense devices managed by the target management center, you could choose to add your target threat defense device as one of the spokes to the existing topology right from the migration tool, without having to manually do it on the management center. See: Optimize, Review, and Validate the Configuration Supported migrations: Secure Firewall ASA • When migrating thrid-party firewalls, you can now select threat defense devices as target, which are part of a high availability pair. Previously, you could only choose standalone threat defense devices as target devices. Supported migrations: Palo Alto Networks, Check Point, and Fortinet firewall migrations • The Secure Firewall migration tool now provides a more enhanced, intuitive demo mode, with guided migration instructions at every step. In addition, you

Version	Supported Features
	can also see versions of target threat defense devices to choose and test based on your requirements. Supported migrations: All
7.0	This release includes the following new features and enhancements: **Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense Migration** • You can now configure a threat defense high availability (HA) pair on the target management center and migrate configurations from a Secure Firewall ASA HA pair to the management center. Choose **Proceed with HA Pair Configuration** on the **Select Target** page and choose an active and a standby device. When selecting the active threat defense device, ensure you have an identical device on the management center for the HA pair configuration to be successful. See Specify Destination Parameters for the Secure Firewall Migration Tool in the *Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool* book for more information. • You can now configure a site-to-site hub and spoke VPN topology using threat defense devices when migrating site-to-site VPN configurations from an ASA device. Click **Add Hub & Spoke Topology** under **Site-to-Site VPN Tunnels** on the **Optimize, Review and Validate Configuration** page. See Optimize, Review, and Validate the Configuration in the *Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool* book for more information. **Fortinet Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate IPv6 and multiple interface and interface zones in SSL VPN and central SNAT configurations from a Fortinet firewall to your threat defense device. See Fortinet Configuration Support in *Migrating Fortinet Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool* book for more information.

Version	Supported Features
6.0.1	This release includes the following new features and enhancements: **Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense Migration** • You can now optimize network and port objects when you migrate configurations from Secure Firewall ASA to threat defense. Review these objects in their respective tabs in the **Optimize, Review and Validate Configuration** page and click **Optimize Objects and Groups** to optimize your list of objects before migrating them to the target management center. The migration tool identifies objects and groups that have the same value and prompts you to choose which to retain. See Optimize, Review, and Validate the Configuration for more information. **FDM-managed Device to Cisco Secure Firewall Threat Defense Migration** • You can now migrate DHCP, DDNS, and SNMPv3 configurations from your FDM-managed device to a threat defense device. Ensure you check the **DHCP** checkbox and **Server**, **Relay**, and **DDNS** checkboxes on the **Select Features** page. See Optimize, Review, and Validate the Configuration for more information. **Fortinet Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate URL objects in addition to other object types from a Fortinet firewall to your threat defense device. Review the **URL Objects** tab in the **Objects** window in **Optimize, Review and Validate Configuration** page during migration. See Optimize, Review, and Validate the Configuration for more information. **Palo Alto Networks Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate URL objects in addition to other object types from a Palo Alto Networks firewall to your threat defense device. Ensure you review the **URL Objects** tab in the **Objects** window in **Optimize, Review and Validate Configuration** page during migration. See Optimize, Review, and Validate the Configuration for more information. **Check Point Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate port objects, FQDN objects, and object groups from a Check Point Firewall to your threat defense device. Review the **Objects** window in **Optimize, Review and Validate Configuration** page during migration. See Optimize, Review, and Validate the Configuration for more information.

