Updating ASA FirePOWER Module Software

Cisco electronically distributes several different types of updates, including major and minor updates to the ASA FirePOWER module software itself, as well as rule updates, geolocation database (GeoDB) updates, and Vulnerability Database (VDB) updates.

Caution This section contains general information on updating the ASA FirePOWER module. Before you update, including the VDB, GeoDB, or intrusion rules, you **must** read the release notes or advisory text that accompanies the update. The release notes provide important information, including prerequisites, warnings, and specific installation and uninstallation instructions.

Unless otherwise documented in the release notes or advisory text, updating does not modify configurations; the settings remain intact.

See the following sections for more information:

Understanding Update Types

License: Any

Cisco electronically distributes several different types of updates, including major and minor updates to the ASA FirePOWER module software itself, as well as intrusion rule updates and VDB updates.

The following table describes the types of updates provided by Cisco. For most update types, you can schedule their download and installation; see Scheduling Tasks, page 31-1 and Using Recurring Rule Updates, page 35-12.

Table 35-1 ASA FirePOWER Module Update Types

Update Type	Description	Schedule?	Uninstall?
patches	Patches include a limited range of fixes (and usually change the fourth digit in the version number; for example, 5.4.0.1).	yes	yes
feature updates	Feature updates are more comprehensive than patches and generally include new features (and usually change the third digit in the version number; for example, 5.4.1).	yes	yes
major updates (major and minor version releases)	Major updates, sometimes referred to as upgrades, include new features and functionality and may entail large-scale changes (and usually change the first or second digit in the version number; for example, 5.3 or 5.4).	no	no
VDB	VDB updates affect the database of known vulnerabilities to which hosts may be susceptible.	yes	no
intrusion rules	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.	yes	no
geolocation database (GeoDB)	GeoDB updates provide updated information on physical locations, connection types, and so on that your system can associate with detected routable IP addresses. You can use geolocation data as a condition in access control rules. You must install the GeoDB to view geolocation details.	yes	no

Note that while you can uninstall patches and other minor updates, you cannot uninstall major updates or return to previous versions of the VDB, GeoDB, or intrusion rules. If you updated to a new major version and you need to revert to an older version, contact Support.

Performing Software Updates

License: Any

There are a few basic steps to updating. First, you **must** prepare for the update by reading the release notes and completing any required pre-update tasks. Then, you can begin the update. You must verify the update's success. Finally, complete any required post-update steps.

For more information, see the following sections:

- Planning for the Update, page 35-2
- Understanding the Update Process, page 35-3
- Updating the ASA FirePOWER Module Software, page 35-4
- Monitoring the Status of Major Updates, page 35-6

Planning for the Update

License: Any

Before you begin the update, you must thoroughly read and understand the release notes, which you can download from the Support Site. The release notes describe new features and functionality, and known and resolved issues. The release notes also contain important information on prerequisites, warnings, and specific installation and uninstallation instructions.

The following sections provide an overview of some of the factors you must consider when planning for the update.

Software Version Requirements

You must make sure you are running the correct software version. The release notes indicate the required version. If you are running an earlier version, you can obtain updates from the Support Site.

Time and Disk Space Requirements

Make sure you have enough free disk space and allow enough time for the update. The release notes indicate space and time requirements.

Configuration Backup Guidelines

Before you begin a major update, Cisco recommends that you delete any backups that reside on the ASA FirePOWER module after copying them to an external location. Regardless of the update type, you should also back up current configuration data to an external location. See Using Backup and Restore, page 37-1.

When to Perform the Update

Because the update process may affect traffic inspection and traffic flow, and because the Data Correlator is disabled while an update is in progress, Cisco recommends you perform the update in a maintenance window or at a time when the interruption will have the least impact.

Understanding the Update Process

License: Any

You use the ASA FirePOWER module interface to update the ASA FirePOWER module.

