Updating System Software

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

Caution

This chapter contains general information on updating the FireSIGHT System. Before you update any part of the FireSIGHT System, 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 supported platforms, compatibility, prerequisites, warnings, and specific installation and uninstallation instructions. Unless otherwise documented in the release notes or advisory text, updating an appliance does not modify its configuration; the settings on the appliance remain intact.

See the following sections for more information:

- Understanding Update Types, page 66-1
- Performing Software Updates, page 66-2
- Uninstalling Software Updates, page 66-11
- Updating the Vulnerability Database, page 66-13
- Importing Rule Updates and Local Rule Files, page 66-15
- Updating the Geolocation Database, page 66-28

Understanding Update Types

License: Any

Cisco electronically distributes several different types of updates, including major and minor updates to the system 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 62-1 and Using Recurring Rule Updates, page 66-19.
Performing Software Updates

License: Any

There are a few basic steps to updating your FireSIGHT System deployment. 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 — first update your Defense Centers, then the devices they manage. You must monitor the update’s progress until it completes, then verify the update’s success. Finally, complete any required post-update steps.

For more information, see the following sections:
- Planning for the Update, page 66-3
- Understanding the Update Process, page 66-3
- Updating a Defense Center, page 66-6
- Updating Managed Devices, page 66-9

Note that while you can uninstall patches and other minor updates to the FireSIGHT System, you cannot uninstall major updates or return to previous versions of the VDB, GeoDB, or intrusion rules. If you updated your appliance to a new major version of the FireSIGHT System, and you need to revert to an older version, contact Support.
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 supported platforms, new features and functionality, known and resolved issues, and product compatibility. 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.

FireSIGHT System Version Requirements

You must make sure your appliances (including software-based devices) are running the correct version of the FireSIGHT System. The release notes indicate the required version. If you are running an earlier version, you can obtain updates from the Support Site.

Operating System Requirements

Make sure the computers where you installed software-based devices are running the correct versions of their operating systems. The release notes indicate the required versions. For information on supported operating systems for virtual devices, see the FireSIGHT System Virtual Installation Guide. For information on supported operating systems for Cisco NGIPS for Blue Coat X-Series, see the Cisco NGIPS for Blue Coat X-Series Installation Guide.

Time and Disk Space Requirements

Make sure you have enough free disk space and allow enough time for the update. When you update a managed device, the update requires additional disk space on the Defense Center. The release notes indicate space and time requirements.

Configuration and Event Backup Guidelines

Before you begin a major update, Cisco recommends that you delete any backups that reside on the appliance after copying them to an external location. Regardless of the update type, you should also back up current event and configuration data to an external location. Event data is not backed up as part of the update process.

You can use the Defense Center to back up event and configuration data for itself and the devices it manages; see Using Backup and Restore, page 70-1.

When to Perform the Update

Because the update process may affect traffic inspection, traffic flow, and link state, 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 on your deployment.

Understanding the Update Process

License: Any

The following diagram summarizes the update process.
Order of Update

You **must** update your Defense Centers before you can update the devices they manage.

Use the Defense Center to Perform the Update

Cisco recommends that you use the Defense Center's web interface to update not only itself, but also the devices it manages. You **must** use the Defense Center to update managed devices that do not have a web interface, such as virtual devices and Cisco NGIPS for Blue Coat X-Series. For major updates to Cisco NGIPS for Blue Coat X-Series, you may need to uninstall the previous version and install the new version. See the *Cisco NGIPS for Blue Coat X-Series Installation Guide* for more information.

The Product Updates page (**System > Updates**) shows the version of each update, as well as the date and time it was generated. It also indicates whether a reboot is required as part of the update.

When you upload updates obtained from Support to your appliance, they appear on the page. Uninstallers for patch and feature updates also appear; see *Uninstalling Software Updates, page 66-11*. On the Defense Center, the page can list VDB updates.
For patches and feature updates, you can take advantage of the automated update feature; see Automating Software Updates, page 62-11.

**Updating Paired Defense Centers**

When you begin to update one Defense Center in a high availability pair, the other Defense Center in the pair becomes the primary, if it is not already. In addition, the paired Defense Centers stop sharing configuration information; paired Defense Centers do not receive software updates as part of the regular synchronization process.

To ensure continuity of operations, do **not** update paired Defense Centers at the same time. First, complete the update procedure for the secondary Defense Centers, then update the primary.

**Updating Clustered Devices**

When you install an update on clustered devices or clustered stacks, the system performs the update on the devices or stacks one at a time. When the update starts, the system first applies it to the backup device or stack, which goes into maintenance mode until any necessary processes restart and the device or stack is processing traffic again. The system then applies the update to the active device or stack, which follows the same process.

To update devices in a clustered stack, you must perform the update from the managing Defense Center on all members of a cluster at once; you cannot perform the upgrade directly from the devices.