Version	Supported Features
6.0	

Version	Supported Features
	This release includes the following new features and enhancements: **Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense Migration** • You can now migrate WebVPN configurations on your Secure Firewall ASA to Zero Trust Access Policy configurations on a threat defense device. Ensure that you check the **WebVPN** checkbox in **Select Features** page and review the new **WebVPN** tab in the **Optimize, Review and Validate Configuration** page. The threat defense device and the target management center must be running on Version 7.4 or later and must be operating Snort3 as the detection engine. • You can now migrate Simple Network Management Protocol (SNMP) and Dynamic Host Configuration Protocol (DHCP) configurations to a threat defense device. Make sure that you check the **SNMP** and **DHCP** checkboxes in the **Select Features** page. If you have configured DHCP on your Secure Firewall ASA, note that the DHCP server, or relay agent and DDNS configurations can also be selected to be migrated. • You can now migrate the equal-cost multipath (ECMP) routing configurations when performing a multi-context ASA device to a single-instance threat defense merged context migration. The **Routes** tile in the parsed summary now includes ECMP zones also, and you can validate the same under the **Routes** tab in the **Optimize, Review and Validate Configuration** page. • You can now migrate dynamic tunnels from the dynamic virtual tunnel interface (DVTI) configurations from your Secure Firewall ASA to a threat defense device. You can map them in the **Map ASA Interfaces to Security Zones, Interface Groups, and VRFs** page. Ensure that your ASA Version is 9.19 (x) and later for this feature to be applicable. **FDM-managed Device to Cisco Secure Firewall Threat Defense Migration** • You can now migrate the Layer 7 security policies including SNMP and HTTP, and malware and file policy configurations from your FDM-managed device to a threat defense device. Ensure that the target management center Version is 7.4 or later and that **Platform Settings** and **File and Malware Policy** checkboxes in **Select Features** page are checked. **Check Point Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate the site-to-site VPN (policy-based) configurations on your Check Point firewall to a threat defense device. Note that this feature applies to Check Point R80 or later versions, and management center and threat defense Version 6.7 or later. Ensure that the **Site-to-Site VPN Tunnels** checkbox is checked in the **Select Features** page. Note that, because this is a device-specific configuration, the migration tool does not display these configurations if you choose to **Proceed without FTD**. **Fortinet Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now optimize your application access control lists (ACLs) when migrating configurations from a Fortinet firewall to your threat defense device.

Version	Supported Features
	Use the **Optimize ACL** button in the **Optimize, Review and Validate Configuration** page to see the list of redundant and shadow ACLs and also download the optimization report to see detailed ACL information.
5.0.1	This release includes the following new features and enhancements: • The Secure Firewall migration tool now supports migration of multiple transparent firewall-mode security contexts from Secure Firewall ASA devices to threat defense devices. You can merge two or more transparent firewall-mode contexts that are in your Secure Firewall ASA device to a transparent-mode instance and migrate them. In a VPN-configured ASA deployment where one or more of your contexts have VPN configurations, you can choose only one context whose VPN configuration you want to migrate to the target threat defense device. From the contexts that you have not selected, only the VPN configuration is ignored and all other configurations are migrated. See Select the ASA Security Context for more information. • You can now migrate site-to-site and remote access VPN configurations from your Fortinet and Palo Alto Networks firewalls to threat defense using the Secure Firewall migration tool. From the **Select Features** pane, select the VPN features that you want to migrate. See the Specify Destination Parameters for the Secure Firewall Migration Tool section in Migrating Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Migration Tool and Migrating Fortinet Firewall to Secure Firewall Threat Defense with the Migration Tool guides. • You can now select one or more routed or transparent firewall-mode security contexts from your Secure Firewall ASA devices and perform a single-context or multi-context migration using the Secure Firewall migration tool.