The Product Updates page (**Configuration > ASA FirePOWER Configuration > Updates**) shows the version of each update, as well as the date and time it was generated. It also indicates whether a software reboot is required as part of the update. When you upload updates obtained from Support, they appear on the page. Uninstallers for patch and feature updates also appear; see Uninstalling Software Updates, page 35-7. The page can also list VDB updates.

Tip For patches and feature updates, you can take advantage of the automated update feature; see Automating Software Updates, page 31-6.

Traffic Flow and Inspection

When you install or uninstall updates, the following capabilities may be affected:

- traffic inspection, including application and user awareness and control, URL filtering, Security Intelligence filtering, intrusion detection and prevention, and connection logging
- traffic flow

The Data Correlator does not run during system updates. It resumes when the update is complete.

The manner and duration of network traffic interruption depends on how yourASA FirePOWER module is configured and deployed, and whether the update reboots the ASA FirePOWER module. For specific information on how and when network traffic is affected for a particular update, see the release notes.

Using the ASA FirePOWER Module During the Update

Regardless of the type of update, do **not** use the ASA FirePOWER module to perform tasks other than monitoring the update.

To prevent you from using the ASA FirePOWER module during a major update, and to allow you to easily monitor a major update's progress, the system streamlines the ASA FirePOWER module interface. You can monitor a minor update's progress in the task queue (**Monitoring > ASA FirePOWER Monitoring > Task Status**). Although you are not prohibited from using the ASA FirePOWER module during a minor update, Cisco recommends against it.

Even for minor updates, the ASA FirePOWER module may become unavailable during the update process. This is expected behavior. If this occurs, wait until you can again access the ASA FirePOWER module. If the update is still running, you **must** continue to refrain from using the ASA FirePOWER module until the update has completed. Note that while updating, the ASA FirePOWER module may reboot a second time; this is also expected behavior.

Caution If you encounter issues with the update (for example, if the update has failed or if a manual refresh of the Update Status page shows no progress), do **not** restart the update. Instead, contact Support.

After the Update

You **must** complete all of the post-update tasks listed in the release notes to ensure that your deployment is performing properly.

The most important post-update task is to reapply access control policies. Note that applying an access control policy may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected; see Applying an Access Control Policy, page 4-10.

Additionally, you should:

- verify that the update succeeded
- update your intrusion rules, VDB, and GeoDB, if necessary
- make any required configuration changes, based on the information in the release notes
- perform any additional post-update tasks listed in the release notes

Updating the ASA FirePOWER Module Software

License: Any

Update the ASA FirePOWER module software in one of two ways, depending on the type of update and whether your ASA FirePOWER module has access to the Internet:

- You can obtain the update directly from the Support Site if your ASA FirePOWER module has access to the Internet. This option is **not** supported for major updates.
- You can manually download the update from the Support Site and then upload it to the ASA FirePOWER module. Choose this option if your ASA FirePOWER module does not have access to the Internet or if you are performing a major update.

For major updates, updating the ASA FirePOWER module removes uninstallers for previous updates.

To update the ASA FirePOWER Module Software:

Step 1 Read the release notes and complete any required pre-update tasks.

Pre-update tasks may include making sure that: the ASA FirePOWER module is running the correct version of the Cisco software, you have enough free disk space to perform the update, you set aside adequate time to perform the update, you backed up configuration data, and so on.

Step 2 Upload the update. You have two options, depending on the type of update and whether your ASA FirePOWER module has access to the Internet:

- For all except major updates, and if your ASA FirePOWER module has access to the Internet, select **Configuration > ASA FirePOWER Configuration > Updates**, then click **Download Updates** to check for the latest updates on either of the following Support Sites:
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)
- For major updates, or if your ASA FirePOWER module does not have access to the Internet, you must first manually download the update from either of the following Support Sites:
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)
- Select **Configuration > ASA FirePOWER Configuration > Updates**, then click **Upload Update**. Click **Choose File** to navigate to and select the update and click **Upload**.

Note Download the update directly from the Support Site, either manually or by clicking **Download Updates** on the Product Updates tab. If you transfer an update file by email, it may become corrupted.

