

Updates

- Content updates, on page 1
- Product upgrades, on page 2
- Guidelines for content updates, on page 2
- Vulnerability database (VDB) updates, on page 3
- Geolocation database (GeoDB) updates, on page 4
- Intrusion rule updates, on page 5
- Intrusion rule update logs, on page 10

Content updates

The system can obtain content updates from the internet. We recommend you schedule or enable automatic content updates whenever possible. Some updates are auto-enabled by the initial setup process or when you enable the related feature. After initial setup, we recommend you review all auto-updates and adjust them if necessary.

Table 1: Content updates

Component	Description	Details
Vulnerability database (VDB)	The Cisco vulnerability database (VDB) is a database of known vulnerabilities to which hosts may be susceptible, as well as fingerprints for operating systems, clients, and applications. The system uses the VDB to help determine whether a particular host increases your risk of compromise.	**Schedule:** As a scheduled task. **Uninstall:** No. **See:** Vulnerability database (VDB) updates, on page 3
Geolocation database (GeoDB)	The Cisco geolocation database (GeoDB) maps IP addresses to countries/continents.	**Schedule:** From its own update page. **Uninstall:** No. **See:** Geolocation database (GeoDB) updates, on page 4

Component	Description	Details
Intrusion rules (SRU/LSP)	Intrusion rule updates provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. Rule updates may also delete rules, provide new rule categories and default variables, and modify default variable values.	**Schedule:** From its own update page. **Uninstall:** No. **See:** Intrusion rule updates, on page 5
Security Intelligence feeds	Security Intelligence feeds are collections of IP addresses, domain names, and URLs that you can use to quickly filter traffic that matches an entry.	**Schedule:** From the object manager. **Uninstall:** No. **See:** *Cisco Secure Firewall Management Center Device Configuration Guide*
URL categories and reputations	URL filtering allows you to control access to websites based on the URL's general classification (category) and risk level (reputation).	**Schedule:** When you configure integrations/cloud services, or as a scheduled task. **Uninstall:** No. **See:** *Cisco Secure Firewall Management Center Device Configuration Guide*

Product upgrades

Guidelines for content updates

Release notes

We recommend you read any release notes or advisory text that accompanies a content update. These provide critical and release-specific information, including compatibility, prerequisites, new capabilities, behavior changes, and warnings.

Scheduled updates

Review scheduled updates to be sure they occur when you intend. The system schedules tasks — including updates — in UTC. This means that when they occur locally depends on the date and your specific location. Also, because updates are scheduled in UTC, they do not adjust for Daylight Saving Time, summer time, or any such seasonal adjustments that you may observe in your location. If you are affected, scheduled updates occur one hour "later" in the summer than in the winter, according to local time.

Vulnerability database (VDB) updates

The Cisco vulnerability database (VDB) is a database of known vulnerabilities to which hosts may be susceptible, as well as fingerprints for operating systems, clients, and applications. The system uses the VDB to help determine whether a particular host increases your risk of compromise.

Cisco issues periodic updates to the VDB. The time it takes to update the VDB and its associated mappings on the Firewall Management Center depends on the number of hosts in your network map. As a rule of thumb, divide the number of hosts by 1000 to determine the approximate number of minutes to perform the update.

The initial setup on the Firewall Management Center automatically downloads and installs the latest VDB from Cisco as a one-time operation. Optionally, schedule tasks to download and install VDB updates and deploy configurations. For more information, see Scheduling.

For VDB 343+, all application detector information is available through Cisco Secure Firewall Application Detectors. This site includes a searchable database of application detectors. The release notes provide information on changes for a particular VDB release.

Schedule VDB updates

If your Firewall Management Center has internet access, we recommend you schedule regular VDB updates. See Scheduling.

Manually update the VDB

Use this procedure to manually update the VDB.

Caution Do not perform tasks related to mapped vulnerabilities while the VDB is updating. Even if the Message Center shows no progress for several minutes or indicates that the update has failed, do not restart the update. Instead, contact Cisco TAC.

In most cases, the first deploy after a VDB update restarts the Snort process, interrupting traffic inspection. The system warns you when this will happen (updated application detectors and operating system fingerprints require a restart; vulnerability information does not). Whether traffic drops or passes without further inspection during this interruption depends on how the targeted device handles traffic. For more information, see *Snort restart traffic behavior* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Procedure

Step 1 Choose **System** (⚙) > **Content Updates** > **VDB Updates**.

In Versions 7.2.0–7.2.5, choose **System** (⚙) > **Updates** > **Content Updates**.

Step 2 Choose how you want to get the VDB onto the Firewall Management Center.