Version	Supported Features
5.0	• Secure Firewall migration tool now supports migration of multiple security contexts from Secure Firewall ASA to threat defense devices. You can choose to migrate configurations from one of your contexts or merge the configurations from all your routed firewall mode contexts and migrate them. Support for merging configurations from multiple transparent firewall mode contexts will be available soon. See Select the ASA Primary Security Context for more information. • The migration tool now leverages the virtual routing and forwarding (VRF) funtionality to replicate the segregated traffic flow observed in a multi-context ASA environment, which will be part of the new merged configuration. You can check the number of contexts the migration tool has detected in a new **Contexts** tile and the same after parsing, in a new **VRF** tile in the **Parsed Summary** page. In addition, the migration tool displays the interfaces to which these VRFs are mapped, in the **Map Interfaces to Security Zones and Interface Groups** page. • You can now try the whole migration workflow using the new demo mode in Secure Firewall migration tool and visualize how your actual migration looks like. See Using the Demo Mode in Firewall Migration Tool for more information. • With new enhancements and bug fixes in place, Secure Firewall migration tool now provides an improved, faster migration experience for migrating Palo Alto Networks firewall to threat defense.
4.0.3	The Secure Firewall migration tool 4.0.3 includes bug fixes and the following new enhancements: • The migration tool now offers an enhanced **Application Mapping** screen for migrating PAN configurations to threat defense. See Map Configurations with Applications in *Migrating Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Migration Tool* guide for more information.
4.0.2	The Secure Firewall migration tool 4.0.2 includes the following new features and enhancements: • The migration tool now has an always-on telemetry; however, you can now choose to send limited or extensive telemetry data. Limited telemetry data inludes few data points, whereas extensive telemetry data sends a more detailed list of telemetry data. You can change this setting from **Settings** > **Send Telemetry Data to Cisco?**.
4.0.1	The Secure Firewall migration tool 4.0.1 includes the following new features and enhancements: The Secure Firewall migration tool now analyzes all objects and object groups based on both their name and configuration, and reuses objects that have the same name and configuration. Only network objects and network object groups were analyzed based on their name and configuration before. Note that the XML profiles in remote access VPNs are still validated only using their name.

Version	Supported Features
4.0	Secure Firewall migration tool 4.0 supports: Migration of FDM-managed device to management center provided the destination management center version is 7.3 or later and the source device manager version is 7.2 or later. The version of the device manager must be equal to or lower than the version of the destination management center. The following options are available for the migration: 1. **Migrate Firepower Device Manager (Shared Configurations only)**: This option allows you to migrate staged migrations. In this case, you can initially migrate all shared configurations and migrate the device configurations at a later stage as per your requirements. During the migration process, only the shared configurations are migrated to the targeted management center. The configuration bundle obtained from the device manager can be uploaded or the device manager credentials can be provided for the tool to fetch the configuration details. Automated fetching of the configuration details is the preferred method. 2. **Migrate Firepower Device Manager (Includes Device and Shared configurations)**: This option allows you to migrate both, the device and the shared configurations from the device manager to the targeted management center. Once the source device and its configuration are migrated to the targeted management center, the FDM-managed device becomes the targeted management center device. For the tool to fetch the configuration details, you must provide the device manager credentials. Only an automated fetching of the configurations is allowed for this migration option. 3. **Migrate Firepower Device Manager (Includes Device and Shared Configurations) to FTD Device (New Hardware)**: This option allows you to migrate both, the device and the shared configuration to a threat defense device managed by the targeted management center. In this case, during the migration process, the source device is not migrated and only the device configuration is migrated to the new threat defense device. The configuration bundle obtained from the device manager can be uploaded or the device manager credentials can be provided for the tool to fetch the configuration details. Automated fetching of the configuration details is the preferred method.

Platform Requirements for the Secure Firewall Migration Tool

The Secure Firewall migration tool has the following infrastructure and platform requirements:

- Runs on a Microsoft Windows 10 64-bit operating system or on a macOS version 10.13 or higher
- Has Google Chrome as the system default browser
- (Windows) Has Sleep settings configured in Power & Sleep to Never put the PC to Sleep, so the system does not go to sleep during a large migration push

- (macOS) Has Energy Saver settings configured so that the computer and the hard disk do not go to sleep during a large migration push

Requirements and prerequisites for the FDM-Managed Device configuration file

You can obtain an FDM-managed device configuration bundle either manually or by connecting to a live FDM-managed device from the Secure Firewall migration tool. A manual upload is only supported for the following options:

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

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

The FDM-managed device configuration bundle that you manually import into the Secure Firewall migration tool must meet the following requirements:

- Contains only valid device manger CLI configurations.
- Includes the version number.
- Configuration bundle should be in .zip format.
- Has a fully exported configuration that is exported from the device manager, see Export the FDM-managed device Configuration File, on page 28.
- Needs to have minimum one .txt file which has the configuration.
- Keys should be provided for encrypted bundle. For unencrypted bundle, the encryption key can be left empty.
- Does not contain syntax errors.
- Has not been hand coded or manually altered.