The update is uploaded.

Step 3 Select **Monitoring > ASA FirePOWER Monitoring > Task Status** to view the task queue and make sure that there are no jobs in process.

Tasks that are running when the update begins are stopped and cannot be resumed; you must manually delete them from the task queue after the update completes. The task queue automatically refreshes every 10 seconds. You must wait until any long-running tasks are complete before you begin the update.

Step 4 Select **Configuration > ASA FirePOWER Configuration > Updates**.

The Product Updates page appears.

Step 5 Click the install icon next to the update you uploaded.

The update process begins. How you monitor the update depends on whether the update is a major or minor update. See the ASA FirePOWER Module Update Types table and the release notes to determine your update type:

- For minor updates, you can monitor the update's progress in the task queue (**Monitoring > ASA FirePOWER Monitoring > Task Status**).
- For major updates, you can begin monitoring the update’s progress in the task queue. However, after the ASA FirePOWER module completes its necessary pre-update checks, you are locked out of the module interface. When you regain access, the Upgrade Status page appears. See Monitoring the Status of Major Updates, page 35-6 for information.

⚠ **Caution** Regardless of the update type, do **not** use the ASA FirePOWER module to perform tasks other than monitoring the update until the update has completed and, if necessary, the ASA FirePOWER module reboots. For more information, see Using the ASA FirePOWER Module During the Update, page 35-4.

Step 6 After the update finishes, access the ASA FirePOWER module interface and refresh the page. Otherwise, the interface may exhibit unexpected behavior. If you are the first user to access the interface after a major update, the End User License Agreement (EULA) may appear. You must review and accept the EULA to continue.

Step 7 If the rule update available on the Support Site is newer than the rules on your ASA FirePOWER module, import the newer rules.

For more information, see Importing Rule Updates and Local Rule Files, page 35-9.

Step 8 Reapply access control policies.

Applying an access control policy may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see Applying an Access Control Policy, page 4-10.

Step 9 If the VDB available on the Support Site is newer than the most recently installed VDB, install the latest VDB.

Installing a VDB update causes a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see Updating the Vulnerability Database, page 35-8.

Monitoring the Status of Major Updates

License: Any

For major updates, the ASA FirePOWER module provides you with a streamlined interface so that you can easily monitor the update process. The streamlined interface also prevents you from using the ASA FirePOWER module to perform tasks other than monitoring the update.You can begin monitoring the update’s progress in the task queue (**Monitoring > ASA FirePOWER Monitoring > Task Status**). However, after the ASA FirePOWER module completes its necessary pre-update checks, you are locked out of the user interface until a streamlined update page appears.

The streamlined interface displays the version you are updating from, the version you are updating to, and the time that has elapsed since the update began. It also displays a progress bar and gives details about the script currently running.

Tip Click **show log for current script** to see the update log. Click **hide log for current script** to hide the log again.

If the update fails for any reason, the page displays an error message indicating the time and date of the failure, which script was running when the update failed, and instructions on how to contact Support. Do **not** restart the update.

⚠ **Caution** If you encounter any other issue with the update (for example, if a manual refresh of the page shows no progress for an extended period of time), do **not** restart the update. Instead, contact Support.

When the update completes, the ASA FirePOWER module displays a success message and reboots. After the ASA FirePOWER module finishes rebooting, complete any required post-update steps.

Uninstalling Software Updates

License: Any

When you apply a patch or feature update, the update process creates an uninstaller that allows you to remove the update.

When you uninstall an update, the resulting Cisco software version depends on the update path. For example, consider a scenario where you updated directly from Version 5.0 to Version 5.0.0.2. Uninstalling the Version 5.0.0.2 patch might result in Version 5.0.0.1, even though you never installed the Version 5.0.0.1 update. For information on the resulting Cisco software version when you uninstall an update, see the release notes.

Note Uninstalling is not supported for major updates. If you updated to a new major version and you need to revert to an older version, contact Support.