**Updating Stacked Devices**

When you install an update on stacked devices, the system performs the updates simultaneously. Each device resumes normal operation when the update completes. Note that:

- If the primary device completes the update before all of the secondary devices, the stack operates in a limited, mixed-version state until all devices have completed the update.
- If the primary device completes the upgrade after all of the secondary devices, the stack resumes normal operation when the update completes on the primary device.

**Traffic Flow and Inspection**

When you install or uninstall updates from a managed device, 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, including switching, routing, and related functionality
- link state

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 the components of the FireSIGHT System that the update affects, how your devices are configured and deployed, and whether the update reboots the device. For specific information on how and when network traffic is affected for a particular update, see the release notes.

**Tip**

When you update clustered devices, the system performs the updates one at a time to avoid traffic interruption.
Chapter 66  Updating System Software

Performing Software Updates

Using the Web Interface During the Update

Regardless of the type of update, do not use the web interface of the appliance you are updating to perform tasks other than monitoring the update.

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

Tip

To monitor updates to its managed devices, use the task queue on the Defense Center.

Even for minor updates, the web interface on the updating appliance may become unavailable during the update process, or the appliance may log you out. This is expected behavior. If this occurs, log in again to view the task queue. If the update is still running, you must continue to refrain from using the web interface until the update has completed. Note that while updating, managed devices may reboot a second time; this is also expected behavior.

Caution

If you encounter issues with the update (for example, if the web interface indicates that the update has failed or if a manual refresh of the task queue or 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, both after you update the Defense Center and then again after you update its managed devices.

Caution

When you apply an access control policy, resource demands may result in a small number of packets dropping without inspection. Additionally, applying some configurations requires the Snort process to restart, which temporarily interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. See Applying an Access Control Policy, page 12-15 and Configurations that Restart the Snort Process, page 1-7.

Additionally, you should:

• verify that the update succeeded
• make sure that all appliances in your deployment are communicating successfully
• 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 a Defense Center

License: Any
Performing Software Updates

Update the Defense Center in one of two ways, depending on the type of update and whether your Defense Center has access to the Internet:

- You can use the Defense Center to obtain the update directly from the Support Site, if your Defense Center 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 Defense Center. Choose this option if your Defense Center does not have access to the Internet or if you are performing a major update.

⚠️ **Caution**

To ensure continuity of operations, do not update paired Defense Centers at the same time; see Updating Paired Defense Centers, page 66-5.

For major updates, updating the Defense Center removes uninstallers for previous updates.

**To update the Defense Center**

**Access:** Admin

---

**Step 1**

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

Pre-update tasks may include making sure that: the Defense Center 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 event and configuration data, and so on.

**Step 2**

Upload the update to the Defense Center. You have two options, depending on the type of update and whether your Defense Center has access to the Internet:

- For all except major updates, and if your Defense Center has access to the Internet, select **System > Updates**, then click **Download Updates** to check for the latest updates. For major updates, or if your Defense Center does not have access to the Internet, you must first manually download the update.

  - Download the updates from either of the following Support Sites:
    - For all Sourcefire updates: [https://support.sourcefire.com/](https://support.sourcefire.com/)
    - For Cisco updates:
  - Select **System > Updates**, then click **Upload Update**. Browse to 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 to the Defense Center.

**Step 3**

Make sure that the appliances in your deployment are successfully communicating and that there are no issues being reported by the health monitor.

**Step 4**

Select **System > 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 5**

Select **System > Updates**.
Performing Software Updates

The Product Updates page appears.

**Step 6**
Click the install icon next to the update you uploaded.

The Install Update page appears.

**Step 7**
Select the Defense Center and click **Install**. If prompted, confirm that you want to install the update and reboot the Defense Center.

The update process begins. How you monitor the update depends on whether the update is a major or minor update. See the FireSIGHT System 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 (**System > Monitoring > Task Status**).
- For major updates, you can begin monitoring the update’s progress in the task queue. However, after the Defense Center completes its necessary pre-update checks, you are logged out. When you log back in, the Upgrade Status page appears. See Monitoring the Status of Major Updates, page 66-10 for information.

**Caution**
Regardless of the update type, do not use the web interface to perform tasks other than monitoring the update until the update has completed and, if necessary, the Defense Center reboots. For more information, see Using the Web Interface During the Update, page 66-6.

**Step 8**
After the update finishes, if necessary, log into the Defense Center.

If you are the first user to log in after a major update, the End User License Agreement (EULA) may appear. You must review and accept the EULA to continue.

**Step 9**
Clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.

**Step 10**
Select **Help > About** and confirm that the software version is listed correctly. Also note the versions of the rule update and VDB on the Defense Center; you will need this information later.

