Welcome to Firepower Migration Tool

This document provides critical and release-specific information for Cisco Firepower Migration Tool. Even if you are familiar with Firepower releases and have previous experience with the migration process, make sure you thoroughly read and understand this document.

New Features in this Release

In this release, the following features have been added:

- **ASA Login**: The Migration Tool allows you to connect to an ASA using the admin credentials and **Enable Password** as configured on the ASA.
  
  If ASA is not configured with **Enable Password**, you can leave the field blank on the Migration Tool.

- **Support for the Bundle Feature**: Provides customer support to download log files, DB, and configuration files during a migration failure. You can also raise a support case with the technical team through an email.

- **Do not Migrate support for NAT and Routes**: The Migration Tool provides support to skip migration of the selected NAT rules and Route interfaces. The previous versions of the Migration Tool provided this option for Access Control rules only.

- **Support for IPv6**: Support for migration of IPv6 configurations in Objects, Interfaces, ACLs, NAT, and Routes.

- **Interface Mapping Enhancements**: The Migration Tool allows you to map an ASA interface name to a physical interface on the FTD object types—physical interfaces, port channel, and subinterfaces. For example, you can map a port channel in ASA to a physical interface in FMC.

- **Inline Grouping Support**: The Migration Tool allows you to parse CSM or ASDM managed configurations.
  
  When you opt to clear the inline grouping CSM or ASDM managed configurations, the predefined objects are replaced with the actual object or member name.
  
  If you do not clear the CSM or ASDM managed configurations, the predefined object names will be retained for migration.

- **Miscellaneous Updates**
  
  - You can download the parsed Access Control, NAT, Network Objects, Port Objects, Interface, and Routes configuration items from the **Review and Validate Configuration** screen in an excel or CSV format.
You cannot import a CSV file.

- You can now configure the batch size limit for Bulk Push in the `app_config` file as follows:
  - For Objects, the batch size cannot exceed 500. The Migration Tool resets the value to 50 and proceeds with the bulk push.
  - For ACLs, Routes, and NAT, the batch size cannot exceed 1000 each. The Migration Tool resets the value to 1000 and proceeds with the bulk push.

**Supported Configurations**

The following configuration elements are supported for migration:

- Network objects
- Service Objects (which are referred to as port objects in Firepower Threat Defense)
- Access lists
- NAT rules
- Interfaces (Exceptions: Redundant, Routed Mode-BVI, VTI (Tunnel Interface))

**Note**

If your source ASA has Port Channel interfaces, you must create Port Channel Interfaces on the Firepower Management Center; subinterfaces will be automatically created.

- Static routes (without SLA track, dynamic routing not supported)
- Routed and transparent firewall mode
- Name command reference supported in network objects and groups, ACLs, and routes

**Migration Workflow**

**Note**

Beginning with release 2.0, the Migration Tool supports migrating Check Point configuration to FTD. Please note this important tip as part of the Migration workflow.

You can obtain ASA configuration items for migration by following one of the following methods:

- **Manual Upload Method**: In a single context mode, use the `show run` command to obtain the ASA configuration. In multi-context mode use the `show tech` command to obtain ASA configuration

- **Connect to the ASA from the Migration Tool**: In a multi-context ASA, select the context to migrate after connecting to the ASA and select a target Firepower Threat Defense device. When you complete
migration of the first context, repeat the steps to migrate other contexts - connect to the ASA, select the context to be migrated and select a target Firepower Threat Defense device.

You can obtain Check Point configuration items for migration only through the manual upload method. To collect the Check Point configuration through manual upload method, do the following:

- **Export Configuration using the Check Point Web Visualization Tool (WVT):** Open the command prompt window to the directory where WVT is saved and extracted, and execute the following command to obtain the Check Point configuration:


- **Export Device configuration using the FMT-CP-Config-Extractor Tool:** Open the FMT-CP-Config-Extractor Tool which is a Windows executable file (.exe) on the workstation that has access to the Check Point Security Gateway.

- **Zip the Exported Files:** Select all the eight files (seven from the Web Visualization Tool (WVT)) and (one .txt file from the FMT-CP-Config-Extractor Tool) and compress them to a zip file.

---

**Firepower Migration Tool Features**

The Firepower Migration Tool provides the following features:

- Validation throughout the migration, including parse and push operations
- Object re-use capability
- Object conflict resolution
- Interface mapping
- Auto-creation or reuse of interface objects (ASA nameif to security zones and interface groups mapping)
- Subinterface limit check for the target Firepower Threat Defense device

**Platforms supported**

- Virtual ASA to Virtual FTD
- Same hardware migration (X to X device migration)
- X to Y device migration (Y having higher number of interfaces)

**Migration Reports**

The Firepower Migration Tool provides the following reports in HTML format with details of the migration:

- Pre-migration report
- Post-migration report
Platform Requirements for the Firepower Migration Tool

The Migration Tool has the following infrastructure and platform requirements:

- Windows 10 operating system or on a macOS version 10.13 or higher
- Google Chrome as the system default browser
- A single instance of the tool per system
- Firepower Management Center and Firepower Threat Defense must be version 6.2.3.3 or above

Documentation

The following documentation is provided with this release:

- Firepower Migration Tool Release Notes
- Migrating ASA to Firepower Threat Defense with the Firepower Migration Tool
- Open Source Used in Cisco Firepower Migration Tool

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note

You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account on Cisco.com. For more information on Bug Search Tool, see Bug Search Tool Help.

Use these dynamic queries for an up-to-date list of open and resolved caveats in Firepower Migration Tool:

- Open Caveats
- Resolved Caveats