- Direct download: Click the **Download Updates** button to immediately download the latest VDB, latest maintenance release, and the latest critical patches for your deployment.

- Manual upload: Click **Upload Update**, then **Choose File** and browse to the VDB. After you choose the file, click **Upload**.

Step 3 Install the VDB.

a) Click the **Install** icon next to the VDB update.
b) Choose the Firewall Management Center.
c) Click **Install**.

Monitor update progress in the Message Center. After the update completes, the system uses the new vulnerability information. However, you must deploy before updated application detectors and operating system fingerprints can take effect.

Step 4 Verify update success.

The current version is displayed on the VDB update page.

What to do next

Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Geolocation database (GeoDB) updates

The geolocation database (GeoDB) is a database that you can leverage to view and filter traffic based on geographical location. We issue periodic updates to the GeoDB, and you must regularly update the GeoDB to have accurate geolocation information. As part of the initial configuration, the system schedules weekly GeoDB updates. We recommend you review this task and make changes if necessary, as described in Schedule GeoDB updates, on page 4.

A GeoDB update overrides any previous versions. The Firewall Management Center automatically updates its managed devices, and unless the update adds new countries (this is rare) you do not need to redeploy. You can see your current version on the GeoDB update page.

Schedule GeoDB updates

As part of the initial configuration, the system schedules weekly GeoDB updates. We recommend you review this task and make changes if necessary, as described in this procedure.

Note that the system does not automatically deploy after GeoDB updates because in most cases it is not necessary. However, after a scheduled GeoDB update adds a new country (this is rare), deploy as soon as you are able. This allows the new country to count as part of its continent. For example, if an update adds Country to Continent, rules that filter based on "Continent" do not match traffic through Country until you deploy.

Procedure

Step 1 Choose **System** (⚙) > **Content Updates** > **Geolocation Updates**.

In Versions 7.2.0–7.2.5, choose **System** (⚙) > **Updates** > **Geolocation Updates**

Step 2 Under **Recurring Geolocation Updates**, check **Enable Recurring Weekly Updates...**.

Step 3 Specify the **Update Start Time**.

Step 4 Click **Save**.

Manually update the GeoDB

Use this procedure to perform an on-demand GeoDB update.

Procedure

Step 1 Choose **System** (⚙) > **Content Updates** > **Geolocation Updates**.

In Versions 7.2.0–7.2.5, choose **System** (⚙) > **Updates** > **Geolocation Updates**

Step 2 Under **One-Time Geolocation Update**, choose how you want to update the GeoDB.

- Direct download: Choose **Download and install...**.
- Manual upload: Choose **Upload and install...**, then click **Choose File** and browse to the package you downloaded earlier.

Step 3 Click **Import**.

Monitor update progress in the Message Center.

Step 4 Verify update success.

The current version is displayed on the GeoDB update page.

What to do next

If the update adds a new country (this is rare), deploy now. Until you deploy, the new country does not count as part of its continent. For example, if an update adds Country to Continent, rules that filter based on "Continent" do not match traffic through Country until you deploy.

Intrusion rule updates

As new vulnerabilities become known, the Talos Intelligence Group releases intrusion rule updates. These updates affect intrusion rules, preprocessor rules, and the policies that use the rules. Intrusion rule updates are cumulative and we recommend you keep the system up to date. You cannot import an intrusion rule update that either matches or predates the version of the currently installed rules.

An intrusion rule update may provide:

- **New and modified rules and rule states**—Rule updates provide new and updated intrusion and preprocessor rules. For new rules, the rule state may be different in each system-provided intrusion policy. For example, a new rule may be enabled in the Security over Connectivity intrusion policy and disabled in the Connectivity over Security intrusion policy. Rule updates may also change the default state of existing rules, or delete existing rules entirely.
- **New rule categories**—Rule updates may include new rule categories, which are always added.
- **Modified preprocessor and advanced settings**—Rule updates may change the advanced settings in the system-provided intrusion policies and the preprocessor settings in system-provided network analysis policies. They can also update default values for the advanced preprocessing and performance options in your access control policies.
- **New and modified variables**—Rule updates may modify default values for existing default variables, but do not override your changes. New variables are always added.

In a multidomain deployment, you can import local intrusion rules in any domain, but you can import intrusion rule updates from Talos in the Global domain only.

Understanding when intrusion rule updates modify policies

Intrusion rule updates can affect both system-provided and custom network analysis policies, as well as all access control policies:

- **System provided**—Changes to system-provided network analysis and intrusion policies, as well as any changes to advanced access control settings, automatically take effect when you re-deploy the policies after the update.
- **Custom**—Because every custom network analysis and intrusion policy uses a system-provided policy as its base, or as the eventual base in a policy chain, rule updates can affect custom network analysis and intrusion policies. However, you can prevent rule updates from automatically making those changes. This allows you to update system-provided base policies manually, on a schedule independent of rule update imports. Regardless of your choice (implemented on a per-custom-policy basis), updates to system-provided policies do not override any settings you customized.

