PAN to Multicloud Defense Migration Workflow

End-to-End Procedure
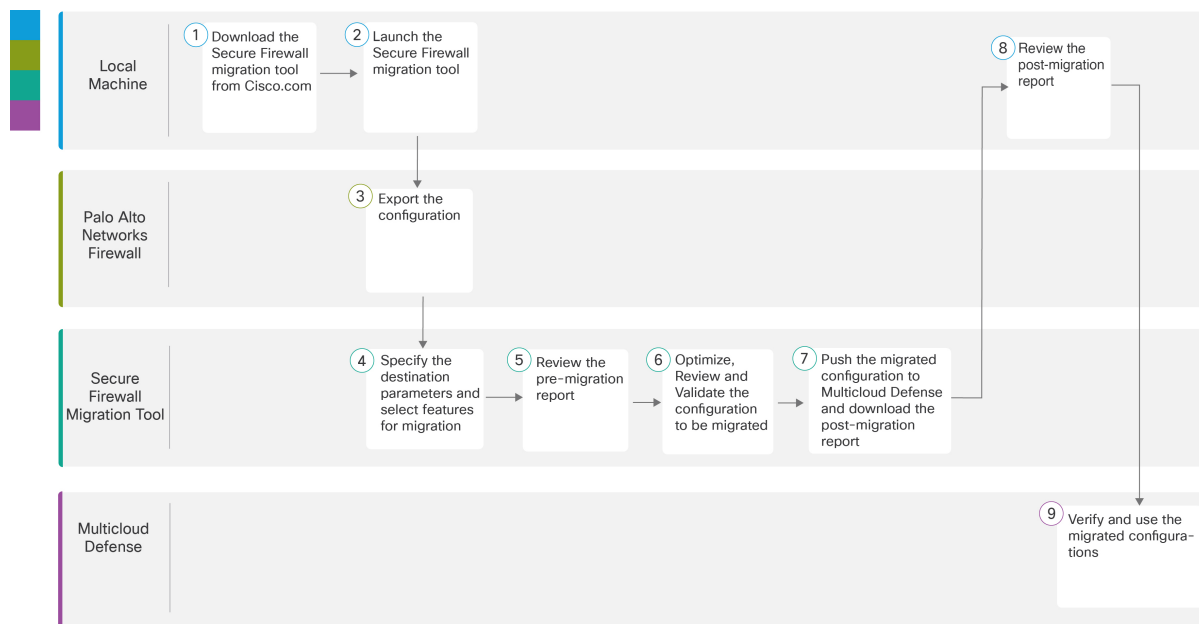
	Workspace	Steps
①	Local machine	Download the latest version of Secure Firewall migration tool from Cisco.com. For detailed steps, see Download the Secure Firewall Migration Tool from Cisco.com.
②	Local Machine	In the local machine, initiate the Secure Firewall Migration tool by double-clicking on the application file that you downloaded from Cisco.com.

	Workspace	Steps
3	Palo Alto Networks Firewall	Export the Configuration File: To export the configuration from Palo Alto Networks Firewall, see Export the Configuration from Palo Alto Networks Firewall, on page 6.
4	Secure Firewall Migration Tool	During this step, you can specify the destination parameters for Multicloud Defense. For detailed steps, see Specify Destination Parameters for Multicloud Defense, on page 7.
5	Secure Firewall migration tool	Navigate to where you downloaded the pre migration report and review the report. For detailed steps, see Review the Pre-Migration Report, on page 9.
6	Secure Firewall Migration Tool	Optimize and review the configuration carefully and validate that it is correct. For detailed steps, see Optimize, Review, and Validate the Configuration to be Migrated, on page 10.
7	Secure Firewall Migration Tool	This step in the migration process sends the migrated configuration to Multicloud Defense and allows you to download the post-migration report. For detailed steps, see Push the Configuration to Multicloud Defense, on page 12.
8	Local Machine	Navigate to where you downloaded the post migration report and review the report. For detailed steps, see Review the Post-Migration Report and Complete the Migration, on page 14.
9	Multicloud Defense	Verify the migrated configurations and use them as required in configuring gateways.

