

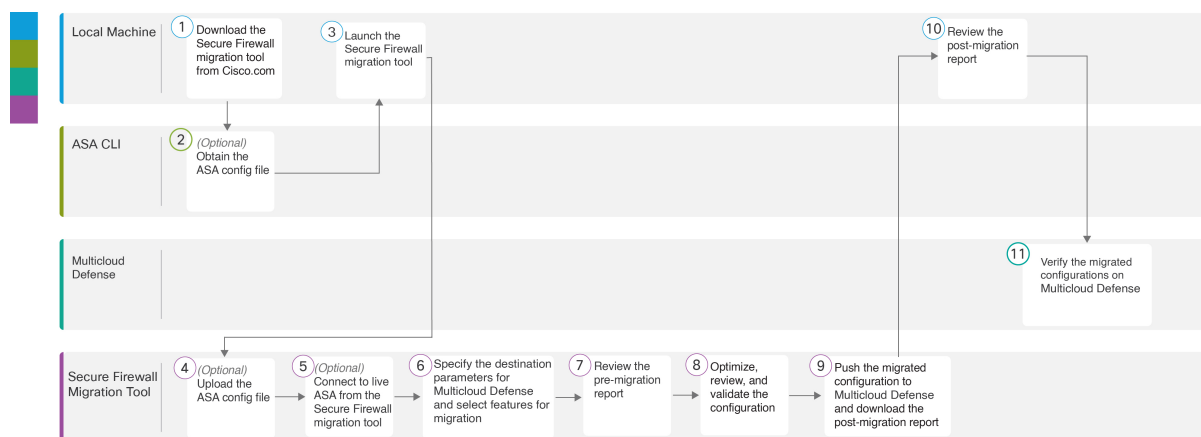


ASA to Multicloud Defense Migration Workflow

- [End-to-End Procedure, on page 1](#)
- [Prerequisites for Migration, on page 2](#)
- [Run the Migration, on page 4](#)

End-to-End Procedure

The following flowchart illustrates the workflow for migrating a Secure Firewall ASA to Multicloud Defense using the Secure Firewall migration tool.



	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	Secure Firewall ASA CLI	Obtain the ASA configuration file: To obtain the ASA config file from ASA CLI, see Obtain the ASA configuration file . If you want to connect to the ASA from the migration tool, skip to step 3.
3	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
4	Secure Firewall migration tool	Upload the ASA config file obtained from ASA CLI, see Upload the ASA Configuration File, on page 6 . If you are planning to connect to live ASA, skip to step 6.
5	Secure Firewall migration tool	You can connect to live ASA directly from the Secure Firewall migration tool. For more information, see Connect to the ASA from the Secure Firewall Migration Tool, on page 7 .
6	Secure Firewall migration tool	Specify the destination parameters for Multicloud Defense. For detailed steps, see Specify Destination Parameters for Multicloud Defense, on page 9 .
7	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 11 .
8	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 12 .
9	Secure Firewall migration tool	Push the configuration to Multicloud Defense.
10	Local machine	Download the postmigration report for verifying how the migration went. For detailed steps, see Review the Post-Migration Report and Complete the Migration, on page 17 .
11	Multicloud Defense	Verify the migrated configurations on Multicloud Defense and use them as required in configuring your gateways.

Prerequisites for Migration

Before you migrate your ASA 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.
-

Obtain the ASA Configuration File

You can use one of the following methods to obtain an ASA configuration file:

- [Export the ASA Configuration File, on page 3](#)
- [Connect to the ASA from the Secure Firewall Migration Tool, on page 7](#)

Export the ASA Configuration File

This task is required only if you want to manually upload an ASA configuration file. If you want to connect to an ASA from the Secure Firewall migration tool, skip to [Connect to the ASA from the Secure Firewall Migration Tool, on page 7](#).

**Note**

Do not hand code or make changes to the ASA configuration after you export the file. These changes will not be migrated, and they create errors in the migration or cause the migration to fail. For example, opening and saving the configuration file in terminal can add white space or blank lines that the Secure Firewall migration tool cannot parse.

Ensure that the exported ASA configuration file does not contain the **--More--** keyword as text, because this can cause the migration to fail.

Procedure

- Step 1** Use the **show running-config** command for the ASA device or context that you are migrating and copy the configuration from there. See [View the Running Configuration](#).

Alternately, use Adaptive Security Device Manager (ASDM) for the ASA device or context that you want to migrate and choose **File > Show Running Configuration in New Window** to obtain the configuration file.

- Step 2** Save the configuration as either `.cfg` or `.txt`.
You cannot upload the ASA configuration to the Secure Firewall migration tool if it has a different extension.
- Step 3** Transfer the ASA configuration file to your computer where you downloaded the Secure Firewall migration tool.
-

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 [Upload the ASA Configuration File, on page 6](#).



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 popups 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, verify the version on Cisco.com.

Step 11 Click **Proceed**.

What to do next

You can proceed to the following step:

- If you have exported ASA configuration to your computer, proceed to [Upload the ASA Configuration File](#).

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, or 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, 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.

Upload the ASA Configuration File

Before you begin

Export the configuration file as `.cfg` or `.txt` from the source device.



Note Do not upload a hand-coded or manually altered configuration file. Text editors add blank lines and other issues to the file that can cause the migration to fail.

Procedure

-
- Step 1** On the **Extract Information** page, in the **Manual Upload** section, click **Upload** to upload configuration file.
- Step 2** Browse to where the ASA configuration file is located and click **Open**.
- The Secure Firewall migration tool uploads the configuration file. For large configuration files, this step takes a longer time. The console provides a line by line log view of the progress, including the configuration line that is being parsed. If you do not see the console, you can find it in a separate window behind the Secure Firewall migration tool.
- Step 3** Click **Start Parsing**.
- The **Parsed Summary** section displays the parsing status.
- Step 4** Review the summary of the elements in the uploaded configuration file that the Secure Firewall migration tool detected and parsed.
- Step 5** Click **Next** to select the target parameters.
-

Connect to the ASA from the Secure Firewall Migration Tool

The Secure Firewall migration tool can connect to an ASA device that you want to migrate and extract the required configuration information.

Before you begin

- Download and launch the Secure Firewall migration tool.



Note If ASA is not configured with **Enable Password**, you can leave the field blank on the Secure Firewall migration tool.

Procedure

-
- Step 1** On the **Extract ASA Information** screen, in the **Connect to ASA** section, click **Connect** to connect to the ASA device that you want to migrate.
- Step 2** On the **ASA Login** screen, enter the following information:
- In the **ASA IP Address/Hostname** field, enter the management IP address or hostname (for single context ASA) or IP address of the admin context or hostname (for a multi-context ASA).

- b. In the **Username**, **Password**, and **Enable Password** fields enter the appropriate administrator login credentials.

Note

If ASA is not configured with an **Enable password**, you can leave the field blank on the Secure Firewall migration tool.

- c. Click **Login**.

When the Secure Firewall migration tool connects to the ASA, it displays a successfully connected to the ASA message.

Step 3 Select the ASA context that you want to migrate from the **Context** drop-down list.

Step 4 (Optional) Select **Collect Hitcounts**.

When checked, this tool computes the number of times an ASA rule was used and the last time the rule was used since ASA uptime or last ASA restart and displays this information on the **Review and Validate** page. This allows you to evaluate the efficacy and relevance of the rule before migration.

Step 5 Click **Start Extraction**.

The Secure Firewall migration tool connects to the ASA and starts extracting configuration information. When the extraction completes successfully, the **Context Selection** section identifies if the uploaded configuration corresponds to a single-context or multi-context ASA.

Connect to a Secure Firewall ASA Managed by Security Cloud Control and Extract Configuration

Before you begin

This procedure is applicable to migrations done using the migration tool hosted on Security Cloud Control.

The migration tool fetches the devices that are currently managed by Security Cloud Control and lets you choose the one from which you want to migrate configurations.



Note Ensure that the Secure Firewall ASA device is online and in synced state, for the migration tool to detect it.

