Scheduling

The following topics explain how to schedule tasks:

About Task Scheduling

You can schedule various tasks to run at designated times, either once or on a recurring basis.

Tasks are scheduled in UTC on the back end, which means 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.

Some tasks are automatically scheduled or performed by the initial setup process:

- A one-time task to download and install the latest VDB.

- A weekly scheduled task to download the latest available software updates and VDB.

- A weekly scheduled task to perform a locally stored configuration-only backup of the management center.

You should review the weekly tasks and adjust if necessary. Optionally, schedule new recurring tasks to actually update the VDB and/or software, and deploy configurations.

👉

Important   We *strongly* recommend you review scheduled tasks to be sure they occur when you intend. Some tasks (such as those involving automated software updates or that require pushing updates to managed devices) may place a significant load on networks with low bandwidths. You should schedule tasks like these to run during periods of low network use. Other tasks, such as deploying configurations, can cause traffic interruptions. You should schedule tasks like these during maintenance windows.

Requirements and Prerequisites for Task Scheduling

Model Support

Any.

Supported Domains

Any

User Roles

- Admin

- Maintenance User

Configuring a Recurring Task

You set the frequency for a recurring task using the same process for all types of tasks.

Note that the time displayed on most pages on the web interface is the local time, which is determined by using the time zone you specify in your local configuration. Further, the management center automatically adjusts its local time display for daylight saving time (DST), where appropriate. However, recurring tasks that span the transition dates from DST to standard time and back do not adjust for the transition. That is, if you create a task scheduled for 2:00 AM during standard time, it will run at 3:00 AM during DST. Similarly, if you create a task scheduled for 2:00 AM during DST, it will run at 1:00 AM during standard time.

Procedure

Step 1   Select **System** (⚙) > **Tools** > **Scheduling**.

Step 2   Click **Add Task**.

Step 3   From the **Job Type** drop-down list, select the type of task that you want to schedule.

Step 4   Click **Recurring** next to the **Schedule task to run** option.

Step 5   In the **Start On** field, specify the date when you want to start your recurring task.

Step 6   In the **Repeat Every** field, specify how often you want the task to recur.

You can either type a number or click **Up** (▲) and **Down** (▼) to specify the interval. For example, type 2 and click **Days** to run the task every two days.

Step 7   In the **Run At** field, specify the time when you want to start your recurring task.

Step 8   For a task to be run on a weekly or monthly basis, select the days when you want to run the task in the **Repeat On** field.

Step 9   Give the job a name.

Step 10   Select the remaining options for the type of task you are creating:

- Backup - Schedule backup jobs as described in .

- Download CRL - Schedule certificate revocation list downloads as described in Configuring Certificate Revocation List Downloads, on page 5.

- Deploy Policies - Schedule policy deployment as described in Automating Policy Deployment, on page 6.

- Nmap Scan - Schedule Nmap scans as described in Scheduling an Nmap Scan, on page 7.

- Report - Schedule report generation as described in Automating Report Generation, on page 8.

- Cisco Recommended Rules - Schedule automatic updates as described in Automating Cisco Recommendations, on page 10.

- Download Latest Update - Schedule software or VDB update downloads as described in Automating Software Downloads, on page 11 or Automating VDB Update Downloads, on page 14.

- Install Latest Update - Schedule installation of software or VDB updates on a management center or managed device as described in Automating Software Installs, on page 13 or Automating VDB Update Installs, on page 15.

- Push Latest Update - Schedule push of software updates to managed devices as described in Automating Software Pushes, on page 12.

- Update URL Filtering Database - Schedule automatic update of URL filtering data as described in Automating URL Filtering Updates Using a Scheduled Task, on page 15.

Step 11   Click **Save**.

Scheduled Backups

You can use the scheduler on a Secure Firewall Management Center to automate its own backups. You can also schedule remote device backups from the management center. For more information on backups, see Backup/Restore.

Note that not all devices support remote backups.

Schedule Management Center Backups

You can use the scheduler on the management center to automate both management center and device backups. Note that not all devices support remote backups. For more information, see Backup/Restore.

Note   As part of the initial configuration, the system schedules weekly configuration-only management center backups (locally stored). We recommend you review this task and make changes if necessary, as described in this topic.

Before you begin

Create a backup profile that specifies your backup preferences. See Create a Backup Profile.

You must be in the global domain to perform this task.

