



Updates

This chapter explains how to perform content updates.



Important

To upgrade the management center, or threat defense software or chassis, see the upgrade guide for the version that your *management center* is *currently* running: <https://cisco.com/go/ftd-fmc-upgrade-726>.

- [About System Updates, on page 1](#)
- [Requirements and Prerequisites for System Updates, on page 3](#)
- [Guidelines and Limitations for System Updates, on page 3](#)
- [Update the Vulnerability Database \(VDB\), on page 4](#)
- [Update the Geolocation Database \(GeoDB\), on page 5](#)
- [Update Intrusion Rules, on page 7](#)
- [Maintain Your Air-Gapped Deployment, on page 15](#)
- [History for System Updates, on page 15](#)

About System Updates

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

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

Table 1: Upgrades and Updates

Component	Description	Details
System software	<p><i>Major</i> software releases contain new features, functionality, and enhancements. They may include infrastructure or architectural changes.</p> <p><i>Maintenance</i> releases contain general bug and security related fixes. Behavior changes are rare, and are related to those fixes.</p> <p><i>Patches</i> are on-demand updates limited to critical fixes with time urgency.</p> <p><i>Hotfixes</i> can address specific customer issues.</p>	<p>Direct Download: Select patches and maintenance releases only, usually some time after the release is available for manual download. The length of the delay depends on release type, release adoption, and other factors. Both on-demand and scheduled downloads are supported.</p> <p>Note In Version 7.2.6, we begin support for on-demand direct download of all releases (except hotfixes). However, support for scheduled downloads of maintenance releases is discontinued. Note that this feature combination is reversed/not available in Version 7.3.x and 7.4.0. Support returns in Version 7.4.1.</p> <p>Schedule Install: Patches and maintenance releases only, as a scheduled task.</p> <p>Uninstall: Patches only.</p> <p>Revert: Major and maintenance releases for threat defense only. Revert is not supported for the management center or for Classic devices.</p> <p>Reimage: Major and maintenance releases only.</p> <p>See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</p>
Vulnerability database (VDB)	The Cisco vulnerability database (VDB) is a database of known vulnerabilities to which hosts may be susceptible, as well as fingerprints for operating systems, clients, and applications. The system uses the VDB to help determine whether a particular host increases your risk of compromise.	<p>Direct Download: Yes.</p> <p>Schedule: Yes, as a scheduled task.</p> <p>Uninstall: No.</p> <p>See: Update the Vulnerability Database (VDB), on page 4</p>
Geolocation database (GeoDB)	The Cisco geolocation database (GeoDB) maps IP addresses to countries/continents.	<p>Direct Download: Yes.</p> <p>Schedule: Yes, from its own update page</p> <p>Uninstall: No.</p> <p>See: Update the Geolocation Database (GeoDB), on page 5</p>
Intrusion rules (SRU/LSP)	<p>Intrusion rule updates provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings.</p> <p>Rule updates may also delete rules, provide new rule categories and default variables, and modify default variable values.</p>	<p>Direct Download: Yes.</p> <p>Schedule: Yes, from its own update page.</p> <p>Uninstall: No.</p> <p>See: Update Intrusion Rules, on page 7</p>

Component	Description	Details
Security Intelligence feeds	Security Intelligence feeds are collections of IP addresses, domain names, and URLs that you can use to quickly filter traffic that matches an entry.	Direct Download: Yes. Schedule: Yes, from the object manager. Uninstall: No. See: Cisco Secure Firewall Management Center Device Configuration Guide
URL categories and reputations	URL filtering allows you to control access to websites based on the URL's general classification (category) and risk level (reputation).	Direct Download: Yes. Schedule: Yes, when you configure integrations/cloud services, or as a scheduled task. Uninstall: No. See: Cisco Secure Firewall Management Center Device Configuration Guide

Requirements and Prerequisites for System Updates

Model Support

Any

Supported Domains

Global unless indicated otherwise.

User Roles

Admin

Guidelines and Limitations for System Updates

Before You Update

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

Scheduled Updates

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



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

Bandwidth Guidelines

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

Update the Vulnerability Database (VDB)

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

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

The initial setup on the management center automatically downloads and installs the latest VDB from Cisco as a one-time operation. Optionally, schedule tasks to download and install VDB updates and deploy configurations. For more information, see [Vulnerability Database Update Automation](#).

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

Schedule VDB Updates

If your management center has internet access, we recommend you schedule regular VDB updates. See [Vulnerability Database Update Automation](#).

Manually Update the VDB

Use this procedure to manually update the VDB.



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

In most cases, the first deploy after a VDB update restarts the Snort process, interrupting traffic inspection. The system warns you when this will happen (updated application detectors and operating system fingerprints require a restart; vulnerability information does not). Whether traffic drops or passes without further inspection during this interruption depends on how the targeted device handles traffic. For more information, see [Snort Restart Traffic Behavior](#).

