

Import/Export

The following topics explain how to use the Import/Export feature:

- Import/Export feature overview, on page 1
- Requirements and prerequisites for import/export, on page 3
- Guidelines for Import/Export, on page 4
- Export configurations, on page 5
- Import configurations, on page 5

Import/Export feature overview

You can use the Import/Export feature to copy configurations between Firewall Management Centers. Import/Export is not a backup tool but can simplify the process of adding a new Firewall Management Center.

Configuration export and import capabilities

You can export a single configuration, or you can export a set of configurations (of the same type or of different types) with a single action. When you later import the package onto another Firewall Management Center, you can choose which configurations in the package to import.

An exported package contains revision information for that configuration, which determines whether you can import that configuration onto another Firewall Management Center. When the Firewall Management Center are compatible, but the package includes a duplicate configuration, the Firewall Management Center offers resolution options.

Exceptions to export behavior

When you export a configuration, the Firewall Management Center also exports other required configurations. For example, exporting an access control policy also exports any subpolicies it invokes, objects and object groups it uses, ancestor policies, and so on. As another example, if you export a platform settings policy with external authentication enabled, the authentication object is exported as well.

There are some exceptions, however:

- System-provided databases and feeds—The Firewall Management Center does not export URL filtering category and reputation data, Cisco Intelligence Feed data, or the geolocation database (GeoDB). Each Firewall Management Center needs to obtain up-to-date information from Cisco.

- Global Security Intelligence lists—The Firewall Management Center exports Global Security Intelligence Block and Do Not Block lists associated with exported configurations. The import process converts these lists to user-created lists, then uses those new lists in the imported configurations. This ensures that imported lists do not conflict with existing Global Block and Do Not Block lists. To use Global lists on the importing Firewall Management Center, manually add the lists to your imported configurations.
- Intrusion policy shared layers—The export process breaks intrusion policy shared layers. The previously shared layer is included in the package, and imported intrusion policies do not contain shared layers.
- Intrusion policy default variable set—The export package includes a default variable set with custom variables and system-provided variables with user-defined values. The import process updates the default variable set on the importing Firewall Management Center with the imported values. However, the import process does **not** delete custom variables not present in the export package. The import process also does not revert user-defined values on the importing Firewall Management Center, for values not set in the export package. Therefore, an imported intrusion policy may behave differently than expected if the importing Firewall Management Center has differently configured default variables.
- Custom user objects—If you have created custom user groups or objects in your Firewall Management Center, and if such a custom user object is a part of any rule in your access control policy, note that the export file (.sfo) does not carry the user object information (including user realms) , and therefore while importing such a policy, any reference to such custom user objects will be removed and will not be imported to the destination Firewall Management Center. To avoid detection issues due to the missing user group, add the customized user objects manually to the new Firewall Management Center, and re-configure the access control policy after import.

Import objects and object groups

When you import objects and object groups:

- Generally, the import process imports objects and groups as new, and you cannot replace existing objects and groups. However, if network and port objects or groups in an imported configuration match existing objects or groups, the imported configuration reuses the existing objects/groups, rather than creating new objects/groups. The Firewall Management Center determines a match by comparing the name (minus any autogenerated number) and content of each network and port object/group.
- If the names of imported objects match existing objects on the importing Firewall Management Center, the Firewall Management Center appends autogenerated numbers to the imported object and group names to make them unique.
- You must map any security zones and interface groups used in the imported configurations to matching-type zones and groups managed by the importing Firewall Management Center.
- If you export a configuration that uses PKI objects containing private keys, the Firewall Management Center decrypts the private keys before export. On import, the Firewall Management Center encrypts the keys with a randomly generated key.

Conflict resolution for duplicate configurations

When you attempt to import a configuration, the Firewall Management Center determines whether a configuration of the same name and type already exists. When an import includes a duplicate configuration, the Firewall Management Center offers resolution options:

Default resolution behavior

- **Keep existing**

  The Firewall Management Center does not import that configuration.

- **Replace existing**

  The Firewall Management Center overwrites the current configuration with the configuration selected for import. This option is not available if the duplicate is in ancestor or descendant domain.

- **Keep newest**

  The Firewall Management Center imports the selected configuration only if its timestamp is more recent than the timestamp on the current configuration. This option is not available if the duplicate is in ancestor or descendant domain.

- **Import as new**

  The Firewall Management Center imports the selected duplicate configuration, appending a system-generated number to the name to make it unique. (You can change this name before completing the import process.) The original configuration remains unchanged.



Note If you modify an imported configuration on the Firewall Management Center and later re-import that configuration to the same Firewall Management Center, you must choose which version of the configuration to keep.

