# Cisco Secure Firewall Migration Tool Release Notes, 10.0.2

**First Published:** 2026-03-23

## About Secure Firewall Migration Tool

The Secure Firewall Migration Tool enables you to migrate your firewall configurations to a supported Secure Firewall Threat Defense managed by a management center. The migration tool supports migration from Secure Firewall ASA, ASA with FirePOWER Services (FPS), FDM-managed devices, as well as third-party firewalls from Microsoft Azure, Check Point, Palo Alto Networks, and Fortinet.

This document provides critical and release-specific information about the Secure Firewall Migration Tool. Even if you are familiar with Secure Firewall releases and have previous experience with the migration process, we recommend that you read and thoroughly understand this document.

## New Features

| Release Version | Feature | Descriptions |
|---|---|---|
| 10.0.2 | Patch release | This patch release contains bug fixes. See Open and Resolved Issues for more information. |

## Open and Resolved Issues

### Resolved Issues

| Bug ID | Description |
|---|---|
| CSCws11375 | During migration from Adaptive Security Appliance (ASA) to Firewall Threat Defense with the Firewall Migration Tool, user objects, object-groups, and referenced access lists are not migrated to the target Firewall Management Center. |
| CSCws26165 | When performing an ASA to Firewall Threat Defense migration with the Firewall Migration Tool, an error appears while pushing Remote Access VPN:<br>`'NoneType' object has no attribute 'name'` |
| CSCws31820 | Migration from ASA to Firewall Threat Defense using Firewall Migration Tool fails with error:<br>`Error while pushing interface: Management only is not supported for Switched/Passive/ERSPAN mode.` |

| Bug ID | Description |
|---|---|
| CSCws38212 | Migration from Check Point firewall to Firewall Threat Defense using Firewall Migration Tool fails with error:<br>`Error while pushing security zone: 'LogRecord' object has no attribute 'message'` |
| CSCws43079 | Migration from ASA to Firewall Threat Defense using Firewall Migration Tool fails with error:<br>`Error while pushing s2s vpn: Non Homogeneous Protected Networks. Endpoints have Protected Networks of different types` |
| CSCws46729 | Parsing is blocked with an error during migration from Palo Alto Networks (PAN) to Firewall Threat Defense using the Firewall Migration Tool:<br>`Internal server error during parsing of PAN config` |
| CSCws49991 | During migration from ASA to Firewall Threat Defense using the Firewall Migration Tool, the tool does not push the tunnel-group configuration. It also fails to map the IP address pool to the group policy in Remote Access (RA) VPN. |
| CSCws83506 | During migration from ASA to Firewall Threat Defense using the Firewall Migration Tool, the tool is unable to identify the Arsenal device as a physical device and displays a parsing error:<br>`?Port Channel migration to Target Platforms ? Virtual FTD is not supported.?` |
| CSCws89585 | During Check Point to Firewall Threat Defense migration using the Firewall Migration Tool, ACL and NAT rules are expanded and appears in an incorrect sequence after migration. |
| CSCws92543 | The migration from ASA to Firewall Threat Defense using the Firewall Migration Tool fails and displays an error message:<br>`Error while pushing interface: Invalid Value for Ether Channel Id, Allowed range: 1 to 8.` |
| CSCws94167 | The configuration exported from PAN through Panorama includes Panorama-specific tags. The Firewall Migration Tool version 10.0 fails to parse the configuration and generates an error message:<br>`"not well-formed (invalid token): line 1, column 0"` |
| CSCws99799 | When migrating the ASA multi-context configuration to Firewall Threat Defense using the merge config option for all contexts, the push to Security Cloud Control in the Australia region fails with an error:<br>`"input payload validation failed"` |
| CSCwt05405 | Migration from ASA to Firewall Threat Defense using Firewall Migration Tool fails with error:<br>`Error while pushing s2s vpn: Non Homogeneous Protected Networks. Endpoints have Protected Networks of different types. Please ensure that all Endpoints are configured with the same Protected Network type.` |