Note that importing a rule update discards all cached changes to network analysis and intrusion policies. For your convenience, the Rule Updates page lists policies with cached changes and the users who made those changes.

Deploying intrusion rule updates

For changes made by an intrusion rule update to take effect, you must redeploy configurations. When importing a rule update, you can configure the system to automatically redeploy to affected devices. This approach is especially useful if you allow the intrusion rule update to modify system-provided base intrusion policies.



Caution Although a rule update by itself does not restart the Snort process when you deploy, other changes you have made may. Restarting Snort briefly interrupts traffic flow and inspection on all devices, including those configured for high availability/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

Recurring intrusion rule updates

As part of the initial configuration, the system schedules daily intrusion rule updates. We recommend you review this task and make changes if necessary, as described in Schedule intrusion rule updates, on page 7. You may want to change the frequency, or enable automatic deploy after rule imports. For high availability Firewall Management Centers, you only need to import the update on the active unit.

Importing local intrusion rules

A local intrusion rule is a custom standard text rule that you import from a local machine as a plain text file with ASCII or UTF-8 encoding. You can create local rules using the instructions in the Snort users manual, which is available at http://www.snort.org.

In a multidomain deployment, you can import local intrusion rules in any domain. You can view local intrusion rules imported in the current domain and ancestor domains.

Schedule intrusion rule updates

As part of the initial configuration, the system schedules daily intrusion rule updates. We recommend you review this task and make changes if necessary, as described in this procedure.

Before you begin

- Make sure your process for updating intrusion rules complies with your security policies.
- Consider the update's effect on traffic flow and inspection due to bandwidth constraints and Snort restarts. We recommend performing updates in a maintenance window.
- Make sure the Firewall Management Center can access the internet.

Procedure

Step 1 Choose **System** (⚙) > **Content Updates** > **Rule Updates**.

In Versions 7.2.0–7.2.5, choose **System** (⚙) > **Updates** > **Rule Updates**

Step 2 Under **Recurring Rule Update Imports**, check **Enable Recurring Rule Update Imports**.

Step 3 Specify the **Import Frequency** and start time.

Step 4 (Optional) Check **Deploy all policies to targeted devices after rule update completes** to deploy after each update.

Step 5 Click **Save**.

Manually update intrusion rules

Use this procedure to perform an on-demand intrusion rule update.

Before you begin

- Make sure your process for updating intrusion rules complies with your security policies.
- Consider the update's effect on traffic flow and inspection due to bandwidth constraints and Snort restarts. We recommend performing updates in a maintenance window.

Procedure

Step 1 Choose **System** (⚙) > **Content Updates** > **Rule Updates**.

In Versions 7.2.0–7.2.5, choose **System** (⚙) > **Updates** > **Rule Updates**

Step 2 Under **One-Time Rule Update/Rules Import**, choose how you want to update intrusion rules.

- Direct download: Choose **Download new rule update...**.
- Manual upload: Choose **Rule update or text rule file...**, then click **Choose File** and browse to the intrusion rule update.

Step 3 (Optional) Check **Reapply all policies...** to deploy after the update.

Step 4 Click **Import**.

Monitor update progress in the Message Center. Even if the Message Center shows no progress for several minutes or indicates that the update has failed, do not restart the update. Instead, contact Cisco TAC.

Step 5 Verify update success.

The current version is displayed on the rule update page.

What to do next

If you did not deploy as a part of the update, deploy now.

Best practices for importing local intrusion rules

Observe the following guidelines when importing a local rule file:

- The rules importer requires that all custom rules are imported in a plain text file encoded in ASCII or UTF-8.
- The text file name can include alphanumeric characters, spaces, and no special characters other than underscore (_), period (.), and dash (-).
- The system imports local rules preceded with a single pound character (#), but they are flagged as deleted.
- The system imports local rules preceded with a single pound character (#), and does not import local rules preceded with two pound characters (##).
- Rules cannot contain any escape characters.

- You do not have to specify a Generator ID (GID) when importing a local rule. If you do, specify only GID 1 for a standard text rule.
- When importing a rule for the first time, do *not* specify a Snort ID (SID) or revision number. This avoids collisions with SIDs of other rules, including deleted rules. The system will automatically assign the rule the next available custom rule SID of 1000000 or greater, and a revision number of 1.

