

Updates

- Content updates, on page 1
- Product upgrades, on page 2
- Guidelines for content updates, on page 2
- Vulnerability database (VDB) updates, on page 2
- Geolocation database (GeoDB) updates, on page 4
- Intrusion rule updates, on page 6

Content updates

Content updates keep your deployment current with changing security and contextual information. The system uses this information to evaluate network activity and respond to changes in the threat landscape. Automatic content updates are often enabled by initial configuration or when you enable the related feature.

Types of content updates

Cloud-Delivered Firewall Management Center uses these types of content updates:

- Vulnerability database (VDB): 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.

  Refer to Vulnerability database (VDB) updates, on page 2.

- Geolocation database (GeoDB): Maps IP addresses to countries and continents.

  Refer to Geolocation database (GeoDB) updates, on page 4.

- Intrusion rules (LSP/SRU): Intrusion rule updates provide new and updated intrusion and preprocessor rules and can modify rule states, categories, variables, and default policy settings.

  Refer to Intrusion rule updates, on page 6.

- Security Intelligence feeds: Collections of IP addresses, domain names, and URLs used to filter matching traffic.

  Refer to List and feed updates for security intelligence feeds.

- URL categories and reputations: Classification and risk information used to control access to websites.

  Refer to Enable URL filtering using category and reputation.

Product upgrades

This guide does not include procedures for upgrading firewall software or chassis. Instead, refer to the Secure Firewall Threat Defense upgrade guides for Cloud-Delivered Firewall Management Center.

Guidelines for content updates

These guidelines apply to all content updates. Refer to the topics for each update type for update-specific guidance.

Release information

Read any release notes or advisory text that accompanies a content update. This information describes compatibility, prerequisites, new capabilities, behavior changes, and warnings.

When to perform content updates

Follow these guidelines when performing and scheduling content updates:

- Scheduled updates: Review scheduled updates to make sure they run at the right time for your environment.
- Traffic inspection and flow: Perform updates that might interrupt traffic during maintenance windows.

Content updates are scheduled in Coordinated Universal Time (UTC), which remains constant year-round. Scheduled updates do not adjust automatically for local time changes, such as daylight saving time or summer time. For example, an update scheduled for 2:00 a.m. during standard time runs at 3:00 a.m. after the local clock moves forward.

Vulnerability database (VDB) updates

The 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.

VDB versions

We periodically release VDB updates. Each update replaces the previous version.

Starting with VDB 357, you can install an earlier VDB as far back as the baseline VDB for Cloud-Delivered Firewall Management Center.

VDB update duration

The time required to update the VDB and its associated mappings on the Cloud-Delivered Firewall Management Center depends on the number of hosts in your network map. Allow approximately one minute for every 1000 hosts.

Scheduled VDB updates

Initial configuration automatically downloads and installs the latest VDB as a one-time operation and creates a weekly task to download future updates. Review the schedule and adjust as needed. To update the VDB and deploy configurations automatically, create separate tasks. For more information, refer to Scheduling.

Deployment after VDB updates

Deploy configuration changes after a VDB update for updated application detectors and operating system fingerprints to take effect. Updated vulnerability information takes effect without deploy.

Caution The first deploy after a VDB update usually restarts Snort because updated application detectors and operating system fingerprints require a restart. Restarting Snort briefly interrupts traffic flow and inspection on all devices, including those configured for high availability or 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.

VDB release information

For VDB 343 and later, Cisco Secure Firewall Application Detectors provides searchable application detector information. The release notes describe changes in each VDB release.

VDB lite

For the Secure Firewall 220, the system installs a smaller VDB (also called VDB lite). This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB.

Manually update the VDB

Perform an on-demand update to keep the VDB current or to install an older VDB.

Before you begin

If you are installing an older VDB, download it manually from https://www.cisco.com/go/firepower-software. Choose any Cloud-Delivered Firewall Management Center model, then open the Coverage and Content Updates page.

Starting with VDB 357, you can install any VDB as far back as the baseline VDB for the Cloud-Delivered Firewall Management Center.