**Step 11**
Verify that all managed devices are successfully communicating with the Defense Center.

**Step 12**
If the rule update available on the Support Site is newer than the rules on your Defense Center, import the newer rules.

For more information, see Importing Rule Updates and Local Rule Files, page 66-15.

**Step 13**
Reapply access control policies.

When you apply an access control policy, resource demands may result in a small number of packets dropping without inspection. Additionally, applying some configurations requires the Snort process to restart, which temporarily interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. See Applying an Access Control Policy, page 12-15 and Configurations that Restart the Snort Process, page 1-7.

**Step 14**
If the VDB available on the Support Site is newer than the VDB on your Defense Center, install the latest VDB.

**Caution**
Installing a VDB update restarts the Snort process when you apply your access control policy, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. See How Snort Restarts Affect Traffic, page 1-9 and Updating the Vulnerability Database, page 66-13 for
more information.

**Step 15** Continue with the next section, Updating Managed Devices, to update Cisco software on the devices that the Defense Center manages.

---

## Updating Managed Devices

**License:** Any

After you update your Defense Centers, Cisco recommends that you use them to update the devices they manage. You **must** use the Defense Center to update managed devices that do not have a web interface, such as virtual devices and Cisco NGIPS for Blue Coat X-Series. For major updates to Cisco NGIPS for Blue Coat X-Series, you may need to uninstall the previous version and install the new version.

Updating managed devices is a two-step process. First, download the update from either of the following Support Sites and upload it to the managing Defense Center:

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

Next, install the software.

---

**Note** Traffic inspection, traffic flow, and link state may be affected during the update, depending on how your devices are configured and deployed, the components that the update affects, and whether the update reboots the devices. For specific information on how and when network traffic is affected for a particular update, see the release notes for that update.

---

**To update managed devices:**

**Access:** Admin

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

Pre-update tasks may include updating your managing Defense Center, backing up event and configuration data, and making sure that the devices are running the correct version of the Cisco software, that computers where you installed software-based devices are running the correct version of their operating systems, that you have enough free disk space to perform the update, that you have set aside adequate time to perform the update, and so on.

**Step 2** Update the FireSIGHT System software on the devices’ managing Defense Center; see Updating a Defense Center, page 66-6.

**Step 3** Download the update from either of the following Support Sites:

- For all Sourcefire updates: [https://support.sourcefire.com/](https://support.sourcefire.com/)
- For Cisco updates:

Different device models may use different updates. For information on the updates you can download, see the release notes.
Performing Software Updates

Step 4  Make sure that the appliances in your deployment are successfully communicating and that there are no issues being reported by the health monitor.

Step 5  On the managing Defense Center, select **System > Updates**.

The Product Updates page appears.

Step 6  Click **Upload Update** to browse to the update you downloaded, then click **Upload**.

The update is uploaded to the Defense Center. The Product Updates tab shows the type of update you just uploaded, its version number, and the date and time when it was generated. The page also indicates whether a reboot is required as part of the update.

Step 7  Click the install icon next to the update you are installing.

The Install Update page appears.

Step 8  Select the devices where you want to install the update, then click **Install**; you can update multiple devices at once if they use the same update. If prompted, confirm that you want to install the update and reboot the devices.

The update process begins. Depending on the size of the file, it may take some time to install the update on all devices. You can monitor the update's progress in the Defense Center's task queue (**System > Monitoring > Task Status**). Note that managed devices may reboot twice during the update; this is normal.

Caution  If you encounter issues with the update (for example, if the task queue indicates that the update has failed or if a manual refresh of the task queue shows no progress), do not restart the update. Instead, contact Support.

Step 9  Optionally, after a major update, log in to the device’s local web interface.

If you are the first user to log in after a major update, the End User License Agreement (EULA) may appear. You must review and accept the EULA to continue. Note that the EULA also appears, and must be accepted, if your first login is via the command line interface rather than the web interface.

Step 10  On the Defense Center, select **Devices > Device Management** and confirm that the devices you updated have the correct version listed.

Step 11  Verify that the devices you updated are successfully communicating with the Defense Center.

Step 12  Reapply access control policies.

When you apply an access control policy, resource demands may result in a small number of packets dropping without inspection. Additionally, applying some configurations requires the Snort process to restart, which temporarily interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. See **Applying an Access Control Policy**, page 12-15 and **Configurations that Restart the Snort Process**, page 1-7.

---

**Monitoring the Status of Major Updates**

**License:** Any
For major updates, the FireSIGHT System provides you with a streamlined web interface so that you can easily monitor the update process. The streamlined interface also prevents you from using the web interface to perform tasks other than monitoring the update.

You can begin monitoring the update’s progress in the task queue (System > Monitoring > Task Queue). However, after the appliance completes its necessary pre-update checks, you and all other users are logged out of the web interface. Unless you are an administrator or a maintenance user, you cannot log back in until the update is complete.