Before you begin

If the management center cannot access the internet, get the update yourself: <https://www.cisco.com/go/firepower-software>. Select or search for your model (or choose any model—you use the same VDB for all management centers), then browse to the *Coverage and Content Updates* page.

Procedure

Step 1 Go to the VDB update page.

- Version 7.2.0–7.2.5: **System** (⚙) > **Updates** > **Content Updates**
- Version 7.2.6+: **System** (⚙) > **Content Updates** > **VDB Updates**

Step 2 Choose how you want to get the VDB onto the management center.

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

Note

In Version 7.2.0–7.2.5, clicking **Download Updates** also immediately gets the latest maintenance release and the latest critical patches for your deployment.

Step 3 Install the VDB.

- a) Click the **Install** icon next to the Vulnerability and Fingerprint Database update.
- b) Choose the management center.
- c) Click **Install**.

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

Step 4 Verify update success.

The VDB update page and **Help** (❓) > **About** both show the current version.

What to do next

Deploy configuration changes; see the [Cisco Secure Firewall Management Center Device Configuration Guide](#).

Update the Geolocation Database (GeoDB)

The geolocation database (GeoDB) is a database that you can leverage to view and filter traffic based on geographical location. We issue periodic updates to the GeoDB, and you must regularly update the GeoDB to have accurate geolocation information. As part of the initial configuration, the system schedules weekly

GeoDB updates. We recommend you review this task and make changes if necessary, as described in [Schedule GeoDB Updates, on page 6](#).

A GeoDB update overrides any previous versions. The management center automatically updates its managed devices, and unless the update adds new countries (this is rare) you do not need to redeploy. You can see your current version on **Help** (?) > **About**.



Note We no longer provide the geolocation IP package, which contained contextual data associated with routable IP addresses. This saves disk space and does not affect geolocation rules or traffic handling in any way. Any contextual data is now stale, and upgrading to most later versions deletes the IP package. Options to download the IP package or view contextual data have no effect, and are removed in later versions.

Schedule GeoDB Updates

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

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



Note The **IP Package Download** option available in some versions has no effect. We no longer provide an IP package. In later versions, this option is removed.

Before you begin

Make sure the management center can access the internet.

Procedure

-
- Step 1** Go to the GeoDB update page.
- Version 7.2.0–7.2.5: **System** (⚙) > **Updates** > **Geolocation Updates**
 - Version 7.2.6+: **System** (⚙) > **Content Updates** > **Geolocation Updates**
- Step 2** Under **Recurring Geolocation Updates**, check **Enable Recurring Weekly Updates...**
- Step 3** Specify the **Update Start Time**.
- Step 4** Click **Save**.
-

Manually Update the GeoDB

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



Note The **IP Package Download** option available in some versions has no effect. We no longer provide an IP package. In later versions, this option is removed.

Before you begin

If the management center cannot access the internet, get the update yourself: <https://www.cisco.com/go/firepower-software>. Select or search for your model (or choose any model—you use the same GeoDB for all management centers), then browse to the *Coverage and Content Updates* page.

Procedure

-
- Step 1** Go to the GeoDB update page.
- Version 7.2.0–7.2.5: **System** (⚙) > **Updates** > **Geolocation Updates**
 - Version 7.2.6+: **System** (⚙) > **Content Updates** > **Geolocation Updates**
- Step 2** Under **One-Time Geolocation Update**, choose how you want to update the GeoDB.
- Direct download: Choose **Download and install...**
 - Manual upload: Choose **Upload and install...**, then click **Choose File** and browse to the package you downloaded earlier.
- Step 3** Click **Import**.
- Monitor update progress in the Message Center.
- Step 4** Verify update success.
- The GeoDB update page and **Help** (❓) > **About** both show the current version.
-

What to do next

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

Update Intrusion Rules

As new vulnerabilities become known, the Talos Intelligence Group releases intrusion rule updates. These updates affect intrusion rules, preprocessor rules, and the policies that use the rules. Intrusion rule updates

are cumulative and we recommend you keep the system up to date. You cannot import an intrusion rule update that either matches or predates the version of the currently installed rules.

An intrusion rule update may provide the following:

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

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

Understanding When Intrusion Rule Updates Modify Policies

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

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

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

Deploying Intrusion Rule Updates

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

**Caution**

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

Recurring Intrusion Rule Updates

As part of the initial configuration, the system schedules daily intrusion rule updates. We recommend you review this task and make changes if necessary, as described in [Schedule Intrusion Rule Updates, on page 9](#). You may want to change the frequency, or enable automatic deploy after rule imports. For high availability management centers, you only need to import the update on the active unit.

Importing Local Intrusion Rules

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

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

Schedule Intrusion Rule Updates

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

Before you begin

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

Procedure

-
- | | |
|---------------|--|
| Step 1 | Go to the rule update page. <ul style="list-style-type: none">• Version 7.2.0–7.2.5: System (⚙) > Updates > Rule Updates• Version 7.2.6+: System (⚙) > Content Updates > Rule Updates |
| Step 2 | Under Recurring Rule Update Imports , check Enable Recurring Rule Update Imports . |
| Step 3 | Specify the Import Frequency and start time. |
| Step 4 | (Optional) Check Reapply all policies... to deploy after each update. |

Step 5 Click **Save**.

