

Scheduling

- Task scheduling, on page 1
- Guidelines for scheduled tasks, on page 2
- Scheduled task types, on page 2
- Schedule a task, on page 4

Task scheduling

Task scheduling is a system management feature that allows you to automate routine jobs to run once or on a recurring basis.

Time zones and seasonal time changes

Tasks are scheduled in Coordinated Universal Time (UTC), which remains constant year-round. Scheduled tasks do not adjust automatically for local time changes, such as daylight saving time or summer time. For example, a task scheduled for 2:00 a.m. during standard time runs at 3:00 a.m. after the local clock moves forward.

The Cloud-Delivered Firewall Management Center evaluates scheduled task times in the display time zone configured for the user who creates the task. If that time zone observes daylight saving time (DST), a task scheduled during the hour skipped when clocks move forward does not run that day, and no error is generated. A task scheduled during the repeated hour when clocks move back runs twice.

To avoid missed or duplicate runs, create reliability-critical tasks, such as backups and feed updates, using a user whose display time zone is UTC or a time zone that does not observe DST, such as Etc/GMT+5 or America/Phoenix.

This behavior can affect device configuration backups, Security Intelligence feed, URL, and DNS updates, VDB and GeoDB updates, scheduled reports, and license reconciliation jobs.

Automatically scheduled tasks

The system automatically schedules these tasks:

- A one-time task to download and install the latest VDB, at initial setup.
- A weekly task to download the latest available, starting at initial setup.
- A daily task to updated certificate revocation lists (CRL), when you configure user or audit log certificates.

Guidelines for scheduled tasks

This section provides general scheduling guidelines. Refer to Scheduled task types, on page 2 for task-specific guidelines and prerequisites.

When to run tasks

Follow these guidelines when scheduling tasks:

- Automatically scheduled tasks: Review automatically scheduled tasks to make sure they run at the right time for your environment.
- Traffic inspection and flow: Schedule tasks that might interrupt traffic during maintenance windows.

Scheduling task sequences

This table lists outcomes that require multiple tasks in sequence. Leave enough time so that each task can finish before the next begins.

Table 1: Outcomes requiring multiple scheduled tasks

Outcome	Tasks
VDB update	**1.** Download Latest Update **2.** Install Latest Update

Scheduled task types

This section describes the available scheduled task types (**Job Type** in the scheduler), as well as options, guidelines, and requirements for each task.

Backup

Purpose: Back up managed devices.

Options:

- **Backup Type**: Device

Guidelines:

- Supported devices: Some devices, such as devices in the public cloud, cannot be backed up.
- Simultaneous backups: Back up no more than 20 devices per task. Do not schedule multiple backup tasks for the same time; start with 30 minutes between backups.
- