

System Updates

The following topics explain how to update Firepower deployments:

- About System Updates, on page 1
- Requirements and Prerequisites for System Updates, on page 3
- Guidelines and Limitations for System Updates, on page 3
- Upgrade System Software, on page 4
- Update the Vulnerability Database (VDB), on page 4
- Update the Geolocation Database, on page 6
- Update Intrusion Rules, on page 8
- Maintain Your Air-Gapped Deployment, on page 17
- History for System Updates, on page 18

About System Updates

You can use the FMC to upgrade the system software for itself and the devices it manages. You can also update various databases and feeds that provide advanced services.

For FMCs with internet access, the system can often obtain updates directly from Cisco. We recommend you schedule or enable automatic updates whenever possible. Some updates are auto-enabled by the initial setup process or when you enable the related feature. Other updates you must schedule yourself. After initial setup, we recommend you review all auto-updates and adjust them if necessary.

Table 1: Upgrades and Updates in FMC Deployments

Component	Description	Details
Firepower software	*Major* software releases contain new features, functionality, and enhancements. They may include infrastructure or architectural changes. *Maintenance* releases contain general bug and security related fixes. Behavior changes are rare, and are related to those fixes. *Patches* are on-demand updates limited to critical fixes with time urgency. *Hotfixes* can address specific customer issues.	**Direct Download:** Select releases only, usually some time after the release is available for manual download. The length of the delay depends on release type, release adoption, and other factors. **Schedule:** Patches only, on **System** > **Tools** > **Scheduling**. **Uninstall:** Patches only. **Reimage:** Major and maintenance releases only. **See:** Upgrade System Software, on page 4
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.	**Direct Download:** Yes. **Schedule:** Yes, on **System** > **Tools** > **Scheduling**. **Uninstall:** No. **See:** Update the Vulnerability Database (VDB), on page 4
Geolocation database (GeoDB)	The Cisco geolocation database (GeoDB) is a database of geographical and connection-related data associated with routable IP addresses.	**Direct Download:** Yes. **Schedule:** Yes, on **System** > **Updates**. **Uninstall:** No. **See:** Update the Geolocation Database, on page 6
Intrusion rules (SRU)	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.	**Direct Download:** Yes. **Schedule:** Yes, on **System** > **Updates**. **Uninstall:** No. **See:** Update Intrusion Rules, on page 8
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.	**Direct Download:** Yes. **Schedule:** Yes, on **Objects** > **Object Management**. **Uninstall:** No. **See:** List and Feed Updates for Security Intelligence

Component	Description	Details
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).	**Direct Download:** Yes. **Schedule:** Yes, on **System** > **Integration** > **Cloud Services** *or* **System** > **Tools** > **Scheduling**, depending on your requirements. **Uninstall:** No. **See:** Enable URL Filtering Using Category and Reputation

Requirements and Prerequisites for System Updates

Model Support

Any

Supported Domains

Global unless indicated otherwise.

User Roles

Admin

Guidelines and Limitations for System Updates

Before You Update

Before you update any component of your Firepower deployment (including intrusion rules, VDB, or GeoDB) read the release notes or advisory text that accompanies the update. These provide critical and release-specific information, including compatibility, prerequisites, new capabilities, behavior changes, and warnings.

Scheduled Updates

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.



Important We *strongly* recommend you review scheduled updates to be sure they occur when you intend.

Bandwidth Guidelines

To upgrade a Firepower appliance (or perform a readiness check), the upgrade package must be on the appliance. Firepower upgrade package sizes vary. Make sure you have the bandwidth to perform a large data transfer to your managed devices. See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).

Upgrade System Software

This guide does not contain detailed upgrade instructions for either system software or companion operating systems. Instead, see the Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.

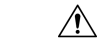
For information on scheduling downloads and installations for system software patches, see Software Update Automation. Note that the initial setup process automatically schedules a weekly patch download. After setup, you should review the auto-scheduled configurations and adjust them if necessary.

Update the 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.

Cisco issues periodic updates to the VDB. The time it takes to update the VDB and its associated mappings on the FMC 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.

When you set up a new or reimaged FMC, the system automatically attempts to update the vulnerability database (VDB). This is a one-time operation. If the FMC has internet access, we recommend you schedule tasks to perform automatic recurring VDB update downloads and installations.