Requirements and Prerequisites for Threat Defense Devices

When you migrate to the management center, it may or may not have a target threat defense device added to it. You can migrate shared policies to a management center for future deployment to a threat defense device. To migrate device-specific policies to a threat defense, you must add it to the management center. As you plan to migrate your FDM-managed device configuration to threat defense, consider the following requirements and prerequisites:

- Threat Defense hardware must be greater than or equal to the FDM-managed device model. Example, if source FDM-managed device model is 2100, then the destination threat defense model can be 2100 or 3100 or 4100 or 9300 and not any model lower than 2100.
- The target threat defense device must be registered with the management center.
- The target threat defense device can be in a high availability configuration.
- The threat defense device can be a standalone device or a container instance. It must **not** be part of a cluster.
  - The target native threat defense device must have at least an equal number of used physical data and port channel interfaces (excluding 'management-only' and subinterfaces) as that of the FDM-managed device; if not you must add the required type of interface on the target threat defense device. Subinterfaces are created by the Secure Firewall migration tool that are based on physical or port channel mapping.
  - If the target threat defense device is a container instance, at minimum it must have an equal number of used physical interfaces, physical subinterfaces, port channel interfaces, and port channel subinterfaces (excluding 'management-only') as that of the FDM-managed device; if not you must add the required type of interface on the target threat defense device.

Note

- Subinterfaces are not created by the Secure Firewall migration tool, only interface mapping is allowed.
- Mapping across different interface types is allowed, for example: physical interface can be mapped to a port channel interface.

FDM-Managed Device Configuration Support

Supported FDM-Managed Device Configuration

The Secure Firewall migration tool can fully migrate the following FDM-managed device configurations:

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

Note Although the Secure Firewall migration tool does not migrate extended service objects (configured for a source and destination), referenced ACL and NAT rules are migrated with full functionality.

- Service object groups, except for nested service object groups

Note Since nesting is not supported on the management center, the Secure Firewall migration tool expands the content of the referenced rules. The rules, however, are migrated with full functionality.

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

  The Secure Firewall migration tool creates IP SLA Objects, maps the objects with the specific static routes, and migrates the objects to management center.

  IP SLA monitor defines a connectivity policy to a monitored IP address and tracks the availability of a route to the IP address. The static routes are periodically checked for availability by sending ICMP echo requests and waiting for the response. If the echo requests are timed-out, the static routes are removed from the routing table and replaced with a backup route. SLA monitoring jobs start immediately after deployment and continue to run unless, you remove the SLA monitor from the device configuration, that is, they do not age out. The IP SLA monitor objects are used in the Route Tracking field of an IPv4 static route policy. IPv6 routes do not have the option to use SLA monitor through route tracking.

- Object Group Search

  Enabling object group search reduces memory requirements for access control policies that include network objects. We recommend you to enable object group search that enhances optimal memory utilization by access policy on threat defense.

Note

- Object Group Search is unavailable for management center or threat defense version earlier than 6.6.
- Object Group Search will not be supported for shared configuration flow and will be disabled.
- Time-based objects

- Time-based objects

  When the Secure Firewall migration tool detects time-based objects that are referenced with access-rules, the Secure Firewall migration tool migrates the time-based objects and maps them with respective access-rules. Verify the objects against the rules in the **Review and Validate Configuration** page.

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

Note You must manually migrate timezone configuration from source FDM-managed device to target FTD.