Procedure

Step 1 Choose **Administration** > **Upgrades & updates** > **Content Updates** > **VDB Updates**.

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

- Direct download: Click **Download Updates**.
- Manual upload: Click **Upload Update**, click **Choose File**, select the VDB, and click **Upload**.

Step 3 Install the VDB.

a) Next to the VDB update you want to install, click either the **Install** icon (for a newer VDB) or the **Rollback** icon (for an older VDB).
b) Choose the Cloud-Delivered Firewall Management Center.
c) Click **Install**.

Monitor update progress in the Message Center. Do not use mapped-vulnerability features while the VDB is updating. If the Message Center shows no progress for several minutes or reports that the update failed, do not restart it. Contact Cisco TAC.

Step 4 Verify update success.

The current version is displayed on the VDB update page.

The system uses the new vulnerability information. However, you must deploy before updated application detectors and operating system fingerprints can take effect.

What to do next

- Deploy configuration changes.
- If configurations reference vulnerabilities, application detectors, or fingerprints that are no longer available, review those configurations to confirm that they handle traffic as expected. A scheduled VDB update can undo a rollback. To retain the older VDB, change the scheduled task or delete any newer VDB packages.

Geolocation database (GeoDB) updates

The geolocation database (GeoDB) maps IP addresses to geographic locations so that you can view and filter traffic by location.

GeoDB versions

We periodically release GeoDB updates. Each update replaces the previous version.

Scheduled GeoDB updates

Initial configuration schedules weekly updates to keep geolocation information accurate. Review the schedule and adjust it as needed. Refer to Schedule GeoDB updates, on page 5.

Deployment after GeoDB updates

The Cloud-Delivered Firewall Management Center automatically updates the GeoDB on managed devices, so deploy is usually unnecessary. If an update adds a new country, which is rare, deploy configuration changes as soon as possible. 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.

Schedule GeoDB updates

Schedule recurring GeoDB updates to keep the installed geolocation information current.

Initial configuration creates a weekly schedule for GeoDB updates. Review the schedule and adjust the start time as needed.

Procedure

Step 1 Choose **Administration** > **Upgrades & updates** > **Content Updates** > **Geolocation Updates**.

Step 2 Configure recurring GeoDB updates.

a) Under **Recurring Geolocation Updates**, check **Enable Recurring Weekly Updates from the Support Site**.

b) Specify the **Update Start Time**.

Step 3 Click **Save**.

Manually update the GeoDB

Perform an on-demand update to keep the GeoDB current.

Procedure

Step 1 Choose **Administration** > **Upgrades & updates** > **Content Updates** > **Geolocation Updates**.

Step 2 Under **One-Time Geolocation Update**, choose how you want to get the GeoDB onto the Cloud-Delivered Firewall Management Center.

- Direct download: Choose **Download and install geolocation update from the Support Site**.
- Manual upload: Choose **Upload and install geolocation update**, click **Choose File**, and select the GeoDB.

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.

The system uses the new geolocation information. However, you must deploy before new countries can take effect. 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.

What to do next

If the update adds a new country, deploy configuration changes.

Intrusion rule updates

An intrusion rule update is a cumulative package that provides new and modified intrusion and preprocessor rules, and modifies the policies that use them.

Intrusion rule update versions

As new vulnerabilities become known, the Talos Intelligence Group releases intrusion rule updates. Keep intrusion rules up to date. Each update replaces the previous version, and you can import only an update that is newer than the currently installed version.

Contents of intrusion rule updates

An intrusion rule update can contain these types of content:

- Rules and rule states: An update can add, modify, or delete intrusion and preprocessor rules. The default state of a new rule can differ between system-provided intrusion policies. For example, a new rule can be enabled in the Security over Connectivity policy and disabled in the Connectivity over Security policy. An update can also change the default state of an existing rule.
- Rule categories: An update can contain new rule categories. Importing the update adds all new categories.
- Preprocessor and advanced settings: An update can change advanced settings in system-provided intrusion policies and preprocessor settings in system-provided network analysis policies. It can also change the default values of advanced preprocessing and performance options in access control policies.
- Variables: An update can change the default values of existing variables without overriding customized values. It also adds new variables.