Caution In most cases, the first deploy after updating the VDB restarts the Snort process on managed devices. The system warns you that this can happen — warnings can appear after manual VDB updates, when you schedule VDB updates, during background VDB updates, when you deploy, and so on. Snort restarts cause an interruption in traffic inspection and, depending on how the managed device handles traffic, possibly interrupts traffic flow. For more information, see Snort® Restart Traffic Behavior.

Manually Update the VDB

To update the VDB, the VDB update package must be on the FMC.

If the Firepower Management Center cannot access the internet, or you want to manually upload the VDB update to the Firepower Management Center, use this procedure. To automate VDB updates, use task scheduling (**System** > **Tools** > **Scheduling**). For details, see Vulnerability Database Update Automation.

Before you begin

- Download the update from https://www.cisco.com/go/firepower-software.

Note Beginning with VDB Release 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.

- Consider the update's effect on traffic flow and inspection due to Snort restarts. We recommend performing updates in a maintenance window.

Procedure

Step 1 Choose **System** > **Updates**, then click **Product Updates**.

Step 2 Choose how you want to upload the VDB update to the FMC.

- Download directly from Cisco.com: Click **Download Updates**. If it can access the Cisco Support & Download site, the Firepower Management Center downloads the latest VDB. Note that the Firepower Management Center also downloads a package for each patch and hotfix (but not major release) associated with the version your appliances are currently running.
- Upload manually: Click **Upload Update**, then **Choose File**. Browse to the update you downloaded earlier, and click **Upload**.

VDB updates appear on the same page as Firepower software upgrade and uninstaller packages.

Step 3 Install the update.

a) Click Install next to the Vulnerability and Fingerprint Database update.
b) Choose the Firepower Management Center.
c) Click **Install**.

Step 4 (Optional) Monitor update progress in the Message Center.

Do not perform tasks related to mapped vulnerabilities until the update completes. 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.

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 5 Verify update success.

Choose **Help** > **About** to view the current VDB version.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Schedule VDB Updates

If your FMC has internet access, we recommend you schedule regular VDB updates. See Vulnerability Database Update Automation.

Update the Geolocation Database

The geolocation database (GeoDB) is a database that you can leverage to view and filter traffic based on geographical location.

The system comes with an initial GeoDB that maps IP addresses to countries/continents, so that information should always be available. If you update the GeoDB, the system also downloads contextual data. This contextual data includes additional location details, as well as connection information such as ISP, connection type, proxy type, domain name, and so on. We issue periodic updates to the GeoDB. You must regularly update the GeoDB to have accurate geolocation information.

As a part of initial configuration the FMC configures a weekly automatic GeoDB update. You can observe the status of this update using the web interface Message Center. If configuring the update fails and your FMC has internet access, we recommend you configure regular GeoDB updates as described in Schedule GeoDB Updates, on page 7.

The time needed to update the GeoDB depends on your appliance, but can take up to 45 minutes depending on the size of the update—for example, if this is the first time you are downloading the full GeoDB. Although a GeoDB update does not interrupt any other system functions (including the ongoing collection of geolocation information), the update does consume system resources while it completes. Consider this when planning your updates.

The GeoDB update overrides any previous versions of the GeoDB and is effective immediately. When you update the GeoDB, the FMC automatically updates the related data on its managed devices. It may take a few minutes for a GeoDB update to take effect throughout your deployment. You do not need to re-deploy after you update.

The **System** > **Updates** > **Geolocation Updates** page and the **Help** > **About** page both list the current version.



Note In May 2022 we split the GeoDB into two packages: a country code package that maps IP addresses to countries/continents, and an IP package that contains contextual data. The new country code package has the same file name as the old all-in-one package. This allows FMCs running Version 7.1 and earlier to continue to obtain GeoDB updates. However, because this package now contains only country code mappings, the contextual data is no longer updated and will grow stale. To obtain fresh data, upgrade or reimage to Version 7.2+ and update the GeoDB. Note that this split does not affect geolocation rules or traffic handling in any way—those rules rely only on the data in the country code package.

Manually Update the GeoDB (Internet Connection)

You can import a new GeoDB update by automatically connecting to the Support Site only if the appliance has Internet access.

Procedure

Step 1 Choose **System** > **Updates**.

Step 2 Click **Geolocation Updates**.

Step 3 Choose **Download and install geolocation update from the Support Site**.

Step 4 Click **Import**.
The system queues a Geolocation Update task, which checks for the latest updates on the Cisco Support Site (http://www.cisco.com/cisco/web/support/index.html).

Step 5 Optionally, monitor the task status; see Viewing Task Messages.