  If you must import rules with SIDs, a SID can be any unique number 1,000,000 or greater.
- When importing an updated version of a local rule you have previously imported, or when reinstating a local rule you have deleted, you *must* include the SID assigned by the system and a revision number greater than the current revision number. You can determine the revision number for a current or deleted rule by editing the rule.



Note The system automatically increments the revision number when you delete a local rule; this is a device that allows you to reinstate local rules. All deleted local rules are moved from the local rule category to the deleted rule category.

- The import fails if a rule contains any of:
  - A SID greater than 2147483647.
  - A list of source or destination ports that is longer than 64 characters.
- Policy validation fails if you enable an imported local rule that uses the deprecated `threshold` keyword in combination with the intrusion event thresholding feature in an intrusion policy.
- All imported local rules are automatically saved in the local rule category.
- The system always sets local rules that you import to the disabled rule state. You must manually set the state of local rules before you can use them in your intrusion policy.

Import local intrusion rules

Use this procedure to import local intrusion rules. Imported intrusion rules appear in the local rule category in a disabled state.

Before you begin

- Make sure your local rule file follows the guidelines described in Best practices for importing local intrusion rules, on page 8.
- Make sure your process for importing local intrusion rules complies with your security policies.
- Consider the import's effect on traffic flow and inspection due to bandwidth constraints and Snort restarts. We recommend scheduling rule updates during maintenance windows.

Procedure

Step 1 Choose **System** (⚙) > **Content Updates** > **Rule Updates**.

In Versions 7.2.0–7.2.5, choose **System** (⚙) > **Updates** > **Rule Updates**.

You can also click **Import Rules** in the intrusion rules editor (**Objects** > **Intrusion Rules**).

Step 2 (Optional) Delete existing local rules.

Click **Delete All Local Rules**, then confirm that you want to move all created and imported intrusion rules to the deleted folder.

Step 3 Under **One-Time Rule Update/Rules Import**, choose **Rule update or text rule file to upload and install**, then click **Choose File** and browse to your local rule file.

Step 4 Click **Import**.

You can monitor import progress in the Message Center. Even if the Message Center shows no progress for several minutes or indicates that the update has failed, do not restart the import. Instead, contact Cisco TAC.

What to do next

- Edit intrusion policies and enable the rules you imported.
- Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Intrusion rule update logs

Note You search the entire Rule Update Import Log database even when you initiate a search by clicking **Search** on the toolbar from the Rule Update Import Log detailed view with only the records for a single import file displayed. Make sure you set your time constraints to include all objects you want to include in the search.

Table 2: Intrusion rule update log details

Field	Description
Action	An indication that one of the following has occurred for the object type: • `new` (for a rule, this is the first time the rule has been stored) • `changed` (for a rule update component or rule, the rule update component has been modified, or the rule has a higher revision number and the same GID and SID) • `collision` (for a rule update component or rule, import was skipped because its revision conflicts with an existing component or rule) • `deleted` (for rules, the rule has been deleted from the rule update) • `enabled` (for a rule update edit, a preprocessor, rule, or other feature has been enabled in a default policy provided with the system) • `disabled` (for rules, the rule has been disabled in a default policy provided with the system) • `drop` (for rules, the rule has been set to Drop and Generate Events in a default policy provided with the system) • `error` (for a rule update or local rule file, the import failed) • `apply` (the **Reapply all policies after the rule update import completes** option was enabled for the import)
Default Action	The default action defined by the rule update. When the imported object type is `rule`, the default action is `Pass`, `Alert`, or `Drop`. For all other imported object types, there is no default action.
Details	A string unique to the component or rule. For rules, the GID, SID, and previous revision number for a changed rule, displayed as `previously (GID:SID:Rev)`. This field is blank for a rule that has not changed.
GID	The generator ID for a rule. For example, `1` (standard text rule, Global domain or legacy GID) or `3` (shared object rule).
Name	The name of the imported object,`All` which for rules corresponds to the rule Message field, and for rule update components is the component name.
Policy	For imported rules, this field displays . This means that the rule was imported successfully, and can be enabled in all appropriate default intrusion policies. For other types of imported objects, this field is blank.
Rev	The revision number for a rule.
Rule Update	The rule update file name.
SID	The SID for a rule.
Time	The time and date the import began.

Field	Description
Type	The type of imported object, which can be one of the following: • `rule update component` (an imported component such as a rule pack or policy pack) • `rule` (for rules, a new or updated rule) • `policy apply` (the **Reapply all policies after the rule update import completes** option was enabled for the import)
Count	The count (`1`) for each record. The Count field appears in a table view when the table is constrained, and the Rule Update Log detailed view is constrained by default to rule update records. This field is not searchable.