Procedure

Step 1	Choose **System** (⚙) > **Tools** > **Scheduling**.
Step 2	From the **Job Type** list, select **Backup**.
Step 3	Specify whether you want to back up **Once** or **Recurring**.

        • For one-time tasks, use the drop-down lists to specify the start date and time.

        • For recurring tasks, see Configuring a Recurring Task, on page 2.

Step 4	Enter a **Job Name**.
Step 5	For the **Backup Type**, click **Management Center**.
Step 6	Choose a **Backup Profile**.
Step 7	(Optional) Enter a **Comment**.

Keep comments brief. They will appear in the Task Details section of the schedule calendar page.

Step 8	(Optional) Enter an email address, or a comma-separated list of email addresses, in the **Email Status To:** field.

For information on setting up an email relay server to send task status messages, see Configuring a Mail Relay Host and Notification Address.

Step 9	Click **Save**.

Schedule Remote Device Backups

You can use the scheduler on the management center to automate both management center and device backups. Note that not all devices support remote backups. For more information, see Backup/Restore.

You must be in the global domain to perform this task.

Procedure

Step 1	Choose **System** (⚙) > **Tools** > **Scheduling**.
Step 2	From the **Job Type** list, select **Backup**.
Step 3	Specify whether you want to back up **Once** or **Recurring**.

        • For one-time tasks, use the drop-down lists to specify the start date and time.

        • For recurring tasks, see Configuring a Recurring Task, on page 2.

Step 4	Enter a **Job Name**.
Step 5	For the **Backup Type**, click **Device**.
Step 6	Select one or more devices.

If your device is not listed, it does not support remote backup.

Step 7 If you did not configure remote storage for backups, choose whether you want to **Retrieve to Management Center**.

- Enabled (default): Saves the backup to the management center in `/var/sf/remote-backup/`.

- Disabled: Saves the backup to the device in `/var/sf/backup/`.

If you configured remote backup storage, backup files are saved remotely and this option has no effect. For more information, see Manage Backups and Remote Storage.

Step 8 (Optional) Enter a **Comment**.

Keep comments brief. They will appear in the Task Details section of the schedule calendar page.

Step 9 (Optional) Enter an email address, or a comma-separated list of email addresses, in the **Email Status To:** field.

For information on setting up an email relay server to send task status messages, see Configuring a Mail Relay Host and Notification Address.

Step 10 Click **Save**.

Configuring Certificate Revocation List Downloads

You must perform this procedure using the local web interface for the management center.

The system automatically creates the Download CRL task when you enable downloading a certificate revocation list (CRL) in the local configuration on an appliance where you enable user certificates or audit log certificates for the appliance. You can use the scheduler to edit the task to set the frequency of the update.

Before you begin

- Enable and configure user certificates or audit log certificates and set one or more CRL download URLs. See Requiring Valid HTTPS Client Certificates and Require Valid Audit Log Server Certificates for more information.

Procedure

Step 1 Select **System** (✿) > **Tools** > **Scheduling**.
Step 2 Click **Add Task**.
Step 3 From **Job Type**, select **Download CRL**.
Step 4 Specify how you want to schedule the CRL download, **Once** or **Recurring**:

- For one-time tasks, use the drop-down lists to specify the start date and time.

- For recurring tasks, see Configuring a Recurring Task, on page 2 for details.

Step 5 Type a name in the **Job Name** field.
Step 6 If you want to comment on the task, type a comment in the **Comment** field.

The comment field appears in the Task Details section of the schedule calendar page; keep comments brief.

Step 7 If you want to email task status messages, type an email address (or multiple email addresses separated by commas) in the **Email Status To:** field. You must have a valid email relay server configured on the management center to send status messages.

Step 8 Click **Save**.

Related Topics

Configuring a Mail Relay Host and Notification Address

Automating Policy Deployment

After modifying configuration settings in the management center, you must deploy those changes to the affected devices.

⚠

Caution When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See Snort Restart Traffic Behavior and Configurations that Restart the Snort Process When Deployed or Activated.

Procedure

Step 1 Select **System** (⚙) > **Tools** > **Scheduling**.

Step 2 Click **Add Task**.

Step 3 From **Job Type**, select **Deploy Policies**.

Step 4 Specify how you want to schedule the task, **Once** or **Recurring**:

- For one-time tasks, use the drop-down lists to specify the start date and time.

- For recurring tasks, see Configuring a Recurring Task, on page 2 for details.