Step 6 After the update finishes, return to the Geolocation Updates page or choose **Help** > **About** to confirm that the GeoDB build number matches the update you installed.

Manually Update the GeoDB (No Internet Connection)

Use this procedure to perform an on-demand update of the GeoDB if the FMC does not have internet access.

Procedure

Step 1 Download the GeoDB from the Cisco Support & Download site: https://www.cisco.com/go/firepower-software.

Select or search for your model (or choose any model—you use the same GeoDB for all FMCs), then browse to the *Coverage and Content Updates* page.

Make sure you download the country code package: Cisco_GEODB_Update-*date-build*. The IP package is for Version 7.2+.

Step 2 Choose **System** > **Updates** > **Geolocation Updates**.

Step 3 Under One-Time Geolocation Update, choose **Upload and install geolocation update**.

Step 4 Click **Choose File**, then browse to the country code package you downloaded earlier.

Step 5 Click **Import**.

You can monitor update progress in the Message Center.

Step 6 Verify update success.
The Geolocation Updates page and the **Help** > **About** page both list the current version.

Schedule GeoDB Updates

As a part of initial configuration the FMC configures a weekly automatic GeoDB update. You can observe the status of this update using the web interface Message Center. If configuring the update fails and your FMC has internet access, we recommend you configure regular GeoDB updates as described in this topic.

Before you begin

Make sure the FMC can access the internet.

Procedure

Step 1 Choose **System** > **Updates**, then click **Geolocation Updates**.

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

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

Step 4 Click **Save**.

Update Intrusion Rules

As new vulnerabilities become known, the Cisco Talos Intelligence Group (Talos) releases intrusion rule updates that you can import onto your Firepower Management Center, and then implement by deploying the changed configuration to your managed devices. These updates affect intrusion rules, preprocessor rules, and the policies that use the rules.

Intrusion rule updates are cumulative, and Cisco recommends you always import the latest update. 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 the following:

- **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.

Recurring Intrusion Rule Updates

You can import rule updates on a daily, weekly, or monthly basis, using the Rule Updates page.

If your deployment includes a high availability pair of Firepower Management Centers, import the update on the primary only. The secondary Firepower Management Center receives the rule update as part of the regular synchronization process.

Applicable subtasks in the intrusion rule update import occur in the following order: download, install, base policy update, and configuration deploy. When one subtask completes, the next subtask begins.

At the scheduled time, the system installs the rule update and deploys the changed configuration as you specified in the previous step. You can log off or use the web interface to perform other tasks before or during the import. When accessed during an import, the Rule Update Log displays a **Red Status** (), and you can view messages as they occur in the Rule Update Log detailed view. Depending on the rule update size and content, several minutes may pass before status messages appear.

As a part of initial configuration the FMC configures a daily automatic intrusion rule update from the Cisco support site. (The FMC deploys automatic intrusion rule updates to affected managed devices when it next deploys affected policies.) You can observe the status of this update using the web interface Message Center. If configuring the update fails and your FMC has internet access, we recommend you configure regular intrusion rule updates as described in Schedule Intrusion Rule Updates, on page 10.

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.

Update Intrusion Rules One-Time Manually

Import a new intrusion rule update manually if your Firepower Management Center does not have Internet access.

Procedure

Step 1 Manually download the update from the Cisco Support Site (http://www.cisco.com/cisco/web/support/index.html).

Step 2 Choose **System** > **Updates**, then click **Rule Updates**.

Step 3 If you want to move all user-defined rules that you have created or imported to the deleted folder, you must click **Delete All Local Rules** in the toolbar, then click **OK**.

Step 4 Choose **Rule Update or text rule file to upload and install** and click **Browse** to navigate to and choose the rule update file.

Step 5 If you want to automatically re-deploy policies to your managed devices after the update completes, choose **Reapply all policies after the rule update import completes**.

Step 6 Click **Import**. The system installs the rule update and displays the Rule Update Log detailed view.

Note Contact Support if you receive an error message while installing the rule update.

Update Intrusion Rules One-Time Automatically

To import a new intrusion rule update automatically, your appliance must have Internet access to connect to the Support Site.

Before you begin

- Ensure the Firepower Management Center has internet access; see Security, Internet Access, and Communication Ports.

Procedure

Step 1 Choose **System** > **Updates**.

Tip You can also click **Import Rules** on the Rule Editor page, which you access by choosing **Policies** > **Intrusion** > **Intrusion Rules**.

Step 2 Click **Rule Updates**.