File list resolution behavior

When you import an access control policy with a file policy that uses clean or custom detection file lists, and a file list presents a duplicate name conflict, the Firewall Management Center offers conflict resolution options as described, but the action taken varies as described in the table:

Resolution Option	Resolution Behavior for the Access Control Policy
Keep existing	Unchanged
Replace existing	Imported as new; file lists are merged
Import as new	Imported as new; file lists are merged
Keep newest and access control policy being imported is the newest	Imported as new; file lists are merged
Keep newest and existing access control policy is the newest	Unchanged

Requirements and prerequisites for import/export

Version requirements

Both Firewall Management Centers must meet version compatibility requirements before you configure import/export.

- Both Firewall Management Centers need to be the same software version.
- For access control and subpolicies (including intrusion policies), ensure the intrusion rule update version matches.

  You cannot use the Import/Export feature to update intrusion rules; you must download and apply the latest rule update version.

Domain requirements

Both Firewall Management Centers must have the same domain hierarchy.



Note If you import a configuration without the same domains, to recover you must first rename the domains and re-export the configuration. Then you can add those new domains to the target Firewall Management Center and import the new configuration.

User roles

- Admin

Guidelines for Import/Export

Supported configurations

You can import and export the following configurations:

- Access control policies and the policies they invoke: prefilter, network analysis, intrusion, SSL, file, Service Policy.
- When exporting policy configuration with dynamic ISE-SGT (Security Group Tag) attributes, ensure that the target Firewall Management Center has the same ISE server configuration. Otherwise, export may lead to object corruption or policy misconfiguration on the target.
- Intrusion policies, independently of access control
- NAT policies
- FlexConfig policies. However, the contents of any secret key variables are cleared when you export the policy. You must manually edit the values of all secret keys after importing a FlexConfig policy that uses secret keys.
- Platform settings
- Health policies
- Alert responses
- Application detectors (both user-defined and those provided by Cisco Professional Services)
- Dashboards

- Custom tables
- Custom workflows
- Saved searches
- Custom user roles
- Report templates
- Third-party product and vulnerability mappings
- Users and groups for user control

Export configurations

Depending on the number of configurations being exported and the number of objects those configurations reference, the export process may take several minutes.

Tip Many list pages include a **YouTube EDU** ( ) icon next to list items. Where this icon is present, you can use it as a quick alternative to the export procedure that follows.

Procedure

Step 1 Choose **System** ( ) > **Tools** > **Import/Export**.

Step 2 Click **Collapse** ( ) and **Expand** ( ) to collapse and expand the list of available configurations.

Step 3 Check the configurations you want to export and click **Export**.

Step 4 Follow your web browser's prompts to save the exported package to your computer.

Import configurations

Depending on the number of configurations being imported and the number of objects those configurations reference, the import process may take several minutes.

Note If you log out of the Firewall Management Center, if you change to a different domain, or if your user session expires after you click **Import**, the import process continues in the background until it is complete. We recommend that you wait for the import process to complete before creating any new objects or policies. Attempting to create them while the import process is still running might result in failures.

Procedure

Step 1 On the importing Firewall Management Center, choose **System** (⚙) > **Tools** > **Import/Export**.

Step 2 Click **Upload Package**.

Step 3 Enter the path to the exported package or browse to its location, then click **Upload**.

Step 4 If there are no version mismatches or other issues, choose the configurations you want to import, then click **Import**.
If you do not need to perform any conflict resolution or interface object mapping, the import completes and a success message appears. Skip the rest of this procedure.

Step 5 If prompted, on the Import Conflict Resolution page, map interface objects used in the imported configurations to zones and groups with matching interface types managed by the importing Firewall Management Center.

Interface object type (security zone or interface group) and interface type (passive, inline, routed, and so on) of source and destination objects must match. For information, see Interfaces.

If the configurations you are importing reference security zones or interface groups that do not already exist, you can map them to existing interface objects, or create new ones.

Note
For individual access control policies, you have the option of replacing an existing policy with the imported ones. However, for nested access control policies, you can only import them as new policies.

Step 6 Click **Import**.

Step 7 If prompted, on the Import Resolution page, expand each configuration and choose the appropriate option as described in Conflict resolution for duplicate configurations, on page 2.

Step 8 Click **Import**.

Step 9 Update all feeds.

For example, go to **Objects** > **Object Management** > **Security Intelligence** and click the **Update Feed** button on the URL, Network, and DNS Lists and Feeds pages.

Imported policies do not include feed contents.

Step 10 Wait for all feed updates to complete before deploying the policies to devices.

What to do next

- Optionally, view a report summarizing the imported configurations; see View task messages.