Prerequisites for Migration

Before you migrate your PAN configuration, execute the following activities:

Download the Secure Firewall Migration Tool from Cisco.com

Before you begin

You must have a Windows 10 64-bit or macOS version 10.13 or higher machine with an internet connectivity to Cisco.com.

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

Procedure

Step 1   On your computer, create a folder for the Secure Firewall migration tool.

We recommend that you do not store any other files in this folder. When you launch the Secure Firewall migration tool, it places the logs, resources, and all other files in this folder.

Note

Whenever you download the latest version of the Secure Firewall migration tool, ensure, you create a new folder and not use the existing folder.

Step 2 Browse to https://software.cisco.com/download/home/286306503/type and click **Firewall Migration Tool**.

The above link takes you to the Secure Firewall migration tool under Firewall NGFW Virtual. You can also download the Secure Firewall migration tool from the threat defense device download areas.

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

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

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

Run the Migration

Launch the Secure Firewall Migration Tool

This task is applicable only if you are using the desktop version of the Secure Firewall migration tool. If you are using the cloud version of the migration tool hosted on Security Cloud Control, skip to Export the Configuration from Palo Alto Networks Firewall .

Note When you launch the desktop version of the Secure Firewall migration tool a console opens in a separate window. As you go through the migration, the console displays the progress of the current step in the Secure Firewall migration tool. If you do not see the console on your screen, it is most likely to be behind the Secure Firewall migration tool.

Before you begin

• Download the Secure Firewall Migration Tool from Cisco.com

• Ensure that your computer has a recent version of the Google Chrome browser to run the Secure Firewall migration tool. For information on how to set Google Chrome as your default browser, see Set Chrome as your default web browser.

• If you are planning to migrate a large configuration file, configure sleep settings so the system doesn't go to sleep during a migration push.

Procedure

Step 1 On your computer, navigate to the folder where you downloaded the Secure Firewall migration tool.

Step 2 Do one of the following:

- On your Windows machine, double-click the Secure Firewall migration tool executable to launch it in a Google Chrome browser.

  If prompted, click **Yes** to allow the Secure Firewall migration tool to make changes to your system.

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

  The Secure Firewall migration tool creates and stores all related files in the folder where it resides, including the log and resources folders.

- On your Mac move, the Secure Firewall migration tool `*.command` file to the desired folder, launch the Terminal application, browse to the folder where the Secure Firewall migration tool is installed and run the following commands:

  ```
  # chmod 750 Firewall_Migration_Tool-version_number.command
  ```

  ```
  # ./Firewall_Migration_Tool-version_number.command
  ```

  The Secure Firewall migration tool creates and stores all related files in the folder where it resides, including the log and resources folders.

  Tip
  When you try to open the Secure Firewall migration tool, you get a warning dialog because the Secure Firewall migration tool is not registered with Apple by an identified developer. For information on opening an application from an unidentified developer, see Open an app from an unidentified developer.

  Note
  Use MAC terminal zip method.

Step 3 On the **End User License Agreement** page, click **I agree to share data with Cisco Success Network** if you want to share telemetry information with Cisco, else click **I'll do later**.

When you agree to send statistics to Cisco Success Network, you are prompted to log in using your Cisco.com account. Local credentials are used to log in to the Secure Firewall migration tool if you choose not to send statistics to Cisco Success Network.

Step 4 On the Secure Firewall migration tool's login page, do one of the following:

- To share statistics with Cisco Success Network, click the **Login with CCO** link to log in to your Cisco.com account using your single sign-on credentials. If you do not have a Cisco.com account, create it on the Cisco.com login page.

  Proceed to step 8, if you have used your Cisco.com account to log in.

- If you have deployed your firewall in an air-gapped network that does not have internet access, contact Cisco TAC to receive a build that works with administrator credentials. Note that this build does not send usage statistics to Cisco, and TAC can provide you the credentials.

Step 5 On the **Reset Password** page, enter the old password, your new password, and confirm the new password.

The new password must have 8 characters or more and must include upper and lowercase letters, numbers, and special characters.