Traffic Flow and Inspection

Uninstalling an update may affect traffic inspection and traffic flow. For specific information on how and when network traffic is affected for a particular update, see the release notes.

After the Uninstallation

After you uninstall the update, verify that the uninstall succeeded. For specific information for each update, see the release notes.

To uninstall a patch or feature update:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Updates**.

The Product Updates page appears.

Step 2 Click the install icon next to the uninstaller for the update you want to remove.

If prompted, confirm that you want to uninstall the update and reboot the ASA FirePOWER module.

The uninstall process begins. You can monitor its progress in the task queue (**Monitoring > ASA FirePOWER Monitoring > Task Status**).

Caution Do **not** use the ASA FirePOWER module interface to perform tasks until the uninstall has completed and, if necessary, the ASA FirePOWER module reboots. For more information, see Using the ASA FirePOWER Module During the Update, page 35-4.

Step 3 Refresh the page. Otherwise, the interface may exhibit unexpected behavior.

Updating the Vulnerability Database

License: Any

The Cisco Vulnerability Database (VDB) is a database of known vulnerabilities to which hosts may be susceptible. The Cisco Vulnerability Research Team (VRT) issues periodic updates to the VDB. To update the VDB, use the Product Updates page.

Note Installing a VDB update with detection updates may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected.You may want to schedule the update during low system usage times to minimize the impact of any system downtime.

Note After you complete a VDB update, reapply any out-of-date access control policy. Keep in mind that installing a VDB or reapplying an access control policy can cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see Applying an Access Control Policy, page 4-10.

This section explains how to plan for and perform manual VDB updates.

To update the vulnerability database:

Step 1 Read the VDB Update Advisory Text for the update.

The advisory text includes information about the changes to the VDB made in the update.

Step 2 Select **Configuration > ASA FirePOWER Configuration > Updates**.

The Product Updates page appears.

Step 3 Upload the update:

- If your ASA FirePOWER module has access to the Internet, click **Download Updates** to check for the latest updates on either of the following Support Sites:
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)
- If your ASA FirePOWER module does not have access to the Internet, manually download the update from one of the following Support Sites, then click **Upload Update**. Click **Choose File** to navigate to and select the update and click **Upload**:
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

Note Download the update directly from the Support Site either manually or by clicking **Download Updates**. If you transfer an update file by email, it may become corrupted.

The update is uploaded.

Step 4 Click the install icon next to the VDB update.

The Install Update page appears.

Step 5 Click **Install**.

Caution The update process begins. You can monitor the update's progress in the task queue (**Monitoring > ASA FirePOWER Monitoring > Task Status**). If you encounter issues with the update (for example, if the task queue indicates that the update has failed) **do not** restart the update. Instead, contact Support.

You must reapply any out-of-date access control policies for the VDB update to take effect; see Applying an Access Control Policy, page 4-10.

Importing Rule Updates and Local Rule Files

License: Any

As new vulnerabilities become known, the Cisco Vulnerability Research Team (VRT) releases rule updates that you can first import onto your ASA FirePOWER module, then implement by applying affected access control, network analysis, and intrusion policies.

Rule updates are cumulative, and Cisco recommends you always import the latest update. You cannot import a rule update that either matches or predates the version of the currently installed rules.

Note Rule updates may contain new binaries, so make sure your process for downloading and installing them complies with your security policies. In addition, rule updates may be large, so import rules during periods of low network use.

A 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.

Understanding When Rule Updates Modify Policies

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 reapply 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. For more information, see Allowing Rule Updates to Modify a System-Provided Base Policy, page 12-4.

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. For more information, see Resolving Conflicts and Committing Policy Changes, page 11-15.

Reapplying Policies

For changes made by a rule update to take affect, you must reapply any modified policies. When importing a rule update, you can configure the system to automatically reapply intrusion or access control policies. This is especially useful if you allow the rule update to modify system-provided base policies.