Step 3 If you want to move all user-defined rules that you have created or imported to the deleted folder, click **Delete All Local Rules** in the toolbar, then click **OK**.

Step 4 Choose **Download new Rule Update from the Support Site**.

Step 5 If you want to automatically re-deploy the changed configuration to managed devices after the update completes, check the **Reapply all policies after the rule update import completes** check box.

Step 6 Click **Import**.
The system installs the rule update and displays the Rule Update Log detailed view.

Caution Contact Support if you receive an error message while installing the rule update.

Schedule Intrusion Rule Updates

As a part of initial configuration the FMC configures a daily automatic intrusion rule update from the Cisco support site. (The FMC deploys automatic intrusion rule updates to affected managed devices when it next deploys affected policies.) You can observe the status of this update using the web interface Message Center.

If configuring the update fails and your FMC has internet access, we recommend you configure regular intrusion rule updates as described in this section.

Procedure

Step 1 Choose **System** > **Updates**.

Tip You can also click **Import Rules** on the Rule Editor page, which you access by choosing **Policies** > **Intrusion** > **Intrusion Rules**.

Step 2 Click **Rule Updates**.

Step 3 If you want to move all user-defined rules that you have created or imported to the deleted folder, click **Delete All Local Rules** in the toolbar, then click **OK**.

Step 4 Check **Enable Recurring Rule Update Imports from the Support Site** check box.

Import status messages appear beneath the **Recurring Rule Update Imports** section heading.

Step 5 In the **Import Frequency** field, specify:

- The frequency of the update (**Daily**, **Weekly**, or **Monthly**)
- The day of the week or month you want the update to occur
- The time you want the update to start

Step 6 If you want to automatically re-deploy the changed configuration to your managed devices after the update completes, check the **Deploy updated policies to targeted devices after rule update completes** check box.

Step 7 Click **Save**.

Caution Contact Support if you receive an error message while installing the intrusion rule update.

The status message under the Recurring Rule Update Imports section heading changes to indicate that the rule update has not yet run.

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.
- In a multidomain deployment, the system assigns a GID of 1 to a rule imported into or created in the Global domain, and a domain-specific GID between 1000 and 2000 for all other domains.

- 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.

  In a multidomain deployment, if multiple administrators are importing local rules at the same time, SIDs within an individual domain might appear to be non-sequential because the system assigned the intervening numbers in the sequence to another domain.
- 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.

- Import local rules on the primary Firepower Management Center in a high availability pair to avoid SID numbering issues.
- The import fails if a rule contains any of the following: .
  - A SID greater than 2147483647.
  - A list of source or destination ports that is longer than 64 characters.
  - When importing into the Global domain in a multidomain deployment, a GID:SID combination uses GID 1 and a SID that already exists in another domain; this indicates that the combination existed before Version 6.2.1. You can reimport the rule using GID 1 and a unique SID.
- 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

- Make sure your local rule file follows the guidelines described in Best Practices for Importing Local Intrusion Rules, on page 11.
- 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.
- You can perform this task in any domain.

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

Procedure

Step 1 Choose **System** > **Updates**, then click **Rule Updates**.

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**.

Step 5 Monitor import progress in the Message Center.

To display the Message Center, click System Status on the menu bar. 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.

What to do next

- Edit intrusion policies and enable the rules you imported.
- Deploy configuration changes; see Deploy Configuration Changes.

Rule Update Log

The Firepower Management Center generates a record for each rule update and local rule file that you import.

Each record includes a time stamp, the name of the user who imported the file, and a status icon indicating whether the import succeeded or failed. You can maintain a list of all rule updates and local rule files that you import, delete any record from the list, and access detailed records for all imported rules and rule update components.

The Rule Update Import Log detailed view lists a detailed record for each object imported in a rule update or local rule file. You can also create a custom workflow or report from the records listed that includes only the information that matches your specific needs.

Intrusion Rule Update Log Table

Table 2: Intrusion Rule Update Log Fields

Field	Description
Summary	The name of the import file. If the import fails, a brief statement of the reason for the failure appears under the file name.
Time	The time and date that the import started.

Field	Description
User ID	The user name of the user that triggered the import.
Status	Whether the import: • **Succeeded** ( ) • failed or is currently in progress **Red Status** ( ) The red status icon indicating an unsuccessful or incomplete import appears on the Rule Update Log page during the import and is replaced by the green icon only when the import has successfully completed.