- Site-to-Site VPN Tunnels
  - Site-to-Site VPN—When the Secure Firewall migration tool detects crypto map configuration in the source FDM-managed device, the Secure Firewall migration tool migrates the crypto map to the management center VPN as point-to-point topology.
  - Crypto map (static/dynamic) based VPN from FDM-managed device
  - Route-based (VTI) FDM VPN
  - Certificate-based VPN migration from FDM-managed device
  - FDM-managed device trustpoint or certificates migration to the management center must be performed manually and is part of the pre-migration activity.
- Dynamic-Route Objects, BGP, and EIGRP
  - Policy-List
  - Prefix-List
  - Community List
  - Autonomous System (AS)-Path
- Remote Access VPN
  - SSL and IKEv2 protocol.
  - Authentication methods—AAA only, Client Certificate only, SAML, AAA, and Client Certificate.
  - AAA—Radius, Local, LDAP, and AD.
  - Connection Profiles, Group-Policy, Dynamic Access Policy, LDAP Attribute Map, and Certificate Map.
  - Standard and Extended ACL.
  - As part of pre-migration activity, perform the following:
    - Migrate the FDM-managed device trustpoints manually to the management center as PKI objects.

    - Retrieve AnyConnect packages, Hostscan Files (Dap.xml, Data.xml, Hostscan Package), External Browser package, and AnyConnect profiles from the source FDM-managed device.
    - Upload all AnyConnect packages to the management center.
    - Upload AnyConnect profiles directly to the management center or from the Secure Firewall migration tool.

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

Partially Supported FDM-Managed Device Configurations

The Secure Firewall migration tool partially supports the following FDM-managed device configurations for migration. Some of these configurations include rules with advanced options that are migrated without those options. If the management center supports those advanced options, you can configure them manually after the migration is complete.

- Access control policy rules that are configured with advanced logging settings, such as severity and time-interval.
- Static routes that are configured with the track option.
- Certificate-based VPN migration.
- Dynamic-Route Objects, EIGRP, and BGP
    - Route-Map

Unsupported FDM-Managed Device Configurations

The Secure Firewall migration tool does not support the following FDM-managed device configurations for migration. If these configurations are supported in the management center, you can configure them manually after the migration is complete.

- SGT-based access control policy rules
- SGT-based objects
- User-based access control policy rules
- NAT rules that are configured with the block allocation option

- Objects with an unsupported ICMP type and code
- Tunneling protocol-based access control policy rules

Note Support with a prefilter on Secure Firewall migration tool and management center 6.5.

- NAT rules that are configured with SCTP
- NAT rules that are configured with host ‘0.0.0.0’
- Default route obtained through DHCP or PPPoE with SLA tracking
- SLA monitor schedule
- Transport mode IPsec transform-set
- FDM-managed device trustpoint migration into management center
- Transparent firewall mode for BGP
- SNMPv3 user groups and host groups

Objects in FDM-Managed Device and Threat Defense

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

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

- Certificate map
- DAP
- Intrusion policy
- Intrusion rules

Guidelines and Limitations

FDM-Managed Device Migration Guidelines

Following are the guidelines for migrating FDM-managed device configuration using Secure Firewall migration tool:

- Each FDM-managed device object has a unique name and configuration—The Secure Firewall migration tool migrates the objects successfully without changes.
- The name of an FDM-managed device object includes one or more special characters that are not supported by the management center—The Secure Firewall migration tool renames the special characters in the object name with a "_" character to meet the management center object naming criteria.
- An FDM-managed device object has the same name and configuration as an existing object in the Management Center—The Secure Firewall migration tool reuses the management center object for the threat defense configuration and does not migrate the FDM-managed device object.
- Multiple FDM-managed device objects have the same name but in different cases—The Secure Firewall migration tool renames such objects to meet the threat defense object naming criteria.

Important The Secure Firewall migration tool analyzes both name and configuration of all objects and object groups. However, XML profiles in remote-access VPN configurations are analyzed only using the name.