- Reapplying an access control policy also reapplies associated network analysis and file policies, but does **not** reapply intrusion policies. It also updates the default values for any modified advanced settings. Because you cannot apply a network analysis policy independently, you **must** reapply access control policies if you want to update preprocessor settings in network analysis policies.
- Reapplying intrusion policies allows you to update rules and other changed intrusion policy settings. You can reapply intrusion policies in conjunction with access control policies, or you can apply only intrusion policies to update intrusion rules without updating any other access control configurations.

When a rule update includes shared object rules, applying an access control or intrusion policy for the first time after the import causes a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information on applying access control and intrusion policies, including requirements, other effects, and recommendations, see Applying an Access Control Policy, page 4-10.

For more information on importing rule updates, see:

- Using One-Time Rule Updates, page 35-10 explains how to import a single rule update from the Support Site.
- Using Recurring Rule Updates, page 35-12 explains how to use an automated feature to download and install rule updates from the Support Site.
- Importing Local Rule Files, page 35-14 explains how to import a copy of a standard text rules file that you have created on a local machine.
- Viewing the Rule Update Log, page 35-15 explains the rule update log.

Using One-Time Rule Updates

License: Any

There are two methods that you can use for one-time rule updates:

- Using Manual One-Time Rule Updates, page 35-10 explains how to manually download a rule update from the Support Site and then manually install the rule update.
- Using Automatic One-Time Rule Updates, page 35-12 explains how to use an automated feature to search the Support Site for new rule updates and upload them.

Using Manual One-Time Rule Updates

License: Any

The following procedure explains how to import a new rule update manually. This procedure is especially useful if your ASA FirePOWER module does not have Internet access.

To manually import a rule update:

Step 1 From a computer that can access the Internet, access either of the following sites:

- **Sourcefire:** (https://support.sourcefire.com/)
- **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

Step 2 Click **Download**, then click **Rules**.

Step 3 Navigate to the latest rule update.

Rule updates are cumulative; you cannot import a rule update that either matches or predates the version of the currently installed rules.

Step 4 Click the rule update file that you want to download and save it to your computer.

Step 5 Select **Configuration > ASA FirePOWER Configuration > Updates**, then select the **Rule Updates** tab.

The Rule Updates page appears.

Tip You can also click **Import Rules** on the Rule Editor page (**Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Rule Editor**).

Step 6 Optionally, click **Delete All Local Rules**, then click **OK** to move all user-defined rules that you have created or imported to the deleted folder. See Deleting Custom Rules, page 23-104 for more information.

Step 7 Select **Rule Update or text rule file to upload and install** and click **Choose File** to navigate to and select the rule update file.

Step 8 Optionally, reapply policies after the update completes:

- Select **Reapply intrusion policies after the rule update import completes** to automatically reapply intrusion policies. Choose only this option to update rules and other changed intrusion policy settings without having to update any other access control configurations you may have made. You **must** select this option to reapply intrusion policies in conjunction with access control policies; reapplying access control policies in this case does not perform a complete apply.
- Select **Reapply access control policies after the rule update import completes** to automatically reapply access control policies and their associated network analysis and file policies, but not intrusion policies. Selecting this option also updates the default values for any modified access control advanced settings. Because you cannot apply a network analysis policy independently of its parent access control policy, you **must** reapply access control policies if you want to update preprocessor settings in network analysis policies.

Step 9 Click **Import**.

The system installs the rule update and displays the Rule Update Log detailed view; see Understanding the Rule Update Import Log Detailed View, page 35-18. The system also applies policies as you specified in the previous step; see Applying an Access Control Policy, page 4-10 and Applying an Intrusion Policy, page 19-7.

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

Using Automatic One-Time Rule Updates

License: Any

The following procedure explains how to import a new rule update by automatically connecting to the Support Site. You can use this procedure only if the ASA FirePOWER module has Internet access.

To automatically import a rule update:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Updates**, then select the **Rule Updates** tab.

The Rule Updates page appears.

Tip You can also click **Import Rules** on the Rule Editor page (**Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Rule Editor**).