Step 5 Type a name in the **Job Name** field.

Step 6 In the **Device** field, select a device where you want to deploy policies.

Step 7 Select or deselect the **Skip deployment for up-to-date devices** check box, as required.

By default, the **Skip deployment for up-to-date devices** option is enabled to improve performance during the policy deployment process.

Note
The system does not perform a scheduled policy deployment task if a policy deployment initiated from the management center web interface is in progress. Correspondingly, the system does not permit you to initiate a policy deployment from the web interface if a scheduled policy deployment task is in-progress.

Step 8 If you want to comment on the task, type a comment in the **Comment** field.

The comment field appears in the Task Details section of the schedule calendar page. The comment field must contain between 3 and 255 characters and cannot include any special characters other than hyphen (-), colon (:), and parentheses ().

Step 9 If you want to email task status messages, type an email address (or multiple email addresses separated by commas) in the **Email Status To:** field. You must have a valid email relay server configured to send status messages.

Step 10 Click **Save**.

Related Topics

Configuring a Mail Relay Host and Notification Address

Configuration Changes that Require Deployment

Nmap Scan Automation

You can schedule regular Nmap scans of targets on your network. Automated scans allow you to refresh information previously supplied by an Nmap scan. Because the system cannot update Nmap-supplied data, you need to rescan periodically to keep that data up to date. You can also schedule scans to automatically test for unidentified applications or servers on hosts in your network.

Note that a Discovery Administrator can also use an Nmap scan as a remediation. For example, when an operating system conflict occurs on a host, that conflict may trigger an Nmap scan. Running the scan obtains updated operating system information for the host, which resolves the conflict.

If you have not used the Nmap scanning capability before, you configure Nmap scanning before defining a scheduled scan.

Related Topics

Nmap Scanning

Scheduling an Nmap Scan

After Nmap replaces a host's operating system, applications, or servers detected by the system with the results from an Nmap scan, the system no longer updates the information replaced by Nmap for the host. Nmap-supplied service and operating system data remains static until you run another Nmap scan. If you plan to scan a host using Nmap, you may want to set up regularly scheduled scans to keep Nmap-supplied operating systems, applications, or servers up to date. If the host is deleted from the network map and re-added, any Nmap scan results are discarded and the system resumes monitoring of all operating system and service data for the host.

Procedure

Step 1 Select **System** (✿) > **Tools** > **Scheduling**.

Step 2 Click **Add Task**.

Step 3 From **Job Type**, select **Nmap Scan**.

Step 4 Specify how you want to schedule the task, **Once** or **Recurring**:

• For one-time tasks, use the drop-down lists to specify the start date and time.

• For recurring tasks, see Configuring a Recurring Task, on page 2 for details.

Step 5	Type a name in the **Job Name** field.
Step 6	In the **Nmap Remediation** field, select an Nmap remediation.
Step 7	In the **Nmap Target** field, select the scan target.
Step 8	In the **Domain** field, select the domain whose network map you want to augment.
Step 9	If you want to comment on the task, type a comment in the **Comment** field.

Tip

The comment field appears in the Task Details section of the calendar schedule page; keep comments brief.

Step 10	If you want to email task status messages, type an email address (or multiple email addresses separated by commas) in the **Email Status To:** field. You must have a valid email relay server configured to send status messages.
Step 11	Click **Save**.

Related Topics

Configuring a Mail Relay Host and Notification Address
Nmap Scanning

Automating Report Generation

You can automate reports so that they run at regular intervals.

Before you begin

• For reports other than risk reports: Create a report template. See Report Templates for more information.

• If you want to distribute email reports using the scheduler, configure a mail relay host and specify report recipients and message information. See Configuring a Mail Relay Host and Notification Address and (for reports other than risk reports) Distributing Reports by Email at Generation Time or (for risk reports) Generating, Viewing, and Printing Risk Reports.

• (Optional) Set or change the file name, output format, time window, or email distribution settings of the scheduled report. See Specify Report Generation Settings for a Scheduled Report, on page 9.

• If you will choose PDF as the report output format, look at the report template and verify that the number of results in each section of the template does not exceed the limit for PDFs. For information, see Report Template Fields.

Procedure

Step 1	Select **System** (⚙) > **Tools** > **Scheduling**.
Step 2	Click **Add Task**.
Step 3	From the **Job Type** list, select a job.
Step 4	Specify how you want to schedule the task, **Once** or **Recurring**:

- For one-time tasks, use the drop-down lists to specify the start date and time.