Tip You can view import details as they appear while an intrusion rule update import is in progress.

Viewing the Intrusion Rule Update Log

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

Procedure

Step 1 Choose **System** > **Updates**.

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

Step 2 Click **Rule Updates**.

Step 3 Click **Rule Update Log**.

Step 4 You have two options:

- View — To view details for each object imported in a rule update or local rule file, click **View** ( ) next to the file you want to view; see Viewing Details of the Intrusion Rule Update Import Log, on page 16.
- Delete — To delete an import file record from the import log, including detailed records for all objects included with the file, click **Delete** ( ) next to the import file name.

Note Deleting the file from the log does not delete any object imported in the import file, but only deletes the import log records.

Fields in an Intrusion Rule Update Log



Tip 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 3: Rule Update Import Log Detailed View Fields

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 on this appliance) • `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 on the appliance) • `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.
Domain	The domain whose intrusion policies can use the updated rule. Intrusion policies in descendant domains can also use the rule. This field is only present in a multidomain deployment.
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, 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 `All`. 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.

Field	Description
Rule Update	The rule update file name.
SID	The SID for a rule.
Time	The time and date the import began.
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; note that in Version 5.0.1 this value replaced the `update` value, which is deprecated) • `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.

Viewing Details of the Intrusion Rule Update Import Log

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

Procedure

Step 1 Choose **System** > **Updates**.

Tip You can also click **Import Rules** on the Rule Editor page, which you access by choosing **Policies** > **Intrusion** > **Intrusion Rules**.

Step 2 Click **Rule Updates**.

Step 3 Click **Rule Update Log**.

Step 4 Click **View** ( ) next to the file whose detailed records you want to view.

Step 5 You can take any of the following actions:

- Bookmark—To bookmark the current page, click **Bookmark This Page**.
- Edit Search—To open a search page prepopulated with the current single constraint, choose **Edit Search** or **Save Search** next to Search Constraints.
- Manage bookmarks—To navigate to the bookmark management page, click **Report Designer**.
- Report—To generate a report based on the data in the current view, click **Report Designer**.
- Search—To search the entire Rule Update Import Log database for rule update import records, click **Search**.
- Sort—To sort and constain records on the current workflow page, see Using Drill-Down Pages for more information.

- Switch workflows—To temporarily use a different workflow, click **(switch workflows)**.

Maintain Your Air-Gapped Deployment

If your Firepower system is not connected to the internet, essential updates will not occur automatically. You must manually obtain and install these updates. See the following information:

- Manually Update the VDB, on page 4
- Update Intrusion Rules One-Time Manually, on page 9
- Manually Update the GeoDB (No Internet Connection), on page 7
- The *Firepower Management Center Software Upgrade Guide* at https://www.cisco.com/c/en/us/td/docs/security/firepower/upgrade/fpmc-upgrade-guide.html

History for System Updates

Feature	Version	Details
Improved Firepower Threat Defense upgrade status reporting and cancel/retry options	6.7.0	You can now view the status of Firepower Threat Defense device upgrades and readiness checks in progress on the Device Management page, as well as a 7-day history of upgrade success/failures. The Message Center also provides enhanced status and error messages. A new Upgrade Status pop-up, accessible from both Device Management and the Message Center with a single click, shows detailed upgrade information, including percentage/time remaining, specific upgrade stage, success/failure data, upgrade logs, and so on. Also on this pop-up, you can manually cancel failed or in-progress upgrades (**Cancel Upgrade**), or retry failed upgrades (**Retry Upgrade**). Canceling an upgrade reverts the device to its pre-upgrade state. **Note** To be able to manually cancel or retry a failed upgrade, you must disable the new auto-cancel option, which appears when you use the FMC to upgrade an Firepower Threat Defense device: **Automatically cancel on upgrade failure and roll back to the previous version**. With the option enabled, the device automatically reverts to its pre-upgrade state upon upgrade failure. Auto-cancel is not supported for patches. In an HA or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. New/modified screens: • **System** > **Update** > **Product Updates** > **Available Updates** > **Install** icon for the Firepower Threat Defense upgrade package • **Devices** > **Device Management** > **Upgrade** • **Message Center > Tasks** New Firepower Threat Defense CLI commands: • **show upgrade status detail** • **show upgrade status continuous** • **show upgrade status** • **upgrade cancel** • **upgrade retry**
Upgrades remove PCAP files to save disk space	6.7.0	To upgrade a Firepower appliance, you must have enough free disk space or the upgrade fails. Upgrades now remove locally stored PCAP files.