Step 2 Optionally, click **Delete All Local Rules**, then click **OK** to move all user-defined rules that you have created or imported to the deleted folder. See Deleting Custom Rules, page 23-104 for more information.

Step 3 Select **Download new Rule Update from the Support Site**.

Step 4 Optionally, reapply policies after the update completes:

- Select **Reapply intrusion policies after the rule update import completes** to automatically reapply intrusion policies. Choose only this option to update rules and other changed intrusion policy settings without having to update any other access control configurations you may have made. You **must** select this option to reapply intrusion policies in conjunction with access control policies; reapplying access control policies in this case does not perform a complete apply.
- Select **Reapply access control policies after the rule update import completes** to automatically reapply access control, network analysis, and file policies, but not intrusion policies. Selecting this option also updates the default values for any modified access control advanced settings. Because you cannot apply a network analysis policy independently of its parent access control policy, you **must** reapply access control policies if you want to update preprocessor settings in network analysis policies.

Step 5 Click **Import**.

The system installs the rule update and displays the Rule Update Log detailed view; see Understanding the Rule Update Import Log Detailed View, page 35-18. The system also applies policies as you specified in the previous step; see Applying an Access Control Policy, page 4-10 and Applying an Intrusion Policy, page 19-7.

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

Using Recurring Rule Updates

License: Any

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

Applicable subtasks in the rule update import occur in the following order: download, install, base policy update, and policy reapply. When one subtask completes, the next subtask begins. Note that you can only apply policies previously applied by the ASA FirePOWER module where the recurring import is configured.

To schedule recurring rule updates:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Updates**, then select the **Rule Updates** tab.

The Rule Updates page appears.

Tip You can also click **Import Rules** on the Rule Editor page (**Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Rule Editor**).

Step 2 Optionally, click **Delete All Local Rules**, then click **OK** to move all user-defined rules that you have created or imported to the deleted folder. See Deleting Custom Rules, page 23-104 for more information.

Step 3 Select **Enable Recurring Rule Update Imports**.

The page expands to display options for configuring recurring imports. Import status messages appear beneath the **Recurring Rule Update Imports** section heading. Recurring imports are enabled when you save your settings.

Tip To disable recurring imports, clear the **Enable Recurring Rule Update Imports** check box and click **Save**.

Step 4 In the **Import Frequency** field, select **Daily**, **Weekly**, or **Monthly** from the drop-down list.

If you selected a weekly or monthly import frequency, use the drop-down lists that appear to select the day of the week or month when you want to import rule updates. Select from a recurring task drop-down list either by clicking or by typing the first letter or number of your selection one or more times and pressing Enter.

Step 5 In the **Import Frequency** field, specify the time when you want to start your recurring rule update import.

Step 6 Optionally, reapply policies after the update completes:

- Select **Reapply intrusion policies after the rule update import completes** to automatically reapply intrusion policies. Choose only this option to update rules and other changed intrusion policy settings without having to update any other access control configurations you may have made. You **must** select this option to reapply intrusion policies in conjunction with access control policies; reapplying access control policies in this case does not perform a complete apply.
- Select **Reapply access control policies after the rule update import completes** to automatically reapply access control policies and their network analysis and file policies, but not intrusion policies. Selecting this option also updates the default values for any modified access control advanced settings. Because you cannot apply a network analysis policy independently of its parent access control policy, you **must** reapply access control policies if you want to update preprocessor settings in network analysis policies.

Step 7 Click **Save** to enable recurring rule update imports using your settings.

The status message under the Recurring Rule Update Imports section heading changes to indicate that the rule update has not yet run. At the scheduled time, the system installs the rule update and applies policies as you specified in the previous step; see Applying an Access Control Policy, page 4-10 and Applying an Intrusion Policy, page 19-7.

You can log off or perform other tasks before or during the import. When accessed during an import, the Rule Update Log displays a red status icon (❗), 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. For more information, see Viewing the Rule Update Log, page 35-15.

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

Importing Local Rule Files

License: Any

A local 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.