| Bug ID | Description |
|---|---|
| CSCwt05548 | During migration from Check Point to Firewall Threat Defense with the Firewall Migration Tool, object groups are split. This splitting causes the configuration to be migrated incorrectly. |
| CSCwt05576 | During Check Point to Firewall Threat Defense migration using the Firewall Migration Tool, ACL and NAT rules are migrated in incorrect sequence. |
| CSCwt05582 | During migration from PAN to Firewall Threat Defense with the Firewall Migration Tool, objects in the ACL are dropped and excluded from the pre-migration report. |
| CSCwt05586 | During migration from Check Point to Firewall Threat Defense with the Firewall Migration Tool, the pre-migration report does not include the unsupported configuration section. |
| CSCwt05604 | During migration from PAN to Firewall Threat Defense using the Firewall Migration Tool, unsupported configurations are not properly displayed in the pre-migration report. |
| CSCwt05613 | When you migrate from PAN to Firewall Threat Defense by using the Firewall Migration Tool, loopback interfaces are not migrated and are marked unsupported. |
| CSCwt07740 | If you migrate a specific context from PAN to Firewall Threat Defense by using the Security Cloud Control hosted Firewall Migration Tool, and then use the option to migrate another configuration from the same, the application mapping window does not display any information. |
| CSCwt09832 | The pre-migration report generated by the Firewall Migration Tool during PAN to Firewall Threat Defense migration does not capture unsupported objects. |
| CSCwt09854 | This enhancement supports migrating inline IP in PAN to Firewall Threat Defense using the Firewall Migration Tool. |
| CSCwt14220 | During migration from Check Point to Firewall Threat Defense with the Firewall Migration Tool, the tool treats URLs as applications and incorrectly maps URLs as applications. |
| CSCwt22115 | When migrating from PAN to Firewall Threat Defense with the Firewall Migration Tool, the number of port objects increased after parsing. |
| CSCwt23544 | When migrating from PAN to Firewall Threat Defense using the Firewall Migration Tool, need to disable the rule if an unsupported object is replaced with "any." |
| CSCwt28622 | The Firewall Migration Tool fails to parse configurations when migrating from PAN to Firewall Threat Defense. |
| CSCwt28626 | During migration from PAN to Firewall Threat Defense using the Firewall Migration Tool, the application mapping page remains blank and prevents you from continuing. |
| CSCwt30157 | During migration from ASA to Firewall Threat Defense using Firewall Migration Tool, the user interface does not display objects or port names during object optimization. |

| Bug ID | Description |
|---|---|
| CSCwt30199 | Migration from ASA with FirePOWER Services to Firewall Threat Defense using Firewall Migration Tool does not work after optimization. |
| CSCwt31473 | The Firewall Migration Tool fails to parse configurations when migrating from PAN to Firewall Threat Defense. |
| CSCwt34919 | This enhancement adds support for implementing static and dynamic objects from PAN to Firewall Threat Defense by using the Firewall Migration Tool. |
| CSCwt35102 | In the source configuration, if a network object or group is specified as the original source and is translated as 'ANY' or 'NONE', the Firewall Migration Tool does not retain the original source, Instead, it converts it to 'ANY' or 'NONE'. |
| CSCwt39327 | A parsing error occurs during PAN to Firewall Threat Defense migration for MAC build:<br>`Blocked - The config has Panorama tags which are not parsed. Please use the device config export from the source device and proceed with migration.` |
| CSCwt41004 | When migrating from any firewall, such as ASA, Checkpoint, PAN, or Fortinet, to Firewall Threat Defense with multi-instance and port channel mapping, migration fails at the interface mapping stage if the Firewall Migration Tool runs version 10.0 or later |
| CSCwt41051 | The Firewall Migration Tool fails to parse configurations when migrating from Check Point to Firewall Threat Defense. |
| CSCwt41233 | When you migrate multi-context configurations from ASA to Firewall Threat Defense using the Firewall Migration Tool, FQDN objects are ignored even if you do not select the "migrate only reference objects" option on the feature mapping page. |
| CSCwt44072 | The Firewall Migration Tool fails to parse configurations when migrating from ASA to Firewall Threat Defense. |
| CSCwt45023 | During PAN to Firewall Threat Defense migration using the Firewall Migration Tool, tool skips the FQDN object group, as well as inline and static URL groups. It creates extra ACLs with any tag and marks it as unsupported. |
| CSCwt45423 | Migration from ASA to Firewall Threat Defense using Firewall Migration Tool fails during interface mapping. Discrepancies cause the configuration push to fail and displays an error:<br>`"Error while pushing interface: 'type'` |
| CSCwt46550 | Migration from Check Point to Firewall Threat Defense using the Firewall Migration Tool fails during configuration parsing. |
| CSCwt48887 | Migration from Fortinet firewall to Firewall Threat Defense using the Firewall Migration Tool fails during configuration parsing. |

# Open and Resolved Caveats

The open caveats for this release can be accessed 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 don't have one, you can register for an account on Cisco.com. For more information on Bug Search Tool, see Bug Search Tool Help.