Step 6 Click **Reset**.

Step 7   Log in with the new password.

> **Note**
> If you have forgotten the password, delete all the existing data from the *<migration_tool_folder>* and reinstall the Secure Firewall migration tool.

Step 8   Review the premigration checklist and make sure you have completed all the items listed.

If you have not completed one or more of the items in the checklist, do not continue until you have done so.

Step 9   Click **New Migration**.

Step 10   On the **Software Update Check** screen, if you are not sure you are running the most recent version of the Secure Firewall migration tool, click the link to verify the version on Cisco.com.

Step 11   Click **Proceed**.

What to do next

You can proceed to the following step:

- If you must extract information from a PAN firewall using the Secure Firewall migration tool, proceed to Configuration File from Palo Alto Firewall (Not Managed by Panorama).

Using the Demo Mode in the Secure Firewall Migration Tool

When you launch the Secure Firewall Migration tool and are on the **Select Source Configuration** page, you can choose to start performing a migration using **Start Migration** or enter the **Demo Mode**.

The demo mode provides an opportunity to perform a demo migration using dummy devices and visualize how an actual migration flow would look like. The migration tool triggers the demo mode based on the selection you make in the **Source Firewall Vendor** drop-down; you can also upload a configuration file or connect to a live device and continue with the migration. You can proceed performing the demo migration by selecting demo source and target devices such as demo FMC, demo FTD devices, and Multicloud Defense.

⚠️

Caution   Choosing **Demo Mode** erases existing migration workflows, if any. If you use the demo mode while you have an active migration in **Resume Migration**, your active migration is lost and needs to be restarted from first, after you use the demo mode.

You can also download and verify the pre-migration report, map interfaces, map security zones, map interface groups, and perform all other actions like you would in an actual migration workflow. However, you can only perform a demo migration up to validation of the configurations. You cannot push the configurations to the demo target devices you selected because this is only a demo mode. You can verify the validation status and the summary and click **Exit Demo Mode** to go the **Select Source Configuration** page again to start your actual migration.

✎

Note   The demo mode lets you leverage the whole feature set of the Secure Firewall Migration Tool, except pushing of configurations, and do a trial run of the end-to-end migration procedure before performing your actual migration.

Export the Configuration from Palo Alto Networks Firewall

You can export the configuration file in the following ways:

Configuration File from Palo Alto Firewall (Not Managed by Panorama)

Follow these steps to extract the configuration from the gateway:

Procedure

Step 1 Navigate to **Device** > **Setup** > **Operations**, and select **Save Named Configuration** *<file_name.xml>*.

Step 2 Click **Ok**.

Step 3 Navigate to **Device** > **Setup** > **Operations**, and click **Export Named Configuration**.

Step 4 Select the *<file_name.xml>* file.

Step 5 Click **Ok**.

Step 6 Select the XML file that contains your running configuration *<file_name.xml>*, and click **Ok** to export the configuration file.

Step 7 Save the exported file to a location, external to the firewall. You can use this backup to upload to the Secure Firewall migration tool to migrate the configuration.

Step 8 (Optional) If you have a NAT policy where the destination NAT has the same source and destination zones, perform these steps:

a) Run the **show routing route** command from CLI on the firewall.

b) Copy the routing table to a *.txt* file.

c) Add the *.txt* file to the folder where you will zip the .txt and the .xml files with the *panconfig.xml*.

These steps are not mandatory for migration. If you do not perform these steps, the destination zones will not be mapped during the Secure Firewall migration tool migration and will be included in the Migration Reports.

Note

Use the **show routing route** command to extract the routing table details. Paste the extracted output in a notepad.

Configuration File from Palo Alto Firewall (Managed by Panorama)

The configuration must be extracted from the gateway if your device is managed by panorama. Merge the panorama configuration with the gateway and extract the configuration.

In the Secure Firewall migration tool user interface, do the following:

Before you begin

Log in to the Palo Alto Firewall web UI using super-user account.

Procedure

Step 1 Navigate to **Device** > **Support** > **Tech Support File**.

Step 2   Click **Generate Tech Support File**.