- For recurring tasks, see Configuring a Recurring Task, on page 2 for details.

Step 5   Type a name in the **Job Name** field.

Step 6   In the **Report Template** field, select a risk report or report template.

Step 7   If you want to comment on the task, type a comment in the **Comment** field.

The comment field appears in the Tasks Details section of the schedule calendar page; keep comments brief.

Step 8   If you want to email task status messages, type an email address (or multiple email addresses separated by commas) in the **Email Status To:** field. You must have a valid email relay server configured to send status messages.

> **Note**
> Configuring this option does **not** distribute the reports.

Step 9   If you do not want to receive report email attachments when reports have no data (for example, when no events of a certain type occurred during the report period), select the **If report is empty, still attach to email** check box.

Step 10   Click **Save**.

Specify Report Generation Settings for a Scheduled Report

You must have Admin or Security Analyst privileges to perform this task.

To specify or change the file name, output format, time window, or email distribution settings of a scheduled report:

Procedure

Step 1   Select **Overview > Reporting > Report Templates**.

Step 2   Click **Edit** for the report template to change.

Step 3   If you will select PDF output:

     a) Look to see whether any of the sections in the report shows a yellow triangle beside the number of results.

     b) If you see any yellow triangles, mouse over the triangle to view the maximum number of results allowable for that section for PDF output.

     c) For each section with a yellow triangle, reduce the number of results to a number below the limit.

     d) When there are no more yellow triangles, click **Save**.

Step 4   Click **Generate**.

> **Note**
> If you want to change report generation settings without generating the report now, you must click **Generate** from the template configuration page. Changes will not be saved if you click **Generate** from the template list view unless you generate the report.

Step 5   Modify settings.

Step 6	To save the new settings without generating the report, click **Cancel**.

To save the new settings and generate the report, click **Generate** and skip the rest of the steps in this procedure.

Step 7	Click **Save**.
Step 8	If you see a prompt to save even though you haven't made changes, click **OK**.

Automating Cisco Recommendations

You can automatically generate rule state recommendations based on network discovery data for your network using the most recently saved configuration settings in a custom intrusion policy.

Note   If the system automatically generates scheduled recommendations for an intrusion policy with unsaved changes, you must discard your changes in that policy and commit the policy if you want the policy to reflect the automatically generated recommendations.

When the task runs, the system automatically generates recommended rule states, and modifies the states of intrusion rules based on the configuration of your policy. Modified rule states take effect the next time you deploy your intrusion policy.

Before you begin

- Configure Cisco recommended rules in an intrusion policy as described in the Cisco Secure Firewall Management Center Device Configuration Guide.

- If you want to email task status messages, configure a valid email relay server.

- You must have the IPS Smart License or Protection Classic License to generate recommendations.

Procedure

Step 1	Choose **System** (✿) > **Tools** > **Scheduling**.
Step 2	Click **Add Task**.
Step 3	From **Job Type**, choose **Cisco Recommended Rules**.
Step 4	Specify how you want to schedule the task, **Once** or **Recurring**:

- For one-time tasks, use the drop-down lists to specify the start date and time.

- For recurring tasks, see for details.

Step 5	Enter a name in the **Job Name** field.
Step 6	Next to **Policies**, choose one or more intrusion policies where you want to generate recommendations. Check **All Policies** check box to choose all intrusion policies.
Step 7	(Optional) Enter a comment in the **Comment** field.

Keep comments brief. Comments appear in the Task Details section of the schedule calendar page.

Step 8   (Optional) To email task status messages, type an email address (or multiple email addresses separated by commas) in the **Email Status To:** field.

Step 9   Click **Save**.

Related Topics

Conflicts and Changes: Network Analysis and Intrusion Policies

About Cisco Recommended Rules

Configuring a Mail Relay Host and Notification Address

Software Upgrade Automation

You can automatically download patches, and apply maintenance releases and patches.

To upgrade the management center, schedule Download and Install tasks. To upgrade managed devices, schedule Download, Push, and Install tasks. Make sure you leave adequate time between the tasks; for example, installations scheduled to occur while a push is still running will fail.

This feature is not supported for major releases. Internet access is required to download upgrade packages. When scheduling upgrades to device groups, the upgrade will run on all grouped devices simultaneously.