Use the Open and Resolved Caveats dynamic query for an up-to-date list of open and resolved caveats in Secure Firewall migration tool.

# Supported Configurations

For information on the supported configurations of the Secure Firewall Migration Tool, refer to the links below:

- Supported Azure Configurations
- Supported ASA Configurations
- Supported ASA with FirePOWER Services Configurations
- Supported Check Point Configurations
- Supported PAN Configurations
- Supported Fortinet Configuration
- Supported FDM-Managed Device Configuration

# Infrastructure and Platform Requirements

The Secure Firewall migration tool requires the following infrastructure and platform:

- Windows 10 64-bit operating system or on a macOS version 10.13 or higher
- Google Chrome as the system default browser

**Tip** We recommend that you use full screen mode on the browser when using the migration tool.

- A single instance of the Secure Firewall migration tool per system
- Management Center and Threat Defense must be version 6.2.3.3 or later

**Note** Remove the previous build before downloading the newer version.

# Related Documentation

For information on the history of Secure Firewall Migration Tool, see:

- History of the ASA Firewall Migration Tool
- History of the ASA with FirePOWER Services Firewall to Threat Defense with the Firewall Migration Tool
- History of the Check Point Firewall Migration Tool
- History of the Palo Alto Networks Firewall Migration Tool
- History of the Fortinet Firewall Migration Tool
- History of the FDM-Managed Device Migration Tool

### Migration Workflow

For information on the migration workflow of the Secure Firewall migration tool, see:

- Export the ASA Configuration File
- Export the ASA with FirePOWER Services Configuration File
- Export the Microsoft Azure Native Firewall Configuration File
- Export the Check Point Configuration Files
- Export the Configuration from Palo Alto Networks Firewall
- Export the Configuration from Fortinet Firewall
- Export the FDM-Managed Device Configuration File

### Migration Reports

The Secure Firewall migration tool provides these reports in HTML format with details of the migration:

- Pre-Migration Report
- Post-Migration Report

### Secure Firewall Migration Tool Capabilities

The Secure Firewall migration tool provides these capabilities:

- 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 name if to security zones and interface groups mapping)
- Auto-creation or reuse of interface objects
- Auto-zone mapping
- User-defined security zone and interface-group creation
- User-defined security zone creation
- Subinterface limit check for the target threat defense device
- Platforms supported:
  - ASA Virtual to Threat Defense Virtual
  - FDM Virtual to Threat Defense Virtual
  - Same hardware migration (X to X device migration)
  - X to Y device migration (Y having higher number of interfaces)
- ACL optimization for source ASA, FDM-managed device, Fortinet, and Checkpoint for ACP rule action.

### Link to Firewall Migration Tool Documents

- Navigating the Cisco Secure Firewall Migration Tool Documentation
- Migrating ASA Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating ASA Firewall with FirePOWER Services to Firewall Threat Defense with the Secure Firewall Migration Tool
- Cisco Secure Firewall ASA to Threat Defense Feature Mapping
- Migrating an FDM-Managed Device to Secure Firewall Threat Defense with the Migration Tool
- Migrating Microsoft Azure Native Firewall to Cisco Secure Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating Check Point Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating Fortinet Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating Cisco Secure Firewall ASA to Cisco Multicloud Defense with the Migration Tool
- Palo Alto Networks to Cisco Secure Firewall Threat Defense Migration Prerequisites Guide
- Migrating Palo Alto Networks Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating Palo Alto Networks Firewall to Cisco Multicloud Defense with the Migration Tool
- Cisco Secure Firewall Migration Tool Compatibility Guide
- Secure Firewall Migration Tool Best Practices Guide