Manually Update Intrusion Rules

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

Before you begin

- Make sure your process for updating intrusion rules complies with your security policies.
- Consider the update's effect on traffic flow and inspection due to bandwidth constraints and Snort restarts. We recommend performing updates in a maintenance window.
- If the management center cannot access the internet, get the update yourself: <https://www.cisco.com/go/firepower-software>. Select or search for your model (or choose any model—you use the same update for all management centers), then browse to the *Coverage and Content Updates* page.

Procedure

Step 1 Go to the rule update page.

- Version 7.2.0–7.2.5: **System** (⚙) > **Updates** > **Rule Updates**
- Version 7.2.6+: **System** (⚙) > **Content Updates** > **Rule Updates**

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

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

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

Step 4 Click **Import**.

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

Step 5 Verify update success.

The rule update page and **Help** (❓) > **About** both show the current version.

What to do next

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

Import Local Intrusion Rules

Use this procedure to import local intrusion rules. Imported intrusion rules appear in the local rule category in a disabled state. You can perform this task in any domain.

Before you begin

- Make sure your local rule file follows the guidelines described in [Best Practices for Importing Local Intrusion Rules, on page 11](#).
- Make sure your process for importing local intrusion rules complies with your security policies.
- Consider the import's effect on traffic flow and inspection due to bandwidth constraints and Snort restarts. We recommend scheduling rule updates during maintenance windows.

Procedure

-
- | | |
|---------------|---|
| Step 1 | Go to the rule update page. <ul style="list-style-type: none">• Version 7.2.0–7.2.5: System (⚙) > Updates > Rule Updates• Version 7.2.6+: System (⚙) > Content Updates > Rule Updates• Any version: Click Import Rules in the intrusion rules editor (Objects > Intrusion Rules). |
| Step 2 | (Optional) Delete existing local rules. <p>Click Delete All Local Rules, then confirm that you want to move all created and imported intrusion rules to the deleted folder.</p> |
| Step 3 | Under One-Time Rule Update/Rules Import , choose Rule update or text rule file to upload and install , then click Choose File and browse to your local rule file. |
| Step 4 | Click Import . <p>You can monitor import progress in the Message Center. Even if the Message Center shows no progress for several minutes or indicates that the update has failed, do not restart the import. Instead, contact Cisco TAC.</p> |
-

What to do next

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

Best Practices for Importing Local Intrusion Rules

Observe the following guidelines when importing a local rule file:

- The rules importer requires that all custom rules are imported in a plain text file encoded in ASCII or UTF-8.

- The text file name can include alphanumeric characters, spaces, and no special characters other than underscore (_), period (.), and dash (-).
- The system imports local rules preceded with a single pound character (#), but they are flagged as deleted.
- The system imports local rules preceded with a single pound character (#), and does not import local rules preceded with two pound characters (##).
- Rules cannot contain any escape characters.
- In a multidomain deployment, the system assigns a GID of 1 to a rule imported into or created in the Global domain, and a domain-specific GID between 1000 and 2000 for all other domains.
- You do not have to specify a Generator ID (GID) when importing a local rule. If you do, specify only GID 1 for a standard text rule.
- When importing a rule for the first time, do *not* specify a Snort ID (SID) or revision number. This avoids collisions with SIDs of other rules, including deleted rules. The system will automatically assign the rule the next available custom rule SID of 1000000 or greater, and a revision number of 1.

If you must import rules with SIDs, a SID can be any unique number 1,000,000 or greater.

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

- When importing an updated version of a local rule you have previously imported, or when reinstating a local rule you have deleted, you *must* include the SID assigned by the system and a revision number greater than the current revision number. You can determine the revision number for a current or deleted rule by editing the rule.



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

- Import local rules on the primary management center in a high availability pair to avoid SID numbering issues.
- The import fails if a rule contains any of the following:
 - A SID greater than 2147483647.
 - A list of source or destination ports that is longer than 64 characters.
 - When importing into the Global domain in a multidomain deployment, a GID:SID combination uses GID 1 and a SID that already exists in another domain; this indicates that the combination existed before Version 6.2.1. You can reimport the rule using GID 1 and a unique SID.
- Policy validation fails if you enable an imported local rule that uses the deprecated `threshold` keyword in combination with the intrusion event thresholding feature in an intrusion policy.
- All imported local rules are automatically saved in the local rule category.
- The system always sets local rules that you import to the disabled rule state. You must manually set the state of local rules before you can use them in your intrusion policy.