Note   As part of the initial configuration, the system schedules weekly downloads. We recommend you review this task and make changes if necessary, as described in Automating Software Downloads, on page 11. This task only downloads the updates. It is your responsibility to install any updates this task downloads.

Related Topics

Management Interfaces

Updates

Automating Software Downloads

Use this procedure to schedule the download of select patches and maintenance releases. You must be in the global domain.

Note   In Version 7.4.1+ this task no longer downloads maintenance releases. To direct-download maintenance (and major) releases to the management center, use **System** (✿) > **Product Upgrades**.

Before you begin

Make sure the management center can access the internet.

Procedure

Step 1   Select **System** (✿) > **Tools** > **Scheduling**.

Step 2   Click **Add Task**.

Step 3   From the **Job Type** list, select **Download Latest Update**.

Step 4   Specify how you want to schedule the task, **Once** or **Recurring**:

- For one-time tasks, use the drop-down lists to specify the start date and time.

- For recurring tasks, see Configuring a Recurring Task, on page 2 for details.

Step 5   Type a name in the **Job Name** field.

Step 6   Next to **Update Items**, check **Software** check box.

Step 7   If you want to comment on the task, type a comment in the **Comment** field.

The comment field appears in the Task Details section of the schedule calendar page; keep comments brief.

Step 8   If you want to email task status messages, type an email address (or multiple email addresses separated by commas) in the **Email Status To:** field. You must have a valid email relay server configured to send status messages.

Step 9   Click **Save**.

Related Topics

Configuring a Mail Relay Host and Notification Address

Automating Software Pushes

If you want to automate the installation of software updates on managed devices, you must push the updates to the devices before installing.

When you create the task to push software updates to managed devices, make sure you allow enough time between the push task and a scheduled install task for the updates to be copied to the device.

You must be in the global domain to perform this task.

Procedure

Step 1   Select **System** (⚙) > **Tools** > **Scheduling**.

Step 2   Click **Add Task**.

Step 3   From the **Job Type** list, select **Push Latest Update**.

Step 4   Specify how you want to schedule the task, **Once** or **Recurring**:

- For one-time tasks, use the drop-down lists to specify the start date and time.

- For recurring tasks, see Configuring a Recurring Task, on page 2 for details.

Step 5   Type a name in the **Job Name** field.

Step 6   From the **Device** drop-down list, select the device that you want to update.

Step 7   If you want to comment on the task, type a comment in the **Comment** field.

The comment field appears in the Task Details section of the schedule calendar page; keep comments brief.

Step 8   If you want to email task status messages, type an email address (or multiple email addresses separated by commas) in the **Email Status To:** field. You must have a valid email relay server configured to send status messages.

Step 9   Click **Save**.

Related Topics

> Configuring a Mail Relay Host and Notification Address

Automating Software Installs

Make sure you allow enough time between the task that pushes the update to a managed device and the task that installs the update.

You must be in the global domain to perform this task.

⚠️

Caution   Depending on the update being installed, the appliance may reboot after the software is installed.

Procedure

Step 1   Select **System** (⚙) > **Tools** > **Scheduling**.

Step 2   Click **Add Task**.

Step 3   From the **Job Type** list, select **Install Latest Update**.

Step 4   Specify how you want to schedule the task, **Once** or **Recurring**:

- For one-time tasks, use the drop-down lists to specify the start date and time.

- For recurring tasks, see Configuring a Recurring Task, on page 2 for details.

Step 5   Type a name in the **Job Name** field.

Step 6   From the **Device** drop-down list, select the appliance (including the management center) where you want to install the update.

Step 7   Next to **Update Items**, check the **Software** check box.

Step 8   If you want to comment on the task, type a comment in the **Comment** field.

The comment field appears in the Task Details section of the schedule calendar page; keep comments brief.

Step 9   If you want to email task status messages, type an email address (or multiple email addresses separated by commas) in the **Email Status To:** field. You must have a valid email relay server configured to send status messages.

Step 10   Click **Save**.

Related Topics

> Configuring a Mail Relay Host and Notification Address

Vulnerability Database Update Automation

You can use the scheduling feature to update the Cisco vulnerability database (VDB), thereby ensuring that you are using the most up-to-date information to evaluate the hosts on your network. You must schedule the download, install, and subsequent deploy as separate tasks, allowing enough time between tasks.