For administrators, when you log back in, the streamlined update page appears.

When using a Defense Center to update a managed device, Cisco recommends that you monitor the update’s progress from the Defense Center’s task queue. Note, however, that if you attempt to log into the device’s local web interface after the appliance finishes its pre-update checks, the streamlined update page appears and you can use it to monitor the update’s progress.

The page displays the version of the FireSIGHT System 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 appliance displays a success message and reboots. After the appliance finishes rebooting, refresh the page to log in and complete any required post-update steps.

Uninstalling Software Updates

License: Any

When you apply a patch or feature update to a Cisco appliance, the update process creates an uninstaller that allows you to remove the update from that appliance, using its web interface.

When you uninstall an update, the resulting Cisco software version depends on the update path for your appliance. For example, consider a scenario where you updated an appliance directly from Version 5.0 to Version 5.0.0.2. Uninstalling the Version 5.0.0.2 patch might result in an appliance running 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 from the web interface is not supported for major updates. If you updated your appliance to a new major version of the FireSIGHT System and you need to revert to an older version, contact Support.
Uninstalling Software Updates

Chapter 66      Updating System Software

Order of Uninstallation
Uninstall the update in the reverse order that you installed it. That is, first uninstall the update from managed devices, then from Defense Centers.

Use the Local Web Interface to Uninstall the Update
You must use the local web interface to uninstall updates; you cannot use the Defense Center to uninstall updates from managed devices. For information on uninstalling a patch from a device that does not have a local web interface (for example, virtual devices or Cisco NGIPS for Blue Coat X-Series), see the release notes.

Note that, although you can use this process to uninstall minor updates for Cisco NGIPS for Blue Coat X-Series, you cannot use this process to uninstall the Cisco NGIPS for Blue Coat X-Series application from the X-Series platform. For more information, see the Cisco NGIPS for Blue Coat X-Series Installation Guide.

Uninstalling the Update from Clustered or Paired Appliances
Clustered devices and Defense Centers in high availability pairs must run the same version of the FireSIGHT System. Although the uninstallation process triggers an automatic failover, appliances in mismatched pairs or clusters do not share configuration information, nor do they install or uninstall updates as part of their synchronization. If you need to uninstall an update from redundant appliances, plan to perform the uninstallations in immediate succession.

You cannot uninstall an update from devices in a clustered stack if uninstalling would revert these devices to a version in which clustered stacking is not supported.

To ensure continuity of operations, uninstall the update from clustered devices and paired Defense Centers one at a time. First, uninstall the update from the secondary appliance. Wait until the uninstallation process completes, then immediately uninstall the update from the primary appliance.

Caution
If the uninstallation process on a clustered device or paired Defense Center fails, do not restart the uninstall or change configurations on its peer. Instead, contact Support.

Uninstalling the Update from Stacked Devices
All devices in a stack must run the same version of the FireSIGHT System. Uninstalling the update from any of the stacked devices causes the devices in that stack to enter a limited, mixed-version state.

To minimize impact on your deployment, Cisco recommends that you uninstall an update from stacked devices simultaneously. The stack resumes normal operation when the update completes on all devices in the stack.

You cannot uninstall an update from devices in a clustered stack if uninstalling would revert these devices to a version in which clustered stacking is not supported.

Traffic Flow and Inspection
Uninstalling an update from managed devices may affect traffic inspection, traffic flow, and link state. 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, there are several steps you should take to ensure that your deployment is performing properly. These include verifying that the uninstall succeeded and that all appliances in your deployment are communicating successfully. For specific information for each update, see the release notes.
To uninstall a patch or feature update using the local web interface:

**Access:** Admin

**Step 1**
Select **System > Updates**.
The Product Updates page appears.

**Step 2**
Click the install icon next to the uninstaller for the update you want to remove.
- On the Defense Center, the Install Update page appears. Select the Defense Center and click **Install**.
- On a managed device, there is no intervening page.

In either case, if prompted, confirm that you want to uninstall the update and reboot the appliance.
The uninstall process begins. You can monitor its progress in the task queue (**System > Monitoring > Task Status**).

**Caution**
Do not use the web interface to perform tasks other than monitoring the update until the uninstall has completed and, if necessary, the appliance reboots. For more information, see Using the Web Interface During the Update, page 66-6.

**Step 3**
After the uninstall finishes, if necessary, log into the appliance.

**Step 4**
Clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.

**Step 5**
Select **Help > About** and confirm that the software version is listed correctly.

**Step 6**
Verify that the appliance where you uninstalled the patch is successfully communicating with its managed devices (for the Defense Center) or its managing Defense Center (for managed devices).

