Configuration Import and Export

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

- About Configuration Import/Export, on page 1
- Requirements and Prerequisites for Configuration Import/Export, on page 3
- Exporting Configurations, on page 3
- Importing Configurations, on page 4

About Configuration Import/Export

You can use the Import/Export feature to copy configurations between appliances. Import/Export is not a backup tool, but can simplify the process of adding new appliances to your deployment.

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 appliance, 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 appliance. When the appliances are compatible but the package includes a duplicate configuration, the system offers resolution options.

Note The importing and exporting appliances must be running the same version of the Firepower System. For access control and its subpolicies (including intrusion policies), the intrusion rule update version must also match. If the versions do not match, the import fails. You cannot use the Import/Export feature to update intrusion rules. Instead, download and apply the latest rule update version.

Configurations that Support Import/Export

Import/Export is supported for the following configurations:

- Access control policies and the policies they invoke: prefilter, network analysis, intrusion, SSL, file, Threat Defense Service Policy
- Intrusion policies, independently of access control
- NAT policies (Firepower Threat Defense only)

- 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

Special Considerations for Configuration Import/Export

When you export a configuration, the system 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 (in a multidomain deployment), 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 system does not export URL filtering category and reputation data, Cisco Intelligence Feed data, or the geolocation database (GeoDB). Make sure all the appliances in your deployment obtain up-to-date information from Cisco.
- Global Security Intelligence lists—The system exports Global Security Intelligence Block and Do Not Block lists associated with exported configurations. (In a multidomain deployment, this occurs regardless of your current domain. The system does **not** export descendant domain lists.) 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 Firepower Management Center in your imported configurations, add them manually.
- 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 Firepower 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 Firepower Management Center, for values not set in the export package. Therefore, an imported intrusion policy may behave differently than expected if the importing Firepower Management Center has differently configured default variables.

- Custom user objects—If you have created custom user groups or objects in your Firepower 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 Firepower Management Center. To avoid detection issues due to the missing user group, add the customized user objects manually to the new Firepower Management Center and re-configure the access control policy after import.

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 system 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 Firepower Management Center, the system 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 Firepower Management Center.
- If you export a configuration that uses PKI objects containing private keys, the system decrypts the private keys before export. On import, the system encrypts the keys with a randomly generated key.

Requirements and Prerequisites for Configuration Import/Export

Model support

Any

Supported domains

Any

User roles

- Admin

Exporting 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 in the Firepower System include an **YouTube EDU** ( ) next to list items. Where this icon is present, you can use it as a quick alternative to the export procedure that follows.

Before you begin

- Confirm that the importing and exporting appliances are running the same version of the Firepower System. For access control and its subpolicies (including intrusion policies), the intrusion rule update version must also match.

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.

Importing 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 system, if you change to a different domain, or if your user session times out after you click **Import**, the import process continues in the background until it is complete.

Before you begin

- Confirm that the importing and exporting appliances are running the same version of the Firepower System. For access control and its subpolicies (including intrusion policies), the intrusion rule update version must also match.

Procedure

Step 1 On the importing appliance, 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 Firepower 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 Interface Objects: Interface Groups and Security Zones.

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 Import Conflict Resolution, on page 5.

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 Viewing Task Messages.

Import Conflict Resolution

When you attempt to import a configuration, the system determines whether a configuration of the same name and type already exists on the appliance. In a multidomain deployment, the system also determines whether a configuration is a duplicate of a configuration defined in the current domain or any of its ancestor or descendant domains. (You cannot view configurations in descendant domains, but if a configuration with a duplicate name exists in a descendant domain, the system notifies you of the conflict.) When an import includes a duplicate configuration, the system offers resolution options suitable to your deployment from among the following:

- **Keep existing**

  The system does not import that configuration.

- **Replace existing**

  The system overwrites the current configuration with the configuration selected for import.

- **Keep newest**

  The system imports the selected configuration only if its timestamp is more recent than the timestamp on the current configuration on the appliance.

- **Import as new**

  The system 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 on the appliance remains unchanged.

The resolution options the system offers depends on whether your deployment uses domains, and whether the imported configuration is a duplicate of a configuration defined in the current domain, or a configuration defined in an ancestor or descendant of the current domain. The following table lists when the system does or does not present a resolution option.

Resolution Option	Firepower Management Center		Managed Device
	Duplicate in current domain	Duplicate in ancestor or descendant domain	
Keep existing	Yes	Yes	Yes
Replace existing	Yes	No	Yes
Keep newest	Yes	No	Yes
Import as new	Yes	Yes	Yes

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 system offers conflict resolution options as described in the table above, but the action the system performs on the policies and file lists varies as described in the table below:

Resolution Option	System Action	
	Access control policy and its associated file policy are imported as new and the file lists are merged	Existing access control policy and its associated file policy and file lists remain unchanged
Keep existing	No	Yes
Replace existing	Yes	No
Import as new	Yes	No
Keep newest and access control policy being imported is the newest	Yes	No
Keep newest and existing access control policy is the newest	No	Yes

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