> **Note** The initial setup on the management center automatically downloads and installs the latest VDB from Cisco as a one-time operation. It also schedules a weekly task to download the latest available software updates, which includes the latest VDB. We recommend you review this weekly task and adjust if necessary. Optionally, schedule a new weekly task to actually update the VDB and deploy configurations.

Related Topics

Management Interfaces

Automating VDB Update Downloads

You must be in the global domain to perform this task.

Before you begin

Make sure the management center has internet access.

Procedure

Step 1   Select **System** (⚙) > **Tools** > **Scheduling**.

Step 2   Click **Add Task**.

Step 3   From the **Job Type** list, select **Download Latest Update**.

Step 4   Specify how you want to schedule the task, **Once** or **Recurring**:

- For one-time tasks, use the drop-down lists to specify the start date and time.

- For recurring tasks, see Configuring a Recurring Task, on page 2 for details.

Step 5   Type a name in the **Job Name** field.

Step 6   Next to **Update Items**, check the **Vulnerability Database** check box.

Step 7   (Optional) Type a brief comment in the **Comment** field.

Step 8   If you want to email task status messages, type an email address (or multiple email addresses separated by commas) in the **Email Status To:** field. You must have a valid email relay server configured to send status messages.

Step 9   Click **Save**.

Related Topics

Configuring a Mail Relay Host and Notification Address

Automating VDB Update Installs

Allow enough time between the task that downloads the VDB update and the task that installs the update.

You must be in the global domain to perform this task.

⚠️

Caution   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.

Procedure

Step 1	Select **System** (⚙) > **Tools** > **Scheduling**.
Step 2	Click **Add Task**.
Step 3	From the **Job Type** list, select **Install Latest Update**.
Step 4	Specify how you want to schedule the task, **Once** or **Recurring**:
	• For one-time tasks, use the drop-down lists to specify the start date and time.
	• For recurring tasks, see Configuring a Recurring Task, on page 2 for details.
Step 5	Type a name in the **Job Name** field.
Step 6	From the **Device** drop-down list, select the management center.
Step 7	Next to **Update Items**, check the **Vulnerability Database** check box.
Step 8	(Optional) Type a brief comment in the **Comment** field.
Step 9	If you want to email task status messages, type an email address (or multiple email addresses separated by commas) in the **Email Status To:** field. You must have a valid email relay server configured to send status messages.
Step 10	Click **Save**.

Related Topics

Configuring a Mail Relay Host and Notification Address

Automating URL Filtering Updates Using a Scheduled Task

In order to ensure that threat data for URL filtering is current, the system must obtain data updates from the Cisco Collective Security Intelligence (CSI) cloud.

By default, when you enable URL filtering, automatic updates are enabled. However, if you need to control when these updates occur, use the procedure described in this topic instead of the default update mechanism.

Although daily updates tend to be small, if it has been more than five days since your last update, new URL filtering data may take up to 20 minutes to download, depending on your bandwidth. Then, it may take up to 30 minutes to perform the update itself.

Before you begin

- Make sure the management center has internet access: Security, Internet Access, and Communication Ports.

- Make sure you have a URL Filtering license and enable URL filtering. For more information, see the *Enable URL Filtering Using Category and Reputation* in the Cisco Secure Firewall Management Center Device Configuration Guide.

- Verify that **Enable Automatic Updates** is not selected on the **Cloud Services** under the **Integration** > **Other Integrations** menu.

- You must be in the Global domain to perform this task.

Procedure

Step 1   Select **System** ( ) > **Tools** > **Scheduling**.

Step 2   Click **Add Task**.

Step 3   From the **Job Type** list, select **Update URL Filtering Database**.

Step 4   Specify how you want to schedule the update, **Once** or **Recurring**:

- For one-time tasks, use the drop-down lists to specify the start date and time.

- For recurring tasks, see Configuring a Recurring Task, on page 2.

Step 5   Type a name in the **Job Name** field.

Step 6   If you want to comment on the task, type a comment in the **Comment** field.

The comment field appears in the Task Details section of the schedule calendar page. Keep comments brief.

Step 7   If you want to email task status messages, type an email address (or multiple email addresses separated by commas) in the **Email Status To:** field. You must have a valid email relay server configured to send status messages.

Step 8   Click **Save**.

Related Topics

Configuring a Mail Relay Host and Notification Address

Scheduled Task Review

After adding scheduled tasks, you can view them and evaluate their status. The View Options section of the page allows you to view scheduled tasks using a calendar and a list of scheduled tasks.