Feature	Version	Details
Custom intrusion rule import warns when rules collide	6.7.0	The FMC now warns you of rule collisions when you import custom (local) intrusion rules. Previously, the system would silently skip the rules that cause collisions—with the exception of Version 6.6.0.1, where a rule import with collisions would fail entirely. On the Rule Updates page, if a rule import had collisions, a warning icon is displayed in the Status column. For more information, hover your pointer over the warning icon and read the tooltip. Note that a collision occurs when you try to import an intrusion rule that has the same SID/revision number as an existing rule. You should always make sure that updated versions of custom rules have new revision numbers; for more best practices, see Best Practices for Importing Local Intrusion Rules, on page 11. New/modified screens: We added a warning icon to **System** > **Updates** > **Rule Updates**.
Get Firepower Threat Defense upgrade packages from an internal web server	6.6.0	Firepower Threat Defense devices can now get upgrade packages from your own internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC. **Note** This feature is supported only for Firepower Threat Defense devices running Version 6.6.0+. It is not supported for upgrades *to* Version 6.6.0, nor is it supported for the FMC or Classic devices. New/modified screens: **System > Updates > Upload Update** button **> Specify software update source** option
FMC downloads and installs the latest VDB during initial setup	6.6.0	When you set up a new or reimaged FMC, the system automatically attempts to update the vulnerability database (VDB). This is a one-time operation. If the FMC has internet access, we recommend you schedule tasks to perform automatic recurring VDB update downloads and installations.
FMC schedules software downloads and GeoDB updates during initial setup	6.5.0	When you set up a new or reimaged FMC, the system automatically schedules: • A weekly task to download software updates for the FMC and its managed devices. • Weekly updates for the GeoDB. The tasks are scheduled in UTC, which means that when they occur locally depends on the date and your specific location. Also, because tasks 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 tasks occur one hour “later” in the summer than in the winter, according to local time. We recommend you review the auto-scheduled configurations and adjust them if necessary.

Feature	Version	Details
FMC upgrades postpone scheduled tasks	6.7.0 6.6.3 6.4.0.10	FMC upgrades now postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. **Note** Before you begin any upgrade, you must still make sure running tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. Note that this feature is supported for all upgrades *from* a supported version. This includes Version 6.4.0.10 and later patches, Version 6.6.3 and later maintenance releases, and Version 6.7.0+. This feature is not supported for upgrades *to* a supported version from an unsupported version.
Signed SRU, VDB, and GeoDB updates	6.4.0	So Firepower can verify that you are using the correct update files, the system now uses *signed* updates for intrusion rules (SRU), the vulnerability database (VDB), and the geolocation database (GeoDB). Earlier versions continue to use unsigned updates. Unless you manually download updates from the Cisco Support & Download site—for example, in an air-gapped deployment—you should not notice any difference in functionality. If, however, you do manually download and install SRU, VDB, and GeoDB updates, make sure you download the correct package for your current version. Signed update files begin with 'Cisco' instead of 'Sourcefire,' and terminate in .sh.REL.tar instead of .sh: • SRU: Cisco_Firepower_SRU-*date-build*-vrt.sh.REL.tar • VDB: Cisco_VDB_Fingerprint_Database-4.5.0-*version*.sh.REL.tar • GeoDB: Cisco_GEODB_Update-*date-build*.sh.REL.tar Do not untar signed (.tar) packages.
Faster upgrade	6.4.0	Improvements to the event database mean that upgrading Firepower appliances is now faster.
Copy upgrade packages to managed devices before the upgrade	6.2.3	You can now copy (or push) an upgrade package from the FMC to a managed device before you run the actual upgrade. This is useful because you can push during times of low bandwidth use, outside of the upgrade maintenance window. When you push to high availability, clustered, or stacked devices, the system sends the upgrade package to the active/control/primary first, then to the standby/data/secondary. New/modified screens: **System** > **Updates**

Feature	Version	Details
FMC warns of Snort restart before VDB updates	6.2.3	The FMC now warns you that Vulnerability Database (VDB) updates restart the Snort process. This interrupts traffic inspection and, depending on how the managed device handles traffic, possibly interrupts traffic flow. You can cancel the install until a more convenient time, such as during a maintenance window. These warnings can appear: • After you download and manually install a VDB. • When you create a scheduled task to install the VDB. • When the VDB installs in the background, such as during a previously scheduled task or as part of a Firepower software upgrade.