View Intrusion Rule Update Logs

The system generates logs of rule updates/imports, listed by timestamp, user, and whether each update succeeded or failed. These logs contain detailed import information on all updated rules and components; see [Intrusion Rule Update Log Details, on page 13](#). Use this procedure to view rule import logs. Note that deleting an import log does not delete the imported objects. In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

Procedure

-
- Step 1** Go to the rule update page.
- Version 7.2.0–7.2.5: **System** (⚙) > **Updates** > **Rule Updates**
 - Version 7.2.6+: **System** (⚙) > **Content Updates** > **Rule Updates**
- Step 2** Click **Rule Update Log**.
- Step 3** (Optional) View details for any rule update by clicking **View** (👁) next to the log file.
-

Intrusion Rule Update Log Details

**Tip**

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

Table 2: Intrusion Rule Update Log Details

Field	Description
Action	<p>An indication that one of the following has occurred for the object type:</p> <ul style="list-style-type: none"> • <code>new</code> (for a rule, this is the first time the rule has been stored on this appliance) • <code>changed</code> (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) • <code>collision</code> (for a rule update component or rule, import was skipped because its revision conflicts with an existing component or rule on the appliance) • <code>deleted</code> (for rules, the rule has been deleted from the rule update) • <code>enabled</code> (for a rule update edit, a preprocessor, rule, or other feature has been enabled in a default policy provided with the system) • <code>disabled</code> (for rules, the rule has been disabled in a default policy provided with the system) • <code>drop</code> (for rules, the rule has been set to Drop and Generate Events in a default policy provided with the system) • <code>error</code> (for a rule update or local rule file, the import failed) • <code>apply</code> (the Reapply all policies after the rule update import completes option was enabled for the import)
Default Action	The default action defined by the rule update. When the imported object type is <code>rule</code> , the default action is <code>Pass</code> , <code>Alert</code> , or <code>Drop</code> . For all other imported object types, there is no default action.
Details	A string unique to the component or rule. For rules, the GID, SID, and previous revision number for a changed rule, displayed as <code>previously (GID:SID:Rev)</code> . This field is blank for a rule that has not changed.
Domain	The domain whose intrusion policies can use the updated rule. Intrusion policies in descendant domains can also use the rule. This field is only present in a multidomain deployment.
GID	The generator ID for a rule. For example, 1 (standard text rule, Global domain or legacy GID) or 3 (shared object rule).
Name	The name of the imported object, which for rules corresponds to the rule Message field, and for rule update components is the component name.
Policy	For imported rules, this field displays <code>All</code> . This means that the rule was imported successfully, and can be enabled in all appropriate default intrusion policies. For other types of imported objects, this field is blank.
Rev	The revision number for a rule.
Rule Update	The rule update file name.
SID	The SID for a rule.
Time	The time and date the import began.

Field	Description
Type	The type of imported object, which can be one of the following: <ul style="list-style-type: none">• <code>rule update component</code> (an imported component such as a rule pack or policy pack)• <code>rule</code> (for rules, a new or updated rule)• <code>policy apply</code> (the Reapply all policies after the rule update import completes option was enabled for the import)
Count	The count (1) for each record. The Count field appears in a table view when the table is constrained, and the Rule Update Log detailed view is constrained by default to rule update records. This field is not searchable.

Maintain Your Air-Gapped Deployment

If your management center is not connected to the internet, essential updates will not occur automatically. You must manually obtain and install these updates.

For more information, see:

- Software upgrade guides: <https://cisco.com/go/ftd-fmc-upgrade>
- [Manually Update the VDB, on page 4](#)
- [Manually Update Intrusion Rules, on page 10](#)
- [Manually Update the GeoDB, on page 7](#)

History for System Updates





Table 3: Version 7.2.10 Features

Feature	Minimum Management Center	Minimum Threat Defense	Details
Threat Defense Upgrade			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Threat defense and chassis upgrade wizards optimized for lower resolution screens.	7.2.10 7.6.0	Any	<p>We optimized the threat defense and chassis upgrade wizards for lower resolution screens (and smaller browser windows). Text appears smaller and certain screen elements are hidden. If you change your resolution or window size mid-session, you may need to refresh the page for the web interface to adjust. Note that the minimum screen resolution to use the management center is 1280 x 720.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Devices > Threat Defense Upgrade • Devices > Chassis Upgrade <p>Version restrictions: Not supported with Version 7.2.0–7.2.9, 7.3.x, 7.4.0–7.4.2.</p>