---

**Updating the Vulnerability Database**

**License:** Any

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 FireSIGHT System correlates the fingerprints with the vulnerabilities to help you determine whether a particular host increases your risk of network compromise. The Cisco Vulnerability Research Team (VRT) issues periodic updates to the VDB.

To update the VDB, use the Product Updates page on the Defense Center. When you upload VDB updates obtained from Support to your appliance, they appear on the page along with updates and uninstaller updates for the FireSIGHT System.

The time it takes to update vulnerability mappings depends on the number of hosts in your network map. You may want to schedule the update during low system usage times to minimize the impact of any system downtime. As a rule of thumb, divide the number of hosts on your network by 1000 to determine the approximate number of minutes to perform the update.
Updated application detectors and operating system fingerprints in the VDB require that you reapply access control policies before they can take effect. After you complete a VDB update, reapply any out-of-date access control policies to your managed devices. For more information, see Applying an Access Control Policy, page 12-15.

Installing a VDB update restarts the Snort process when you apply your access control policy, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. See How Snort Restarts Affect Traffic, page 1-9 and Updating the Vulnerability Database, page 66-13 for more information.

This section explains how to plan for and perform manual VDB updates. You can take advantage of the automated update feature to schedule VDB updates; see Automating Vulnerability Database Updates, page 62-15.

To update the vulnerability database:

Access: Admin

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, as well as product compatibility information.

Step 2 Select System > Updates.

The Product Updates page appears.

Step 3 Upload the update to the Defense Center:

- If your Defense Center has access to the Internet, click Download Updates to check for the latest updates one either of the following Support Sites:
  - Sourcefire: (https://support.sourcefire.com/)
  - Cisco: (http://www.cisco.com/cisco/web/support/index.html)

- If your Defense Center does not have access to the Internet, manually download the update from one of the following Support Sites, then click Upload Update. Browse to the update and click Upload:
  - Sourcefire: (https://support.sourcefire.com/)
  - Cisco: (http://www.cisco.com/cisco/web/support/index.html)

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

The Install Update page appears.

Step 5 Select the Defense Center, then click Install.

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 to the Defense Center.
The update process begins. Depending on the number of hosts in your network map, installing the update may take some time. You can monitor the update’s progress in the task queue (System > Monitoring > Task Status).

Caution

Do not use the web interface to perform tasks related to mapped vulnerabilities until the update has completed. If you encounter issues with the update (for example, if the task queue indicates that the update has failed or if a manual refresh of the task queue shows no progress) do not restart the update. Instead, contact Support.

Step 6

After the update finishes, select Help > About to confirm that the VDB build number matches the update you installed.

You must reapply any out-of-date access control policies for the VDB update to take effect; see Applying an Access Control Policy, page 12-15.

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 Defense Center, then implement by applying affected access control, network analysis, and intrusion policies to your managed devices.

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

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 24-4.

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 and the users who made those changes. For more information, see *Resolving Conflicts and Committing Policy Changes*, page 23-16.

Reapplying Policies

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

- Reapplying an access control policy also re-applies associated SSL, 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.

---

**Caution**

When you apply an access control or intrusion policy, resource demands may result in a small number of packets dropping without inspection. Additionally, applying some configurations requires the Snort process to restart. This includes applying an access control or intrusion policy after importing an intrusion rule update that includes a new or updated shared object rule. Restarting the Snort process temporarily interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. See *Configurations that Restart the Snort Process*, page 1-7 and *How Snort Restarts Affect Traffic*, page 1-9 for more information.

---

For more information on importing rule updates, see:

- **Using One-Time Rule Updates**, page 66-17 explains how to import a single rule update from the Support Site.

- **Using Recurring Rule Updates**, page 66-19 explains how to use an automated feature on the web interface to download and install rule updates from the Support Site.

- **Importing Local Rule Files**, page 66-20 explains how to import a copy of a standard text rules file that you have created on a local machine.
There are two methods that you can use for one-time rule updates:

- **Using Manual One-Time Rule Updates**, page 66-17 explains how to manually download a rule update from the Support Site to your local machine and then manually install the rule update.

- **Using Automatic One-Time Rule Updates**, page 66-18 explains how to use an automated feature on the web interface 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 Defense Center does not have Internet access.

**To manually import a rule update:**

**Access:** Admin

---

**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**
Log into your appliance’s web interface.

**Step 6**
Select **System > Updates**, then select the **Rule Updates** tab.

The Rule Updates page appears.

---

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

**Step 7**
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 36-107 for more information.

**Step 8**
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 9**
Optionally, reapply policies to your managed devices 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 SSL, 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 10** 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 66-25. The system also applies policies as you specified in the previous step; see **Applying an Access Control Policy**, page 12-15 and **Applying an Intrusion Policy**, page 31-8.