FDM-managed device Configuration Limitations

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

- Unsupported objects and NAT rules are not migrated.
- Unsupported ACL rules are migrated as disabled rules into the management center.
- All supported FDM-managed device crypto map VPN will be migrated as management center point-to-point topology.
- Unsupported or incomplete static crypto map VPN topologies are not migrated.
- You cannot migrate some FDM-managed device configurations, for example, dynamic routing to threat defense. Migrate these configurations manually.
- Nested service object-groups or port groups are not supported on the management center. As part of conversion, the Secure Firewall migration tool expands the content of the referenced nested object-group or port group.

- The Secure Firewall migration tool splits the extended service object or groups with source and destination ports that are in one line into different objects across multiple lines. References to such access control rules are converted into management center rules with the exact same meaning.
- If the source FDM-managed device configuration has access control rules that do not refer to specific tunneling protocols (like GRE, IP-in-IP and IPv6-in-IP), but these rules match unencrypted tunnel traffic on the FDM-managed device, then, on migration to the threat defense, the corresponding rules will not behave in the same way they do on the FDM-managed device. We recommend that you create specific tunnel rules for these in the Prefilter policy, on the threat defense.
- Supported FDM-managed device crypto map will be migrated as point-to-point topology.
- If an AS-Path object with the same name in management center appears, then the migration stops with the following error message:

  "Conflicting AS-Path object name detected in the management center, please resolve conflict in management center to proceed further"
- Route-Map Object is partially migrated using Secure Firewall migration tool. The match and set clauses are not supported due to API limitations.
- Layer 7 policies such as identity policy, SSL policy, security intelligence, SGT, and user-based rules are not migrated due to API Limitations.

Limitations for RA VPN Migration

Remote Access VPN migration is supported with the following limitations:

- Custom attributes, SSL settings and VPN load balancing migration is not supported due to API limitations.
- LDAP server is migrated with encryption type as "none".
- DfltGrpPolicy is not migrated as the policy is applicable for the entire management center. You can make the necessary changes directly on the management center.
- For a radius server, if dynamic authorization is enabled, the AAA server connectivity should be through an interface and not dynamic routing. If FDM-managed device configuration is found with AAA server with dynamic authorization enabled without interface, the Secure Firewall migration tool ignores dynamic authorization. You must enable dynamic-authorization manually after selecting an interface on the management center.
- Bypass access control sysopt permit-vpn option is not enabled under RA VPN policy. However, if required, you can enable it from the management center.
- AnyConnect client module and profile values can be updated under group policy only when the profiles are uploaded from Secure Firewall migration tool to the management center.
- You need to map the certificates directly on the management center.
- IKEv2 parameters are not migrated by default. You must add them through the management center.

Supported Platforms for Migration

The following FDM-managed device and threat defense platforms are supported for migration with the Secure Firewall migration tool. For more information about the supported threat defense platforms, see Cisco Secure Firewall Compatibility Guide.

Supported Source FDM-Managed Device Platforms

You can use the Firewall Migration Tool to migrate the configuration from the following FDM-managed device platforms:

- Firepower 1000 Series
- Firepower 2100 Series
- Secure Firewall 3100 Series
- Firepower 4100 Series
- Secure Firewall 4200 Series
- Firepower 9300 Series
- FDM virtual on VMware, AWS, Azure, KVM

Supported Target Threat Defense Platforms

You can use the Secure Firewall migration tool to migrate a source configuration to the following standalone or container instance of the threat defense platforms:

- Firepower 1000 Series
- Firepower 2100 Series
- Secure Firewall 3100 Series
- Firepower 4100 Series
- Secure Firewall 4200 Series
- Firepower 9300 Series that includes:
  - SM-24
  - SM-36
  - SM-40
  - SM-44
  - SM-48
  - SM-56
- Threat Defense on VMware, deployed using VMware ESXi, VMware vSphere Web Client, or vSphere standalone client

- Threat Defense Virtual on Microsoft Azure Cloud or AWS Cloud

Note

- For pre-requisites and pre-staging of threat defense virtual in Azure, see Getting Started with Secure Firewall Threat Defense Virtual and Azure.
- For pre-requisites and pre-staging of threat defense virtual in AWS Cloud, see Threat Defense Virtual Prerequisites.