Table 4: Version 7.2.6 Features

Feature	Minimum Management Center	Minimum Threat Defense	Details
Upgrade			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Improved upgrade starting page and package management.	7.2.6 7.4.1	Any	<p>A new upgrade page makes it easier to choose, download, manage, and apply upgrades to your entire deployment. This includes the management center, threat defense devices, and any older NGIPSv/ASA FirePOWER devices. The page lists all upgrade packages that apply to your current deployment, with suggested releases specially marked. You can easily choose and direct-download packages from Cisco, as well as manually upload and delete packages.</p> <p>Internet access is required to retrieve the list/direct download upgrade packages. Otherwise, you are limited to manual management. Patches are not listed unless you have at least one appliance at the appropriate maintenance release (or you manually uploaded the patch). You must manually upload hotfixes.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • System() > Product Upgrades is now where you upgrade the management center and all managed devices, as well as manage upgrade packages. • System() > Content Updates is now where you update intrusion rules, the VDB, and the GeoDB. • Devices > Threat Defense Upgrade takes you directly to the threat defense upgrade wizard. • System() > Users > User Role > Create User Role > Menu-Based Permissions allows you to grant access to Content Updates (VDB, GeoDB, intrusion rules) without allowing access to Product Upgrades (system software). <p>Deprecated screens/options:</p> <ul style="list-style-type: none"> • System() > Updates is deprecated. All threat defense upgrades now use the wizard. • The Add Upgrade Package button on the threat defense upgrade wizard has been replaced by a Manage Upgrade Packages link to the new upgrade page. <p>Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0.</p>
Suggested release notifications.	7.2.6 7.4.1	Any	<p>The management center now notifies you when a new suggested release is available. If you don't want to upgrade right now, you can have the system remind you later, or defer reminders until the next suggested release. The new upgrade page also indicates suggested releases.</p> <p>Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0.</p> <p>See: Cisco Secure Firewall Management Center New Features by Release</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
Updated internet access requirements for direct-downloading software upgrades.	7.2.6 7.4.1	Any	<p>Upgrade impact. The system connects to new resources.</p> <p>The management center has changed its direct-download location for software upgrade packages from sourcefire.com to amazonaws.com.</p> <p>Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0.</p>
Threat Defense Upgrade			
Enable revert from the threat defense upgrade wizard.	7.2.6 7.4.1	Any, if upgrading to 7.1+	<p>You can now enable revert from the threat defense upgrade wizard.</p> <p>Other version restrictions: You must be upgrading threat defense to Version 7.1+. Not supported with management center Version 7.3.x or 7.4.0.</p>
Select devices to upgrade from the threat defense upgrade wizard.	7.2.6	Any	<p>Use the wizard to select devices to upgrade.</p> <p>You can now use the threat defense upgrade wizard to select or refine the devices to upgrade. On the wizard, you can toggle the view between selected devices, remaining upgrade candidates, ineligible devices (with reasons why), devices that need the upgrade package, and so on. Previously, you could only use the Device Management page and the process was much less flexible.</p>
View detailed upgrade status from the threat defense upgrade wizard.	7.2.6 7.4.1	Any	<p>The final page of the threat defense upgrade wizard now allows you to monitor upgrade progress. This is in addition to the existing monitoring capability on the Upgrade tab on the Device Management page, and on the Message Center. Note that as long as you have not started a new upgrade flow, Devices > Threat Defense Upgrade brings you back to this final wizard page, where you can view the detailed status for the current (or most recently complete) device upgrade.</p> <p>Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0.</p>
Unattended threat defense upgrades.	7.2.6	Any	<p>The threat defense upgrade wizard now supports unattended upgrades, using a new Unattended Mode menu. You just need to select the target version and the devices you want to upgrade, specify a few upgrade options, and step away. You can even log out or close the browser.</p>
Simultaneous threat defense upgrade workflows by different users.	7.2.6	Any	<p>We now allow simultaneous upgrade workflows by different users, as long as you are upgrading different devices. The system prevents you from upgrading devices already in someone else's workflow. Previously, only one upgrade workflow was allowed at a time across all users.</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
Skip pre-upgrade troubleshoot generation for threat defense devices.	7.2.6	Any	<p>You can now skip the automatic generating of troubleshooting files before major and maintenance upgrades by disabling the new Generate troubleshooting files before upgrade begins option. This saves time and disk space.</p> <p>To manually generate troubleshooting files for a threat defense device, choose System(⚙️) > Health > Monitor, click the device in the left panel, then View System & Troubleshoot Details, then Generate Troubleshooting Files.</p>
Management Center Upgrade			
New upgrade wizard for the management center.	7.2.6 7.4.1	Any	<p>A new upgrade starting page and wizard make it easier to perform management center upgrades. After you use System(⚙️) > Product Upgrades to get the appropriate upgrade package onto the management center, click Upgrade to begin.</p> <p>Other version restrictions: Only supported for management center upgrades from Version 7.2.6+/7.4.1+. Not supported for upgrades from Version 7.3.x or 7.4.0.</p> <p>See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</p>
Hotfix high availability management centers without pausing synchronization.	7.2.6 7.4.1	Any	<p>Unless otherwise indicated by the hotfix release notes or Cisco TAC, you do not have to pause synchronization to install a hotfix on high availability management centers.</p> <p>Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0.</p>
Content Updates			
Scheduled tasks download patches and VDB updates only.	7.2.6 7.4.1	Any	<p>Upgrade impact. Scheduled download tasks stop retrieving maintenance releases.</p> <p>The Download Latest Update scheduled task no longer downloads maintenance releases; now it only downloads the latest applicable patches and VDB updates. To direct-download maintenance (and major) releases to the management center, use System(⚙️) > Product Upgrades.</p> <p>Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0.</p>