Note the following regarding importing local rules:

- The text file name can include alphanumeric characters, spaces, and no special characters other than underscore (_), period (.), and dash (-).
- You do not have to specify a Generator ID (GID); if you do, you can specify only GID 1 for a standard text rule or 138 for a sensitive data rule.
- Do **not** specify a Snort ID (SID) or revision number when importing a rule for the first time; 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.
- You **must** include the SID assigned by the system and a revision number greater than the current revision number when importing an updated version of a local rule that you have previously imported.

  To view the revision number for a current local rule, display the Rule Editor page, click on the local rule category to expand the folder, then click **Edit** next to the rule.
- You can reinstate a local rule that you have deleted by importing the rule using the SID assigned by the system and a revision number greater than the current revision number. Note that the system automatically increments the revision number when you delete a local rule; this is a device that allows you to reinstate local rules.

  To view the revision number for a deleted local rule, display the Rule Editor page, click on the deleted rule category to expand the folder, then click **Edit** next to the rule.
- You cannot import a rule file that includes a rule with a SID greater than 2147483647; the import will fail.
- If you import a rule that includes a list of source or destination ports that is longer than 64 characters, the import will fail.
- 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. See Setting Rule States, page 20-19 for more information.
- You must make sure that the rules in the file do not contain any escape characters.
- The rules importer requires that all custom rules are imported in ASCII or UTF-8 encoding.

- All imported local rules are automatically saved in the local rule category.
- All deleted local rules are moved from the local rule category to the deleted rule category.
- The system imports local rules preceded with a single pound character (#).
- The system ignores local rules preceded with two pound characters (##) and does not import them.
- 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. See Configuring Event Thresholding, page 20-21 for more information.

To import local rule files:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Update**, then select the **Rule Updates** tab.

The Rule Updates page appears.

Step 2 Select **Rule Update or text rule file to upload and install** and click **Choose File** to navigate to the rule file. Note that all rules uploaded in this manner are saved in the local rule category.

Tip You can import **only** plain text files with ASCII or UTF-8 encoding.

Step 3 Click **Import**.

The rule file is imported. Make sure you enable the appropriate rules in your intrusion policies. The rules are not activated until the next time you apply the affected policies.

Note The system does **not** use the new rule set for inspection until after you apply your intrusion policies. See Applying an Access Control Policy, page 4-10 for procedures.

Viewing the Rule Update Log

License: Any

The ASA FirePOWER module 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. Actions you can take in the Rule Update Log are described in the following table.

Table 35-2 Rule Update Log Actions

To...	You can...
learn more about the contents of the columns in the table	find more information in Understanding the Rule Update Log Table, page 35-16.
delete an import file record from the import log, including detailed records for all objects included with the file	click the delete icon (🗑) next to the file name for the import file. **Note** Deleting the file from the log does not delete any object imported in the import file, but only deletes the import log records.
view details for each object imported in a rule update or local rule file	click the view icon (🔍) next to the file name for the import file.

See the following sections for more information:

- Understanding the Rule Update Log Table, page 35-16 describes the fields in the list of rule updates and local rule files that you import.
- Viewing Rule Update Import Log Details, page 35-17 describes the detailed record for each object imported in a rule update or local rule file.
- Understanding the Rule Update Import Log Detailed View, page 35-18 describes each field in the Rule Update Log detailed view.

To view the Rule Update Log:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Updates**, then select the **Rule Updates** tab.

The Rule Updates page appears.

Tip You can also click **Import Rules** on the Rule Editor page (**Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Rule Editor**).

Step 2 Click **Rule Update Log**.

The Rule Update Log page appears. This page lists each imported rule update and local rule file.

Understanding the Rule Update Log Table

License: Any

The fields in the list of rule updates and local rule files that you import are described in the following table.

Table 35-3 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.
User ID	The user name of the user that triggered the import.
Status	Whether the import: • succeeded (✓) • failed or is currently in progress (!) **Tip** 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.