**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 appliance has Internet access.

**To automatically import a rule update:**

**Access:** Admin

**Step 1** Select **System > Updates**, then select the **Rule Updates** tab.

The Rule Updates page appears.

**Tip** You can also click **Import Rules** on the Rule Editor page (**Policies > Intrusion > 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 36-107 for more information.

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

**Step 4** Optionally, reapply policies to your managed devices 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.
Chapter 66      Updating System Software

Importing Rule Updates and Local Rule Files

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 66-25. The system also applies policies as you specified in the previous step; see Applying an Access Control Policy, page 12-15 and Applying an Intrusion Policy, page 31-8.

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

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 appliance where the recurring import is configured.

To schedule recurring rule updates:

Access: Admin

Step 1  Select System > Updates, then select the Rule Updates tab.

The Rule Updates page appears.

Tip  You can also click Import Rules on the Rule Editor page (Policies > Intrusion > 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 36-107 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.

- Select Reapply access control policies after the rule update import completes to automatically reapply access control policies and their associated SSL, 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.
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 to your managed devices 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 SSL, 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 12-15 and
Applying an Intrusion Policy, page 31-8.

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 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

**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](http://www.snort.org).

Note the following regarding importing local rules:

- The text file name can include alphanumerical 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 (Policies > Intrusion
> Rule Editor), 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 (Policies > Intrusion
> Rule Editor), 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 32-20 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 (#), but they are flagged as
deleted.

- The system ignores local rules preceded with two pound characters (##) and does not import them.

- Cisco strongly recommends that you import local rules on the primary Defense Center in a High
Availability Pair to avoid SID numbering issues.

- 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 32-22 for more information.

To import local rule files:

Access: Admin

---

**Step 1**
Select Policies > Intrusion > Rule Editor.
The Rule Editor page appears.

**Step 2**
Click Import Rules.
The Import Rules page appears.

**Tip**
You can also select System > Updates, then select the Rule Updates tab.
Step 3

Select **Rule Update or text rule file to upload and install** and click **Browse** to navigate to your 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 4

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

Managed devices do not use the new rule set for inspection until after you apply their intrusion policies. See **Applying an Access Control Policy, page 12-15** for procedures.

Viewing the Rule Update Log

**License:** Any

The Defense 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 fields in the Rule Update Log are described in the following table.

<table>
<thead>
<tr>
<th>Table 66-2</th>
<th>Rule Update Log Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>To...</td>
<td>You can...</td>
</tr>
<tr>
<td>learn more about the contents of the columns in the table</td>
<td>find more information in <strong>Understanding the Rule Update Log Table, page 66-23</strong>.</td>
</tr>
<tr>
<td>delete an import file record from the import log, including detailed records for all objects included with the file</td>
<td>click the delete icon (✓) next to the file name for the import file. <strong>Note</strong> Deleting the file from the log does not delete any object imported in the import file, but only deletes the import log records.</td>
</tr>
<tr>
<td>view details for each object imported in a rule update or local rule file</td>
<td>click the view icon (✓) next to the file name for the import file.</td>
</tr>
</tbody>
</table>

See the following sections for more information:

- **Understanding the Rule Update Log Table, page 66-23** describes the fields in the list of rule updates and local rule files that you import.

- **Viewing Rule Update Import Log Details, page 66-24** 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 66-25** describes each field in the Rule Update Log detailed view.
• Searching the Rule Update Import Log, page 66-26 explains how you can search the import log for specific records or for all records matching the search criteria.

To view the Rule Update Log:

Access: Admin

---

Step 1
Select System > Updates, then select the Rule Updates tab.

The Rule Updates page appears.

Tip
You can also click Import Rules on the Rule Editor page, which you access by selecting Policies > Intrusion > 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 66-3 Rule Update Log Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>The name of the import file. If the import fails, a brief statement of the reason for the failure appears under the file name.</td>
</tr>
<tr>
<td>Time</td>
<td>The time and date that the import started.</td>
</tr>
<tr>
<td>User ID</td>
<td>The user name of the user that triggered the import.</td>
</tr>
<tr>
<td>Status</td>
<td>Whether the import:</td>
</tr>
<tr>
<td></td>
<td>• succeeded (✅)</td>
</tr>
<tr>
<td></td>
<td>• failed or is currently in progress (⚠️)</td>
</tr>
</tbody>
</table>

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 workflow page.