Table 5: Version 7.2.0 Features

Feature	Details
Threat Defense Upgrade	

Feature	Details
Copy upgrade packages ("peer-to-peer sync") from device to device.	<p>Instead of copying upgrade packages to each device from the management center or internal web server, you can use the threat defense CLI to copy upgrade packages between devices ("peer to peer sync"). This secure and reliable resource-sharing goes over the management network but does not rely on the management center. Each device can accommodate 5 package concurrent transfers.</p> <p>This feature is supported for Version 7.2.x–7.4.x standalone devices managed by the same Version 7.2.x–7.4.x standalone management center. It is not supported for:</p> <ul style="list-style-type: none"> • Container instances. • Device high availability pairs and clusters. These devices get the package from each other as part of their normal sync process. Copying the upgrade package to one group member automatically syncs it to all group members. • Devices managed by high availability management centers. • Devices in different domains, or devices separated by a NAT gateway. • Devices upgrading from Version 7.1 or earlier, regardless of management center version. • Devices running Version 7.6+. <p>New/modified CLI commands: configure p2psync enable, configure p2psync disable, show peers, show peer details, sync-from-peer, show p2p-sync-status</p>
Auto-upgrade to Snort 3 after successful threat defense upgrade.	<p>When you use a Version 7.2+ management center to upgrade threat defense to Version 7.2+, you can now choose whether to Upgrade Snort 2 to Snort 3.</p> <p>After the software upgrade, eligible devices upgrade from Snort 2 to Snort 3 when you deploy configurations. For devices that are ineligible because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For help, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide for your version.</p> <p>Version restrictions: Not supported for threat defense upgrades to Version 7.0.x or 7.1.x.</p>
Upgrade for single-node clusters.	<p>You can now use the device upgrade page (Devices > Device Upgrade) to upgrade clusters with only one active node. Any deactivated nodes are also upgraded. Previously, this type of upgrade would fail. This feature is not supported from the system updates page (System(⚙️)Updates).</p> <p>Hitless upgrades are also not supported in this case. Interruptions to traffic flow and inspection depend on the interface configurations of the lone active unit, just as with standalone devices.</p> <p>Supported platforms: Firepower 4100/9300, Secure Firewall 3100</p>



Feature	Details
Revert threat defense upgrades from the CLI.	<p>You can now revert threat defense upgrades from the device CLI if communications between the management center and device are disrupted. Note that in high availability/scalability deployments, revert is more successful when all units are reverted simultaneously. When reverting with the CLI, open sessions with all units, verify that revert is possible on each, then start the processes at the same time.</p> <p>Caution Reverting from the CLI can cause configurations between the device and the management center to go out of sync, depending on what you changed post-upgrade. This can cause further communication and deployment issues.</p> <p>New/modified CLI commands: upgrade revert, show upgrade revert-info.</p>
Management Center Upgrade	
Management center upgrade does not automatically generate troubleshooting files.	<p>To save time and disk space, the management center upgrade process no longer automatically generates troubleshooting files before the upgrade begins. Note that device upgrades are unaffected and continue to generate troubleshooting files.</p> <p>To manually generate troubleshooting files for the management center, choose System() > Health > Monitor, click Firewall Management Center in the left panel, then View System & Troubleshoot Details, then Generate Troubleshooting Files.</p>

Table 6: Version 7.1.0 Features

Feature	Details
Threat Defense Upgrade	
Revert a successful device upgrade.	<p>You can now revert major and maintenance upgrades to FTD. Reverting returns the software to its state just before the last upgrade, also called a <i>snapshot</i>. If you revert an upgrade after installing a patch, you revert the patch as well as the major and/or maintenance upgrade.</p> <p>Important If you think you might need to revert, you must use System() > Updates to upgrade FTD. The System Updates page is the only place you can enable the Enable revert after successful upgrade option, which configures the system to save a revert snapshot when you initiate the upgrade. This is in contrast to our usual recommendation to use the wizard on the Devices > Device Upgrade page.</p> <p>This feature is not supported for container instances.</p> <p>Minimum FTD: 7.1</p>

Feature	Details
Improvements to the upgrade workflow for clustered and high availability devices.	<p>We made the following improvements to the upgrade workflow for clustered and high availability devices:</p> <ul style="list-style-type: none"> • The upgrade wizard now correctly displays clustered and high availability units as groups, rather than as individual devices. The system can identify, report, and preemptively require fixes for group-related issues you might have. For example, you cannot upgrade a cluster on the Firepower 4100/9300 if you have made unsynced changes on Firepower Chassis Manager. • We improved the speed and efficiency of copying upgrade packages to clusters and high availability pairs. Previously, the FMC copied the package to each group member sequentially. Now, group members can get the package from each other as part of their normal sync process. • You can now specify the upgrade order of data units in a cluster. The control unit always upgrades last.