Click the view icon (🔍) next to the rule update or file name to view the Rule Update Log detailed page for the rule update or local rule file, or click the delete icon (🗑) to delete the file record and all detailed object records imported with the file.

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

Viewing Rule Update Import Log Details

License: Any

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.

The following table describes specific actions you can perform on a Rule Update Import Log detailed view.

Table 35-4 Rule Update Import Log Detailed View Actions

To...	You can...
learn more about the contents of the columns in the table	find more information in Understanding the Rule Update Import Log Detailed View, page 35-18.

To view the Rule Update Import Log Detailed View:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Updates**, then select the **Rule Updates** tab.

The Rule Updates page appears.

Tip You can also click **Import Rules** on the Rule Editor page (**Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Rule Editor**).

Step 2 Click **Rule Update Log**.

The Rule Update Log page appears.

Step 3 Click the view icon (🔍) next to the file whose detailed records you want to view.

The table view of detailed records appears.

Understanding the Rule Update Import Log Detailed View

License: Any

You can view a detailed record for each object imported in a rule update or local rule file. The fields in the Rule Update Log detailed view are described in the following table.

Table 35-5 Rule Update Import Log Detailed View Fields

Field	Description
Time	The time and date the import began.
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.
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 intrusion policies after the Rule Update import completes** option was enabled for the import)
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 ASA FirePOWER module) • `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 system-provided policy) • `disabled` (for rules, the rule has been disabled in a system-provided policy) • `drop` (for rules, the rule has been set to Drop and Generate Events in a system-provided policy) • `error` (for a rule update or local rule file, the import failed) • `apply` (the **Reapply intrusion 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.
GID	The generator ID for a rule. For example, `1` (standard text rule) or `3` (shared object rule).
SID	The SID for a rule.
Rev	The revision number for a rule.

Table 35-5 Rule Update Import Log Detailed View Fields (continued)

Field	Description
Policy	For imported rules, this field displays `All`, which indicates that the imported rule was included in all system-provided intrusion policies. For other types of imported objects, this field is blank.
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.
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.

Updating the Geolocation Database

License: Any

The Cisco Geolocation Database (GeoDB) is a database of geographical data associated with routable IP addresses. The ASA FirePOWER module provides the country and continent. When your system detects GeoDB information that matches a detected IP address, you can view the geolocation information associated with that IP address. Cisco issues periodic updates to the GeoDB.

To update the GeoDB, use the Geolocation Updates page (**Configuration > ASA FirePOWER Configuration > Updates > Geolocation Updates**). When you upload GeoDB updates, they appear on this page.

The installation usually takes 30 to 40 minutes. 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.

This section explains how to plan for and perform manual GeoDB updates. You can also take advantage of the automated update feature to schedule GeoDB updates; for more information, see Automating Geolocation Database Updates, page 31-5.

To update the geolocation database:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Updates**.

The Product Updates page appears.

Step 2 Click the **Geolocation Updates** tab.

The Geolocation Updates page appears.

Step 3 Upload the update.

- If your ASA FirePOWER module has access to the Internet, click **Download and install geolocation update from the Support Site** to check for the latest updates on either of the following Support Sites:
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)
- If your ASA FirePOWER module does not have access to the Internet, manually download the update from either of the Support Sites, then click **Upload and install geolocation update**. Click **Choose File** to navigate to and select the update and click **Import**:
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

Note Download the update directly from the Support Site, either manually or by clicking **Download and install geolocation update from the Support Site** on the Geolocation Updates page. If you transfer an update file by email, it may become corrupted.

The update process begins. The average duration of update installation is 30 to 40 minutes. You can monitor the update's progress in the task queue (**Monitoring > ASA FirePOWER Monitoring > Task Status**).

Step 4 After the update finishes, return to the Geolocation Updates page to confirm that the GeoDB build number matches the update you installed.

The GeoDB update overrides any previous versions of the GeoDB and is effective immediately. Although it may take a few minutes for a GeoDB update to take effect throughout your deployment, you do not have to reapply access control policies after you update.