Policy changes from intrusion rule updates

Intrusion rule updates can affect system-provided and custom network analysis and intrusion policies, as well as the access control policies that use them. The effects depend on the policy type.

- System-provided policies: Changes to system-provided network analysis and intrusion policies and advanced access control settings take effect after you redeploy the configuration.
- Custom policies: Every custom network analysis and intrusion policy is based directly or indirectly on a system-provided policy. For each custom policy, you can prevent rule updates from automatically applying changes from its base policy. You can then apply the base-policy changes manually on a schedule independent of rule update imports. Updates do not override customized settings.



Caution Importing an intrusion rule update discards all cached changes to network analysis and intrusion policies. Before you import an update, use the Rule Updates page to identify policies with cached changes and the users who made them.

Scheduled intrusion rule updates

Initial configuration creates a daily schedule for intrusion rule updates. Review the schedule and adjust the frequency as needed. Refer to Schedule intrusion rule updates, on page 7.

Deployment after intrusion rule updates

Deploy configuration changes after an intrusion rule update for the update's changes to take effect. You can configure an import to deploy automatically to affected devices. Automatic deployment is especially useful when you allow updates to modify system-provided base intrusion policies.



Caution Although a rule update by itself does not restart Snort 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 or 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.

Schedule intrusion rule updates

Schedule recurring intrusion rule updates to keep the installed intrusion rules current.

Before you begin

Make sure your process for updating intrusion rules complies with your security policies.

Initial configuration creates a daily schedule for intrusion rule updates. Review the schedule and adjust the frequency as needed. You can also configure automatic deployment after each rule update. Automatic deployment can disrupt traffic inspection and flow.

Procedure

Step 1 Choose **Administration** > **Upgrades & updates** > **Content Updates** > **Rule Updates**.

Step 2 Configure recurring rule updates.

a) Under **Recurring Rule Update Imports**, check **Enable Recurring Rule Update Imports**.
b) Specify the **Import Frequency** and start time.
c) (Optional) Check **Deploy all policies to targeted devices after rule update completes**.

Step 3 Click **Save**.

Manually update intrusion rules

Perform an on-demand update to keep intrusion rules current.

Before you begin

Make sure your process for updating intrusion rules complies with your security policies.

Procedure

Step 1 Choose **Administration** > **Upgrades & updates** > **Content Updates** > **Rule Updates**.

Step 2 Configure the one-time rule update.

a) Under **One-Time Rule Update/Rules Import**, choose how to update intrusion rules.

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

b) (Optional) Check **Reapply all policies after the rule update import completes**.

Step 3 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 4 Verify update success.

The current version is displayed on the rule update page.

What to do next

If you did not deploy configuration changes as part of the update, deploy them now.

Guidelines for importing custom Snort 2 rules

Use these guidelines to import custom standard text rules for use in Snort 2 intrusion policies.

File and rule syntax requirements

Import rules using a rule file that meets these requirements:

- Use a plain text file encoded in ASCII or UTF-8.
- Use only alphanumeric characters, spaces, underscores (_), periods (.), and hyphens (-) in the file name.
- To import a rule in the deleted state, precede it with one number sign (`#`). A rule preceded by two number signs (`##`) is not imported.
- Do not use escape characters in rules.
- Limit each source or destination port list to 64 characters. A longer list causes the import to fail.

For more information on writing custom rules, refer to *Custom Snort 2 Intrusion Policies for Access Control* and to the Snort manual at http://www.snort.org.

SID, GID, and revision number requirements

Follow these requirements for SIDs, GIDs, and revision numbers:

- Do not specify a GID. A standard text rule receives GID 1.
- Leave the SID and revision number unspecified when importing a rule for the first time. The rule receives an available SID of 1000000 or greater and a revision number of 1.
- If you must specify a SID for a new rule, use an unassigned value from 1000000 through 2147483647 (the 32-bit limit).
- When importing an updated or previously deleted rule, include its assigned SID and a revision number greater than its current revision number.