<table>
<thead>
<tr>
<th>Table 66-4</th>
<th>Rule Update Import Log Detailed View Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>To...</td>
<td>You can...</td>
</tr>
<tr>
<td>learn more about the contents of the columns in the table</td>
<td>find more information in Understanding the Rule Update Import Log Detailed View, page 66-25.</td>
</tr>
<tr>
<td>sort and constrain records on the current workflow page</td>
<td>find more information in Sorting Drill-Down Workflow Pages, page 58-34.</td>
</tr>
<tr>
<td>temporarily use a different workflow</td>
<td>click (switch workflows). For information on selecting workflows, see Selecting Workflows, page 58-16. For information on creating custom workflows, see Creating Custom Workflows, page 58-39.</td>
</tr>
<tr>
<td>bookmark the current page so that you can quickly return to it</td>
<td>click Bookmark This Page. For more information, see Using Bookmarks, page 58-37.</td>
</tr>
<tr>
<td>navigate to the bookmark management page</td>
<td>click View Bookmarks. For more information, see Using Bookmarks, page 58-37.</td>
</tr>
<tr>
<td>generate a report based on the data in the current view</td>
<td>click Report Designer. For more information, see Creating a Report Template from an Event View, page 57-9.</td>
</tr>
<tr>
<td>search the entire Rule Update Import Log database for rule update import records</td>
<td>click Search. From more information, see Searching the Rule Update Import Log, page 66-26.</td>
</tr>
<tr>
<td>open a search page prepopulated with the current single constraint</td>
<td>select Edit Search or Save Search next to Search Constraints. From more information, see the Table View and Drill-Down Page Features table.</td>
</tr>
</tbody>
</table>

To view the Rule Update Import Log Detailed View:
Access: Admin

Step 1
Select System > Updates, then select the Rule Updates tab.
The Rule Updates page appears.

Tip
You can also click Import Rules on the Rule Editor page, which you access by selecting Policies > Intrusion > 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 66-5  Rule Update Import Log Detailed View Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The time and date the import began.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the imported object, which for rules corresponds to the rule Message field, and for rule update components is the component name.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of imported object, which can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• rule update component (an imported component such as a rule pack or policy pack)</td>
</tr>
<tr>
<td></td>
<td>• rule (for rules, a new or updated rule; note that in Version 5.0.1 this value replaced the update value, which is deprecated)</td>
</tr>
<tr>
<td></td>
<td>• policy apply (the Reapply intrusion policies after the Rule Update import completes option was enabled for the import)</td>
</tr>
<tr>
<td>Action</td>
<td>An indication that one of the following has occurred for the object type:</td>
</tr>
<tr>
<td></td>
<td>• new (for a rule, this is the first time the rule has been stored on this appliance)</td>
</tr>
<tr>
<td></td>
<td>• 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)</td>
</tr>
<tr>
<td></td>
<td>• collision (for a rule update component or rule, import was skipped because its revision conflicts with an existing component or rule on the appliance)</td>
</tr>
<tr>
<td></td>
<td>• deleted (for rules, the rule has been deleted from the rule update)</td>
</tr>
<tr>
<td></td>
<td>• enabled (for a rule update edit, a preprocessor, rule, or other feature has been enabled in a default policy provided by Cisco)</td>
</tr>
<tr>
<td></td>
<td>• disabled (for rules, the rule has been disabled in a default policy provided by Cisco)</td>
</tr>
<tr>
<td></td>
<td>• drop (for rules, the rule has been set to Drop and Generate Events in a default policy provided by Cisco)</td>
</tr>
<tr>
<td></td>
<td>• error (for a rule update or local rule file, the import failed)</td>
</tr>
<tr>
<td></td>
<td>• apply (the Reapply intrusion policies after the Rule Update import completes option was enabled for the import)</td>
</tr>
<tr>
<td>Default Action</td>
<td>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.</td>
</tr>
<tr>
<td>GID</td>
<td>The generator ID for a rule. For example, 1 (standard text rule) or 3 (shared object rule). See Table 41-7 on page 41-39 for more information.</td>
</tr>
<tr>
<td>SID</td>
<td>The SID for a rule.</td>
</tr>
<tr>
<td>Rev</td>
<td>The revision number for a rule.</td>
</tr>
</tbody>
</table>
Searching the Rule Update Import Log

License: Any

Note: Beta Users: This feature will be fully explained in the final version of the documentation.

You can search the import log for specific records or for all records matching the search criteria. You may want to create customized searches and save them to reuse later.

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. See Specifying Time Constraints in Searches, page 60-5 for more information.

The search criteria you can use are described in the following table. Note that record searches are case-insensitive. For example, searching for RULE or rule yields the same results.