Step 3   Click **Download Tech Support File** once the generated file is available.

Step 4   Unzip and Untar the file and then navigate to the path *\opt\pancfg\mgmt\saved-configs* to retreive the *merged-running-config.xml* file.

What to do next

Zip the Exported Files

Zip the Exported Files

Export the *panconfig.xml* for the Palo Alto Gateway firewall and *route.txt* (if you have the NAT rules with the same source zone and destination zone).

Specify Destination Parameters for Multicloud Defense

Before you begin

If you are using the Security Cloud Control-hosted migration tool:

- ensure that you have a Security Cloud Control tenant with Multicloud Defense enabled on it.

- ensure that you have purchased the required operating licenses for Multicloud Defense.

Note   You can migrate configurations to Multicloud Defense even during the 90-day free trial because the trial experience offers full functionality of a paid subscription.

If you are using the desktop version of the migration tool:

- ensure that you have obtained the base URL of Multicloud Defense and the Security Cloud Control tenant name.

- ensure that you have created an API key and also copied the **API Key ID** and **API Key Secret** that Multicloud Defense generates when you create the API key. See Create an API Key in Multicloud Defense for more information.

Procedure

Step 1   On the **Select Target** window, choose **Multicloud Defense**.

Step 2   Specify the following parameters in the correponding fields to enable the connection between the migration tool and Multicloud Defense:

- **Enter Base URL**: This is the base URL that you see on your browser when you connect to your Multicloud Defense controller. For example, when you are in the controller dashboard, copy the link on your browser, excluding the **/dashboard** part. The URL looks like https://xxxx.mcd.apj.cdo.cisco.com

- **Enter Tenant Name**: The name of your Security Cloud Control tenant. Copy it from the profile drop-down on the top-right corner when you are in the Multicloud Defense window or from **Administration** > **General Settings** if you are in the Security Cloud Control window.

- **Enter API Key ID**: The **API Key ID** that Multicloud Defense controller generates when you create an API key by navigating to **System and Accounts** > **API Keys**. Specify a name for the key, your email address, the role you want the API key to have, and the API key lifetime to generate a key. The default key lifetime is set to 365 days.

- **Enter API Key Secret**: The **API Key Secret** that Multicloud Defense controller generates when you create an API key.

  Note

  Ensure you copy both the **API Key ID** and **API Key Secret** when they are displayed only at the time of creating the API key. If you missed to copy them, delete the API key that you created, generate a new one, and make sure you copy them this time.
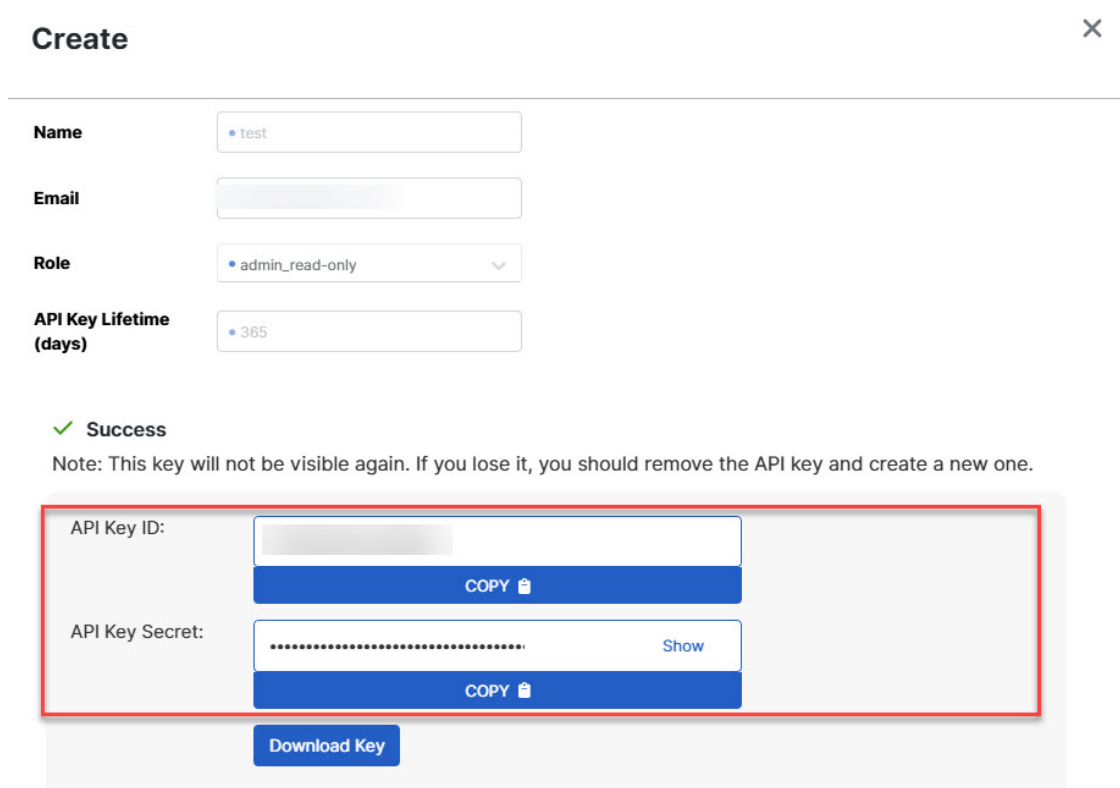
Step 3   Click **Connect** and wait to receive the **Successfully gathered** message, which confirms that the connection attempt to Multicloud Defense is a success.