For each of these environments, once pre-staged as per the requirements, the Secure Firewall migration tool requires network connectivity to connect to the management center in Microsoft Azure or AWS Cloud, and then migrate the configuration to the management center in the Cloud.

Note The pre-requisites of pre-staging the management center or threat defense virtual is required to be completed before using the Secure Firewall migration tool, to have a successful migration.

Supported Target Management Center for Migration

The Secure Firewall migration tool supports migration to threat defense devices managed by the management center and cloud-delivered Firewall Management Center.

Management Center

The management center is a powerful, web-based, multi-device manager that runs on its own server hardware, or as a virtual device on a hypervisor. You can use both On-Prem and Virtual management center as a target management center for migration.

The management center should meet the following guidelines for migration:

- The Management Center software version that is supported for migration, as described in Supported Software Versions for Migration, on page 23.
- You have obtained and installed smart licenses for threat defense that include all features that you plan to migrate from the interface, as described in the following:
  - The Getting Started section of Cisco Smart Accounts on Cisco.com.
  - Register the Firewall Management Center with the Cisco Smart Software Manager.
  - Licensing the Firewall System
  - You have enabled management center for REST API.

    On the management center web interface, navigate to **System** > **Configuration** > **Rest API Preferences** > **Enable Rest API** and check the **Enable Rest API** check box.

Important You need to have an administrator user role in management center to enable REST API. For more information on management center user roles, see User Roles.

Cloud-Delivered Firewall Management Center

The cloud-delivered Firewall Management Center is a management platform for threat defense devices and is delivered via Cisco Defense Orchestrator. The cloud-delivered Firewall Management Center offers many of the same functions as a management center.

You can access the cloud-delivered Firewall Management Center from CDO. CDO connects to cloud-delivered Firewall Management Center through the Secure Device Connector (SDC). For more information about cloud-delivered Firewall Management Center, see Managing Cisco Secure Firewall Threat Defense Devices with Cloud-Delivered Firewall Management Center.

The Secure Firewall migration tool supports cloud-delivered Firewall Management Center as a destination management center for migration. To select the cloud-delivered Firewall Management Center as destination management center for migration, you need to add the CDO region and generate the API token from CDO portal.

CDO Regions

CDO is available in three different regions and the regions can be identified with the URL extension.

Table 1: CDO Regions and URL

Region	CDO URL
Europe Region	https://defenseorchestrator.eu/
US Region	https://defenseorchestrator.com/
APJC Region	https://www.apj.cdo.cisco.com/

Supported Software Versions for Migration

The following are the supported Secure Firewall migration tool, FDM-managed device and threat defense versions for migration:

Supported Secure Firewall Migration Tool Versions

The versions posted on software.cisco.com are the versions formally supported by our engineering and support organizations. We strongly recommend you download the latest version of Secure Firewall migration tool from software.cisco.com.

Supported FDM-Managed Device Versions

The Secure Firewall migration tool supports migration from an FDM-managed device that is running threat defense software version 7.2 and later.

Supported Management Center Versions for source FDM-Managed Device Configuration

For an FDM-managed device, the Secure Firewall migration tool supports migration to a threat defense device managed by a management center that is running version 7.2+.

Note

- Some features are only supported in the latest version of management center and threat defense.
- For optimum migration times, we recommend that you upgrade the management center to suggested release version mentioned in the software.cisco.com/downloads.

Supported Threat Defense Versions

For FDM-managed device, the Secure Firewall migration tool supports migration to a device that is running threat defense version 7.2 and later.

For detailed information about the Cisco Firewall software and hardware compatibility, including operating system and hosting environment requirements, for threat defense, see the Cisco Firewall Compatibility Guide.