Table 7: Version 7.0.0 Features

Feature	Details
Threat Defense Upgrade	
Improved FTD upgrade performance and status reporting.	FTD upgrades are now easier faster, more reliable, and take up less disk space. A new Upgrades tab in the Message Center provides further enhancements to upgrade status and error reporting.

Feature	Details
Easy-to-follow upgrade workflow for FTD devices.	<p>A new device upgrade page (Devices > Device Upgrade) on the FMC provides an easy-to-follow wizard for upgrading Version 6.4+ FTD devices. It walks you through important pre-upgrade stages, including selecting devices to upgrade, copying the upgrade package to the devices, and compatibility and readiness checks.</p> <p>To begin, use the new Upgrade Firepower Software action on the Device Management page (Devices > Device Management > Select Action).</p> <p>As you proceed, the system displays basic information about your selected devices, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If a device does not "pass" a stage in the wizard, it does not appear in the next stage.</p> <p>If you navigate away from wizard, your progress is preserved, although other users with Administrator access can reset, modify, or continue the wizard.</p> <p>Note</p> <p>You must still use System(⚙️) > Updates to upload or specify the location of FTD upgrade packages. You must also use the System Updates page to upgrade the FMC itself, as well as all non-FTD managed devices.</p> <p>Note</p> <p>In Version 7.0, the wizard does not correctly display devices in clusters or high availability pairs. Even though you must select and upgrade these devices as a unit, the wizard displays them as standalone devices. Device status and upgrade readiness are evaluated and reported on an individual basis. This means it is possible for one unit to appear to "pass" to the next stage while the other unit or units do not. However, these devices are still grouped. Running a readiness check on one, runs it on all. Starting the upgrade on one, starts it on all.</p> <p>To avoid possible time-consuming upgrade failures, <i>manually</i> ensure all group members are ready to move on to the next step of the wizard before you click Next.</p>
Upgrade more FTD devices at once.	<p>The number of devices you can upgrade at once is now limited by your management network bandwidth—not the system's ability to manage simultaneous upgrades. Previously, we recommended against upgrading more than five devices at a time.</p> <p>Important</p> <p>Only upgrades to FTD Version 6.7+ using the FTD upgrade wizard see this improvement. If you are upgrading devices to an older FTD release—even if you are using the new upgrade wizard—we still recommend you limit to five devices at a time.</p>
Upgrade different device models together.	<p>You can now use the FTD upgrade wizard to queue and invoke upgrades for all FTD models at the same time, as long as the system has access to the appropriate upgrade packages.</p> <p>Previously, you would choose an upgrade package, then choose the devices to upgrade using that package. That meant that you could upgrade multiple devices at the same time <i>only</i> if they shared an upgrade package. For example, you could upgrade two Firepower 2100 series devices at the same time, but not a Firepower 2100 series and a Firepower 1000 series.</p>

Table 8: Version 6.7.0 Features

Feature	Details
Threat Defense Upgrade	
Upgrades remove PCAP files to save disk space.	Upgrades now remove locally stored PCAP files. To upgrade, you must have enough free disk space or the upgrade fails.
Improved FTD upgrade status reporting and cancel/retry options.	<p>You can now view the status of FTD device upgrades and readiness checks in progress on the Device Management page, as well as a 7-day history of upgrade success/failures. The Message Center also provides enhanced status and error messages.</p> <p>A new Upgrade Status pop-up, accessible from both Device Management and the Message Center with a single click, shows detailed upgrade information, including percentage/time remaining, specific upgrade stage, success/failure data, upgrade logs, and so on.</p> <p>Also on this pop-up, you can manually cancel failed or in-progress upgrades (Cancel Upgrade), or retry failed upgrades (Retry Upgrade). Canceling an upgrade reverts the device to its pre-upgrade state.</p> <p>Note To be able to manually cancel or retry a failed upgrade, you must disable the new auto-cancel option, which appears when you use the FMC to upgrade an FTD device: Automatically cancel on upgrade failure and roll back to the previous version. With the option enabled, the device automatically reverts to its pre-upgrade state upon upgrade failure.</p> <p>Auto-cancel is not supported for patches. In an HA or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • System (gear icon) > Updates > Product Updates > Available Updates > Install icon for the FTD upgrade package • Devices > Device Management > Upgrade • Message Center > Tasks <p>New/modified CLI commands: show upgrade status detail, show upgrade status continuous, show upgrade status, upgrade cancel, upgrade retry</p>
Content Updates	

Feature	Details
Custom intrusion rule import warns when rules collide.	<p>The FMC now warns you of rule collisions when you import custom (local) intrusion rules. Previously, the system would silently skip the rules that cause collisions—with the exception of Version 6.6.0.1, where a rule import with collisions would fail entirely.</p> <p>On the Rule Updates page, if a rule import had collisions, a warning icon is displayed in the Status column. For more information, hover your pointer over the warning icon and read the tooltip.</p> <p>Note that a collision occurs when you try to import an intrusion rule that has the same SID/revision number as an existing rule. You should always make sure that updated versions of custom rules have new revision numbers.</p> <p>New/modified screens: We added a warning icon to System ⚙️ > Updates > Rule Updates.</p>