Step 4   The **Select Features** lets you select the configurations that you want to migrate to Multicloud Defense. **Access Control** and **Migrate Only Reference Objects** checkboxes are checked by default.

Note that other configurations from the source firewall such as interfaces and routes are not supported for this migration.

Step 5 Click **Proceed** and **Start Conversion**. Wait for the migration tool to parse the source configurations.

Step 6 Review the summary of the elements that the Secure Firewall migration tool converted.

To check whether your configuration file is successfully uploaded and parsed, download and verify the **Pre-Migration Report** before you continue with the migration.

Step 7 Click **Download Report** and save the **Pre-Migration Report**.

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

Step 8 Click **Next**.

Review the Pre-Migration Report

If you have missed to download the Pre-Migration Reports during migration, use the following link to download:

Pre-Migration Report Download Endpoint—http://localhost:8888/api/downloads/pre_migration_summary_html_format

Note You can download the reports only when the Secure Firewall migration tool is running.

Procedure

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

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

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

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

- A summary of the supported configuration elements that can be successfully migrated to threat defense or Multicloud Defense and specific features selected for migration.

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

- **Partially Supported Configuration**—Details of configuration elements that can be only partially migrated. These configuration elements include rules and objects with advanced options where the rule or the object can be migrated without the advanced options. Review these lines, verify whether the

advanced options are supported in , and if so, plan to configure those options manually after you complete the migration with the Secure Firewall migration tool.

- **Unsupported Configuration**—Details of configuration elements that cannot be migrated because the Secure Firewall migration tool does not support migration of those features. Review these lines, verify whether each feature is supported in , and if so, plan to configure the features manually after you complete the migration with the Secure Firewall migration tool.

- **Ignored Configuration**—Details of configuration elements that are ignored because they are not supported by the Multicloud Defense or the Secure Firewall migration tool. The Secure Firewall migration tool does not parse these lines. Review these lines, verify whether each feature is supported in Multicloud Defense, and if so, plan to configure the features manually.

Step 3 If the **Pre-Migration Report** recommends corrective actions, complete those corrections on the interface, export the configuration file again and upload the updated configuration file before proceeding.

Step 4 After your configuration file is successfully uploaded and parsed, return to the Secure Firewall migration tool, and click **Next** to continue the migration.

Optimize, Review, and Validate the Configuration to be Migrated

Before you begin

The **Optimize, Review and Validate Configuration** page lets you review and validate the configuration parameters that you are about to migrate to the target Multicloud Defense. In this step, the migration tool validates the configurations against the existing configuration on Multicloud Defense and suggests changes that need to be performed for the migration to be successful, such as associating access control rules and renaming objects to avoid duplicates on the target Multicloud Defense.