Procedure

Step 1 In the **Extract Cisco ASA (8.4+) Information** page, the migration tool displays the Secure Firewall ASA devices that are managed by Security Cloud Control.

Step 2 From the **Select ASA Device** drop-down, choose the device whose configuration you want to migrate.

Step 3 Click **Connect**.

Step 4 (Optional) Check the **Collect Hitcounts** checkbox.

When checked, this tool computes the number of times a rule was used and the last time the rule was used since the device's uptime or last device restart, and displays this information on the **Optimize, Review, and Validate Configuration** page. This allows you to evaluate the efficacy and relevance of the rule before migration.

Step 5 Click **Start Extraction**.

Specify Destination Parameters for Multicloud Defense

Before you begin

- 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.

- 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 corresponding 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.

Create



Name

Email

Role

API Key Lifetime (days)

✓ **Success**

Note: This key will not be visible again. If you lose it, you should remove the API key and create a new one.

API Key ID:

API Key Secret: [Show](#)

[Download Key](#)

- 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:

- **Overall Summary**—The method used to extract the ASA configuration information or connecting to a live ASA configuration.

A summary of the supported ASA 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 ASA 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.
- **Object and Object Groups Conflict Resolution**—Details of ASA network and service objects and object, service, and protocol object groups that have conflicts across the contexts you are trying to migrate. To view detailed information about these object conflicts, click the **Link for Conflict Count**; you can check the reason for the conflicts and also know how the migration tool is handling the conflicts.
- **Ignored Configuration**—Details of ASA 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 ASA interface, export the configuration file again and upload the updated configuration file before proceeding.

Step 4 After your ASA 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 corresponding redundant and shadowed ACLs tabulated in an Excel file. Use the **Detailed ACL Information** sheet to view more ACL information. For more information on the ACL optimization report, see [Reporting for ACL Optimization, on page 15](#).

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.
- To edit an access control list policy, select the row by checking the check box for the policy, and choose **Actions > Edit**.

All rules that are not applicable are grayed out in the table.



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

Choose the following tabs and review the mappings:

- Network Objects
- Port Objects
- Security Group Tag 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 (Optional) On the **Network Objects** and the **Port Objects** tabs, review all the network objects, network groups, port objects, port groups, and their values. To rename an object or object group, select the object and choose **Actions > Rename**.

- Click **Optimize Objects and Groups** to optimize your list of objects before migrating them. The migration tool identifies objects and groups that have the same value and prompts you to choose which to retain.
- Click  to move objects from **Conflict Detected** column to **Objects/Groups Retained** column and click  to move them back. Note that the ones that are referenced in most configurations are displayed in bolded text.
- Click **Auto Select** to automatically select all the objects and groups with most number of references. However, you can still manually override the autoselection and move objects between columns because manual selection takes higher priority.

- Click **Optimize**. The migration tool performs the optimization and displays an optimization summary with optimization data including retained and duplicate objects. For a detailed version of the optimization report, refer to the postmigration report.
- Click **Proceed** and **Validate**.

Note

The objects and groups which are not chosen to be retained are not migrated and are replaced with the retained objects in the configurations they were used, such as in ACL configurations. This ensures the list of objects being migrated is fully optimized and there are no duplicate objects migrated.

- Step 4** On the **Security Group Tag Objects** tab, review all the values. To rename an object or object group, select the object and choose **Actions > Rename**.

SGT object tag value must range from 0 to 65535.

SGT objects support multi-context configuration.

Note

To migrate the SGT objects configuration, ensure that the management center and threat defense version are 7.0 or later.

- Step 5** 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 6** 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 7** When the validation is complete and the **Validation Status** dialog box displays the message **Successfully Validated**, continue with pushing the configuration to Multicloud Defense.

Reporting for ACL Optimization

The ACL optimization report displays the following information:

- Summary Sheet—Displays the summary of the ACL optimization.