Table 9: Version 6.6.0 Features

Feature	Details
Threat Defense Upgrade	
Get FTD upgrade packages from an internal web server.	<p>FTD devices can now get upgrade packages from your own internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC.</p> <p>Note This feature is supported only for FTD devices running Version 6.6+. It is not supported for upgrades <i>to</i> Version 6.6, nor is it supported for the FMC or Classic devices.</p> <p>New/modified screens: We added a Specify software update source option to the page where you upload upgrade packages.</p>
Content Updates	
Automatic VDB update during initial setup.	<p>When you set up a new or reimaged FMC, the system automatically attempts to update the vulnerability database (VDB).</p> <p>This is a one-time operation. If the FMC has internet access, we recommend you schedule tasks to perform automatic recurring VDB update downloads and installations.</p>

Table 10: Version 6.5.0 Features

Feature	Details
Content Updates	

Feature	Details
Automatic software downloads and GeoDB updates.	<p>When you set up a new or reimaged FMC, the system automatically schedules:</p> <ul style="list-style-type: none"> • A weekly task to download software updates for the FMC and its managed devices. • Weekly updates for the GeoDB. <p>The tasks are scheduled in UTC, which means that when they occur locally depends on the date and your specific location. Also, because tasks are scheduled in UTC, they do not adjust for Daylight Saving Time, summer time, or any such seasonal adjustments that you may observe in your location. If you are affected, scheduled tasks occur one hour “later” in the summer than in the winter, according to local time. We recommend you review the auto-scheduled configurations and adjust them if necessary.</p>

Table 11: Version 6.4.0 Features

Feature	Details
Management Center Upgrade	
Upgrades postpone scheduled tasks.	<p>The management center upgrade process now postpones scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot.</p> <p>Note Before you begin any upgrade, you must still make sure running tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed.</p> <p>Note that this feature is supported for all upgrades <i>from</i> a supported version. This includes Version 6.4.0.10 and later patches, Version 6.6.3 and later maintenance releases, and Version 6.7.0+. This feature is not supported for upgrades <i>to</i> a supported version from an unsupported version.</p>
Content Updates	

Feature	Details
Signed SRU, VDB, and GeoDB updates.	<p>So the system can verify that you are using the correct update files, Version 6.4+ uses <i>signed</i> updates for intrusion rules (SRU), the vulnerability database (VDB), and the geolocation database (GeoDB). Earlier versions continue to use unsigned updates.</p> <p>Unless you manually download updates from the Cisco Support & Download site—for example, in an air-gapped deployment—you should not notice any difference in functionality. If, however, you do manually download and install SRU, VDB, and GeoDB updates, make sure you download the correct package for your current version.</p> <p>Signed update files begin with 'Cisco' instead of 'Sourcefire,' and terminate in .sh.REL.tar instead of .sh, as follows:</p> <ul style="list-style-type: none"> • SRU: Cisco_Firepower_SRU-date-build-vrt.sh.REL.tar • VDB: Cisco_VDB_Fingerprint_Database-4.5.0-version.sh.REL.tar • GeoDB: Cisco_GEODB_Update-date-build.sh.REL.tar <p>We will provide both signed and unsigned updates until the end-of-support for versions that require unsigned updates. Do not untar signed (.tar) packages. If you accidentally upload a signed update to an older FMC or ASA FirePOWER device, you must manually delete it. Leaving the package takes up disk space, and also may cause issues with future upgrades.</p>

Table 12: Version 6.2.3 Features

Feature	Details
Device Upgrade	
Copy upgrade packages to managed devices before the upgrade.	<p>You can now copy (or push) an upgrade package from the FMC to a managed device before you run the actual upgrade. This is useful because you can push during times of low bandwidth use, outside of the upgrade maintenance window.</p> <p>When you push to high availability, clustered, or stacked devices, the system sends the upgrade package to the active/control/primary first, then to the standby/data/secondary.</p> <p>New/modified screens: System ⚙️ > Updates</p>
Content Updates	
FMC warns of Snort restart before VDB updates.	<p>The FMC now warns you that Vulnerability Database (VDB) updates restart the Snort process. This interrupts traffic inspection and, depending on how the managed device handles traffic, possibly interrupts traffic flow. You can cancel the install until a more convenient time, such as during a maintenance window.</p> <p>These warnings can appear:</p> <ul style="list-style-type: none"> • After you download and manually install a VDB. • When you create a scheduled task to install the VDB. • When the VDB installs in the background, such as during a previously scheduled task or as part of a software upgrade.

Feature	Details
Deprecated: Geolocation details	We no longer provide the geolocation IP package, which contained contextual data associated with routable IP addresses. This saves disk space and does not affect geolocation rules or traffic handling in any way. Any contextual data is now stale, and upgrading to most later versions deletes the IP package. Options to download the IP package or view contextual data have no effect, and are removed in later versions.