After you validate, a flashing tab indicates that there is action you need to perform on the tab.

Procedure

Step 1 On the **Access Control** tab that lists all your access control list (ACL) entries, you can do the following:

- Click **Optimize ACL** to let the migration tool identify all the shadow and redundant ACLs and choose whether to migrate them as disabled ACLs or to exclude them from being migrated.

  Secure Firewall Migration Tool ACL Optimization Overview

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

  The ACL optimization supports the following ACL types:

  - Redundant ACL—When two ACLs have the same set of configurations and rules, then removing the non-base ACL will not impact the network. For example, if any two rule allows FTP and IP traffic on the same network with no rules that are defined for denying access, the first rule can be deleted.

  - Shadow ACL—The first ACL completely shadows the configurations of the second ACL. If two rules have similar traffic, the second rule is not applied to any traffic as it appears later in the access

list. If the two rules specify different actions for traffic, you can either move the shadowed rule or edit any one of the rules to implement the required policy. For example, the base rule may deny the IP traffic, and the shadowed rule may allow FTP traffic for a given source or destination.

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

- The disabled ACLs are not considered during the optimization process.

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

  - Source and Destination Network

  - Source and Destination Port

Click **Download Report** to review the ACL name and the correponding redundant and shadowed ACLs tabulated in an Excel file. Use the **Detailed ACL Information** sheet to view more ACL information.

Click **Proceed** to start the optimization process.

- For each entry in the table, review the mappings and verify that they are correct.

A migrated Access Policy Rule uses the ACL name as prefix and appends the ACL rule number to it to make it easier to map back to the configuration file. For example, if an ACL is named "inside_access," then the first rule (or ACE) line in the ACL will be named as "inside_access_#1." If a rule must be expanded because of TCP or UDP combinations, an extended service object, or some other reason, the Secure Firewall migration tool adds a numbered suffix to the name. For example, if the allow rule is expanded into two rules for migration, they are named "inside_access _#1-1" and " inside_access_#1-2".

For any rule that includes an unsupported object, the Secure Firewall migration tool appends an "_UNSUPPORTED" suffix to the name.

- If you do not want to migrate or want to migrate a few ACLs as disabled, check the checkboxes against the row, click **Actions**, and choose the relevant option. Check the **Select all entries** checkbox to perform bulk changes.

Step 2 On the **Objects** tab, you can do the following:

Choose the following tabs and review the mappings:

- Network Objects

- Port Objects

- FQDN Objects

- URL Objects

If you want to rename an object, check the checkbox against the object row, click **Actions**, and choose **Rename**. Check the **Select all entries** checkbox to perform bulk changes.

Step 3 After you have completed your review, click **Validate**. Note that the mandatory fields that need your attention keeps flickering until you enter values in them. The **Validate** button gets enabled only after all the mandatory fields are filled.

During validation, the Secure Firewall migration tool connects to Multicloud Defense, reviews the existing objects, and compares those objects to the list of objects to be migrated. If an object already exists in Multicloud Defense, the Secure Firewall migration tool does the following:

- If the object has the same name and configuration, the Secure Firewall migration tool reuses the existing object and does not create a new object in Multicloud Defense.

- If the object has the same name but a different configuration, the Secure Firewall migration tool reports an object conflict.

You can view the validation progress in the console.

Step 4 When the validation is complete, if the **Validation Status** dialog box shows one or more object conflicts, do the following:

a) Click **Resolve Conflicts**.

The Secure Firewall migration tool displays a warning icon on either or both of the **Network Objects** or **Port Objects** tab, depending upon where the object conflicts were reported.

b) Click the tab and review the objects.
c) Check the entry for each object that has a conflict and choose **Actions** > **Resolve Conflicts**.
d) In the **Resolve Conflicts** window, complete the recommended action.

For example, you might be prompted to add a suffix to the object name to avoid a conflict with the existing Multicloud Defense object. You can accept the default suffix or replace it with one of your own.

e) Click **Resolve**.
f) When you have resolved all object conflicts on a tab, click **Save**.
g) Click **Validate** to revalidate the configuration and confirm that you have resolved all object conflicts.