	A	B	C	D
1	Sl.no	ACL name	Redundant ACLs	Shadowed ACLs
2	1	outsideACL_#1		outsideACL_#2, outsideACL_#3, outsideACL_#4, outsideACL_#5,
3	2	outsideACL_#13		outsideACL_#6, outsideACL_#7, outsideACL_#8, outsideACL_#9,
4	3	outsideACL_#14		outsideACL_#10, outsideACL_#11, outsideACL_#12
5	4	outsideACL_#19		outsideACL_#17, outsideACL_#18
6	5	outsideACL_#25		outsideACL_#15, outsideACL_#16, outsideACL_#17, outsideACL_#18
7	6	outsideACL_#26		outsideACL_#20, outsideACL_#21, outsideACL_#22,
8	7	outsideACL_#31		outsideACL_#23, outsideACL_#24
9	8	outsideACL_#34		outsideACL_#27, outsideACL_#28, outsideACL_#29, outsideACL_#30
10	9	dmzACL_#1		outsideACL_#32, outsideACL_#33
11	10	dmzACL_#2	dmzACL_#5	
12	11	dmzACL_#3		dmzACL_#5
13	12	dmzACL_#4		
14	13	dmzACL_#6		dmzACL_#7, dmzACL_#8, dmzACL_#9, dmzACL_#10
15	14	dmzACL_#11		dmzACL_#13
16	15	dmzACL_#12		
17	16	extACL_#1		
18	17	extACL_#2		
19	18	extACL_#3		extACL_#4, extACL_#5, extACL_#6
20	19	extACL_#7		
21	20	extACL_#8	extACL_#9, extACL_#10	
22	21	extACL_#11		
23	22	extACL_#12	extACL_#13	
24	23	extACL_#14		
25	24	extACL_#15		
26	25	extACL_#16		
27	26	extACL_#17		extACL_#18, extACL_#19
28	27	localtoremove_#1		
29	28	opt_#1		opt_#3
30	29	opt_#2	opt_#4	opt_#5
31	30	opt_#6-1	opt_#17-1	opt_#7-1, opt_#8-1
32	31	opt_#9-1	opt_#10-1	
33	32	opt_#11-1	opt_#12-1	opt_#13-1
34	33	opt_#14-1		opt_#15-1, opt_#16-1
35	34	opt_#18		
36	35	opt_#19		opt_#20, opt_#21
37	36	opt_#22-1	opt_#23-1	

- Detailed ACL Information—Displays the details of base ACL. Each ACL comes with a ACL type (Shadow or Redundant) tag to identify the base ACL for comparison and its association with the optimization category.

Push the Configuration to Multicloud Defense

1	Sl.no	ACL name	Source zone	Destination zone	Source network	Destination network	Source port	Destination port	Action	ACL type
2	1	outsideACL_#1	outside	ANY	any	10.0.0.0/8	ANY	ANY	permit	
3		outsideACL_#2	outside	ANY	any	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
4		outsideACL_#3	outside	ANY	192.168.0.1	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
5		outsideACL_#4	outside	ANY	192.168.0.10	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
6		outsideACL_#5	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
7		outsideACL_#6	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
8		outsideACL_#7	outside	ANY	any	10.1.1.0/24	ANY	tcp:80	permit	Shadowed by outsideACL_#1
9		outsideACL_#8	outside	ANY	any	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
10		outsideACL_#9	outside	ANY	200.200.200.1	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
11		outsideACL_#10	outside	ANY	10.10.10.10, 10.10.0.0/16	10.10.0.0/19, 10.99.99.99, 10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
12		outsideACL_#11	outside	ANY	any	10.10.10.10, 10.10.0.0/16, 10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.10.0.0/16, 10.10.0.0/19	ANY	ANY	permit	Shadowed by outsideACL_#1
13		outsideACL_#12	outside	ANY	any	192.168.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
14	2	outsideACL_#13	outside	ANY	any	192.168.0.0/16	ANY	ANY	permit	
15		outsideACL_#17	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:443	permit	Shadowed by outsideACL_#13
16		outsideACL_#18	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:80	permit	Shadowed by outsideACL_#13

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.

You can also view a comparison chart that illustrates the difference between the count of pre-migration and post-migration states.

- 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.