To determine the current revision number, edit the imported rule. Deleting a custom rule moves it to the deleted rule category and increments its revision number. You can then import a later revision to reinstate the rule.

Import custom Snort 2 rules

Import custom standard text rules so you can enable them in Snort 2 intrusion policies.

This procedure applies only to custom standard text rules for Snort 2 intrusion policies. For Snort 3, refer to the rule-tuning topics in *Custom Snort 3 Intrusion Policies for Access Control*.

Before you begin

- Make sure your custom rule file follows the guidelines in Guidelines for importing custom Snort 2 rules, on page 8.
- Make sure your process for importing custom rules complies with your security policies.

Procedure

Step 1 Choose **Administration** > **Upgrades & updates** > **Content Updates** > **Rule Updates**.

You can also click **Import Rules** in the intrusion rules editor (**Policies** > **+ Show more** > **Security policies** > **Intrusion Rules**).

Step 2 (Optional) Delete all existing custom rules.

To replace all existing custom rules with the rules in the new file, click **Delete All Local Rules**. The deleted rules move to the deleted rule category, and their revision numbers increase.

Step 3 Import the rule file.

a) Under **One-Time Rule Update/Rules Import**, choose **Rule update or text rule file to upload and install**.
b) Click **Choose File**, select your rule file, and 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 import has failed, do not restart the import. Instead, contact Cisco TAC.

- Imported rules are added to the local rule category in a disabled state.
- Imported rules receive Generator ID (GID) 1.

- New imported rules receive an available Snort ID (SID) of 1000000 or greater and a revision of 1.

What to do next

- Edit Snort 2 intrusion policies and enable the rules you imported.

  Do not enable an imported rule that uses the deprecated `threshold` keyword in an intrusion policy that also uses intrusion event thresholding. This combination causes policy validation to fail.

- Deploy configuration changes.

Intrusion rule update logs

The Rule Update Log on the Rule Updates page records each intrusion rule update and custom Snort 2 rule import, including its time, user, and status. Each log also identifies the affected rules and components. Deleting a log does not delete the imported objects.

Intrusion rule update log fields

This table explains the fields in intrusion rule update logs.

Table 1: Intrusion rule update log fields

Field	Description
Action	Identifies how the import affected the object.
Default action	For a rule, the default action defined by the update is Pass, Alert, or Drop. The field is blank for other object types.
Details	Identifies the affected component or rule. For a changed rule, the field displays the GID, SID, and previous revision number in `GID:SID:Rev` format. The field is blank for a rule that has not changed.
GID	The generator ID for a rule. For example: • A GID of 1 identifies a standard text rule. • A GID of 3 identifies a shared object rule.
Name	The name of the imported object. For a rule, the name corresponds to the rule's Message field. For a rule update component, the field displays the component name.
Policy	For an imported rule, the field displays `All` when the import succeeds and the rule can be enabled in all applicable system-provided default intrusion policies. The field is blank for other object types.
Rev	The revision number for a rule.
Rule update	The rule update file name.
SID	The Snort ID for a rule.
Time	The time and date the import began.

Field	Description
Type	Identifies the imported object as a rule update component, rule, or policy apply. A policy apply record indicates that the option to reapply all policies after the import was enabled.

Action values

The Action field in intrusion rule update logs uses these values.

Table 2: Action values in intrusion rule update logs

Action	Meaning
new	The rule was stored for the first time.
changed	A rule update component was modified, or a rule was imported with a higher revision number and the same GID and SID.
collision	The import was skipped because the revision conflicts with an existing component or rule.
deleted	The rule was deleted from the rule update.
enabled	A rule, preprocessor, or other feature was enabled in a system-provided default policy.
disabled	A rule was disabled in a system-provided default policy.
drop	A rule was set to Drop and Generate Events in a system-provided default policy.
error	The update or import failed.
apply	The option to reapply all policies after the import was enabled.

Searching intrusion rule update logs

A search from the detailed log view searches the entire database, not only the selected import. Use the time range to limit the results to relevant records.