Step 5 When the validation is complete and the **Validation Status** dialog box displays the message **Successfully Validated**, continue with pushing the configuration to Multicloud Defense.

Push the Configuration to Multicloud Defense

Before you begin

You cannot push the configuration to Multicloud Defense if you have not successfully validated the configuration and resolved all object conflicts.

Note Do not make any configuration changes or deploy to any device while the Secure Firewall migration tool is sending the configuration to Multicloud Defense.

Procedure

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

Step 2 Click **Push Configuration** to send the source firewall configuration to Multicloud Defense.

The Secure Firewall migration tool displays a summary of the progress of the migration. You can view detailed, line-by-line progress of which the components that are being pushed to Multicloud Defense in the console.

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

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

Step 3   After the migration is complete, click **Download Report** to download and save the post-migration report.

A copy of the **Post-Migration Report** is also saved in the `Resources` folder in the same location as the Secure Firewall migration tool.

Step 4   If your migration failed, review the post-migration report, log file, and unparsed the configuration file carefully to understand what caused the failure.

You can also contact the support team for troubleshooting.

Migration Failure Support

If the migration is unsuccessful, contact Support.

a.   On the **Complete Migration** screen, click the **Support** button.

The **Help** support page appears.

b.   Check the **Support Bundle** check box and then select the configuration files to download.

Note
The Log and dB files are selected for download by default.

c.   Click **Download**.

The support bundle file is downloaded as a .zip to your local path. Extract the zip folder to view the log files, DB, and the configuration files.

d.   Click **Email us** to email the failure details for the technical team.

You can also attach the downloaded support files to your email.

e.   Click **Visit TAC page** to create a TAC case in the Cisco support page.

Note
You can open a TAC case at any time during the migration from the support page.

Review the Post-Migration Report and Complete the Migration

Before you begin

The post-migration report provides details on ACL count under various categories, ACL optimization, and the overall view of optimization performed on the configuration file.

Procedure

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

Step 2 Open the post-migration report and carefully review its contents to understand how your source configuration was migrated.

    a. **Migration Summary**—A summary of the configuration that was successfully migrated from your source firewall to Multicloud Defense.

    b. **Object Conflict Handling**—Details of the objects that were identified as having conflicts with existing objects in Multicloud Defense. If the objects have the same name and configuration, the Secure Firewall migration tool reused the Multicloud Defense object. If the objects have the same name but a different configuration, you renamed those objects. Review these objects carefully and verify that the conflicts were appropriately resolved.

    c. **Access Control Rules That You Chose Not to Migrate**—Details of the rules that you choose not to migrate with the Secure Firewall migration tool. Review these rules that were disabled by the Secure Firewall migration tool and were not migrated. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.

    d. **Partially Migrated Configuration**—Details of the rules that were only partially migrated, including rules with advanced options where the rule could be migrated without the advanced options. Review these lines, verify whether the advanced options are supported in Multicloud Defense, and if so, configure these options manually.

    e. **Unsupported Configuration**—Details of the source firewall configuration elements that were not migrated because the Secure Firewall migration tool does not support migration of those features. Review these lines, verify whether each feature is supported in Multicloud Defense. If so, configure those features manually in Multicloud Defense.

    f. **Expanded Access Control Policy Rules**—Details of the source firewall access control policy rules that were expanded from a single point rule into multiple Multicloud Defense rules during migration.

    g. **Actions Taken on Access Control Rules**

        • **Access Rules You Chose Not to Migrate**—Details of the access control rules that you choose not to migrate with the Secure Firewall migration tool. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually in Multicloud Defense.

        • **Access Rules with Rule Action Change**—Details of all Access Control Policy Rules that had 'Rule Action' changed using the Secure Firewall migration tool. The Rule Action values are - Allow, Trust, Monitor, Block, Block with reset. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually in Multicloud Defense.

Note

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

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

Step 4   Verify and ensure that all the migrated configuration parameters are available on Multicloud Defense.