<table>
<thead>
<tr>
<th>Search Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Specify the date and time the record was generated. See Specifying Time Constraints in Searches, page 60-5 for the syntax for entering time.</td>
<td>&gt; 2006-01-15 13:30:00 returns all rule records imported after January 15, 2006 at 1:30 PM.</td>
</tr>
<tr>
<td>Name</td>
<td>Specify all or part of the content of the rule Message field. You can use an asterisk (*) as a wildcard character in this field.</td>
<td><em>dhcp</em> returns all rule records with DHCP in the Message field.</td>
</tr>
<tr>
<td>Type</td>
<td>Specify the type of record, which can be rule update component, rule, or policy apply. Note that you can use the update search value to search for rules imported prior to Version 5.0.1.</td>
<td>update returns imported rule update components such as a rule pack or policy pack; rule returns rule updates, including new rules; policy apply returns a table row of information for rule updates where intrusion policies were automatically reapplied following the update.</td>
</tr>
<tr>
<td>Action</td>
<td>Specify an action for the object you want to view. See the Rule Update Import Log Detailed View Fields table for a list of actions you can specify.</td>
<td>When the type is rule, new returns all rules imported for the first time on the appliance.</td>
</tr>
<tr>
<td>GID</td>
<td>Specify the generator ID for the rule.</td>
<td>3 returns all shared object rules.</td>
</tr>
<tr>
<td>SID</td>
<td>Specify a signature ID or a range of SIDs for a rule.</td>
<td>923 returns the record for the rule with the SID 923.</td>
</tr>
</tbody>
</table>
Importing Rule Updates and Local Rule Files

Table 66-6  Rule Update Import Log Search Criteria (continued)

<table>
<thead>
<tr>
<th>Search Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rev</td>
<td>Specify the revision number for the rule.</td>
<td>3 returns rules with the revision number 3.</td>
</tr>
<tr>
<td>Policy</td>
<td>Specify the default policy the rule is imported into.</td>
<td>All returns rules imported into all default policies.</td>
</tr>
<tr>
<td>Rule Update</td>
<td>Specify the Rule Update filename.</td>
<td>filename returns all records for the specified import file.</td>
</tr>
<tr>
<td>Details</td>
<td>Specify details on the imported object.</td>
<td>previously* returns the record for all rules that have changed.</td>
</tr>
</tbody>
</table>

For more information on searching, including how to load and delete saved searches, see Searching for Events, page 60-1.

To search the Rule Update Import Log:

Access: Admin/Intrusion Admin

Step 1 Select Analysis > Search.
The Search page appears.

Step 2 From the Table drop-down list, select Rule Update Import Log.
The page reloads with the appropriate constraints.

Tip
You can also click Search on the Rule Update Log detailed view; see Viewing Rule Update Import Log Details, page 66-24.

Step 3 Optionally, if you want to save the search, enter a name for the search in the Name field.
If you do not enter a name, the web interface automatically creates one when you save it.

Step 4 Enter your search criteria in the appropriate fields, as described in the Rule Update Import Log Search Criteria table. If you enter multiple criteria, the search returns the records that match all the criteria.

Step 5 If you want to save the search so that other users can access it, clear the Save As Private check box.
Otherwise, leave the check box selected to save the search as private.
If you want to use the search as a data restriction for a custom user role, you must save it as a private search.

Step 6 You have the following options:
- Click Search to start the search.
  Your search results appear in the default Rule Update Import Log detailed view workflow. To use a different workflow, including a custom workflow, click (switch workflows). For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3.
- Click Save if you are modifying an existing search and want to save your changes.
- Click Save as New Search to save the search criteria. The search is saved (and associated with your user account if you selected Save As Private) so that you can run it at a later time.
Updating the Geolocation Database

License: FireSIGHT

Supported Defense Centers: Any except DC500

The Cisco Geolocation Database (GeoDB) is a database of geographical data (such as country, city, coordinates, and so on) and connection-related data (such as Internet service provider, domain name, connection type, and so on) associated with routable IP addresses. When your system detects GeoDB information that matches a detected IP address, you can view the geolocation information associated with that IP address. You must install the GeoDB on your system to view any geolocation details other than country or continent. Cisco issues periodic updates to the GeoDB.

To update the GeoDB, use the Geolocation Updates page (System > Updates > Geolocation Updates) on the Defense Center. When you upload GeoDB updates you obtained from Support or from your appliance, they appear on this page.

Time needed to update the GeoDB depends on your appliance; 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 62-9. For more information on geolocation, see Using Geolocation, page 58-20.

To update the geolocation database:

Access: Admin

Step 1
Select System > Updates.

The Product Updates page appears.

Step 2
Click the Geolocation Updates tab.

The Geolocation Updates page appears.

Step 3
Upload the update to the Defense Center.

- If your Defense Center 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 Support Sites:
  - Sourcefire: (https://support.sourcefire.com/)
  - Cisco: (http://www.cisco.com/cisco/web/support/index.html)
- If your Defense Center does not have access to the Internet, manually download the update from either of the Support Sites, then click Upload and install geolocation update. Browse to 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; this may vary depending on your appliance hardware. You can monitor the update’s progress in the task queue (System > Monitoring > Task Status).

**Step 4** After the update finishes, return to the Geolocation Updates page or select Help > About 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. When you update the GeoDB, the Defense Center automatically updates its managed devices. 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.