The Calendar view option allows you to view which scheduled tasks occur on which day.

The Task List shows a list of tasks along with their status. The task list appears below the calendar when you open the calendar. In addition, you can view it by selecting a date or task from the calendar.

You can edit a scheduled task that you previously created. This feature is especially useful if you want to test a scheduled task once to make sure that the parameters are correct. Later, after the task completes successfully, you can change it to a recurring task.

There are two types of deletions you can perform from the Schedule View page. You can delete a specific one-time task that has not yet run or you can delete every instance of a recurring task. If you delete an instance of a recurring task, all instances of the task are deleted. If you delete a task that is scheduled to run once, only that task is deleted.

Task List Details

Table 1: Task List Columns

Column	Description
Name	Displays the name of the scheduled task and the comment associated with it.
Type	Displays the type of scheduled task.
Start Time	Displays the scheduled start date and time.
Frequency	Displays how often the task is run.
Last Run Time	Displays the actual start date and time. For a recurring task, this applies to the most recent execution.
Last Run Status	Describes the current status for a scheduled task: • A **Check mark**( ) indicates that the task ran successfully. • A question mark icon (**Question Mark** ( )) indicates that the task is in an unknown state. • An exclamation mark icon ( ) indicates that the task failed. For a recurring task, this applies to the most recent execution.
Next Run Time	Displays the next execution time for a recurring task. Displays N/A for a one-time task.
Creator	Displays the name of the user that created the scheduled task.
Edit	Edits the scheduled task.
Delete	Deletes the scheduled task.

Viewing Scheduled Tasks on the Calendar

You can view a scheduled task on the calendar.

Procedure

Step 1 Select **System** (⚙) > **Tools** > **Scheduling**.

Step 2 You can perform the following tasks using the calendar view:

- Click **Double Left Arrow** (≪) to move back one year.

- Click **Single Left Arrow** (‹) to move back one month.

- Click **Single Right Arrow** (›) to move forward one month.

- Click **Double Right Arrow** (≫) to move forward one year.

- Click **Today** to return to the current month and year.

- Click **Add Task** to schedule a new task.

- Click a date to view all scheduled tasks for the specific date in a task list table below the calendar.

- Click a specific task on a date to view the task in a task list table below the calendar.

Editing Scheduled Tasks

You can edit scheduled tasks.

Procedure

Step 1 Select **System** (⚙) > **Tools** > **Scheduling**.

Step 2 On the calendar, click either the task that you want to edit or the day on which the task appears.

Step 3 In the **Task Details** table, click **Edit** (✎) next to the task you want to edit.

Step 4 Edit the task.

Step 5 Click **Save**.

Deleting Scheduled Tasks

You can delete a scheduled task.

Procedure

Step 1   Select **System** (✿) > **Tools** > **Scheduling**.

Step 2   In the calendar, click the task you want to delete. For a recurring task, click an instance of the task.

Step 3   In the **Task Details** table, click **Delete** (🗑), then confirm your choice.

History for Scheduled Tasks

Feature	Minimum Management Center	Minimum Threat Defense	Details
Scheduled tasks download patches and VDB updates only.	7.2.6 7.4.1	Any	**Upgrade impact. Scheduled download tasks stop retrieving maintenance releases.** 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**. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0.
Automatic VDB downloads.	7.3.0	Any	Initial setup schedules a weekly task to download the latest available software updates, which now includes the latest VDB. We recommend you review this weekly task and adjust if necessary, as well as schedule a new weekly task to actually update the VDB. You must deploy configurations for new application detectors and operating system fingerprints to take effect. New/modified screens: The **Vulnerability Database** check box is now enabled by default in the system-created **Weekly Software Download** scheduled task.
Automatic intrusion rule updates.	6.6	Any	Initial setup enables daily intrusion rule updates. We recommend you review this task and adjust if necessary. For the updated rules to take effect you must deploy configurations.
Automatic software downloads and configuration backups.	6.5	Any	Initial setup schedules weekly tasks to: • Download the latest available software updates for the FMC and its managed devices. • Perform a locally stored configuration-only backup. We recommend you review these tasks and adjust as necessary.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Schedule remote backups of many managed devices.	6.4	Any	Schedule device backups. New/modified screens: When configuring a recurring backup, you can now choose a **Backup Type**: management center vs device. Platform restrictions: Device must support on-demand backup; see Requirements for Backup and Restore.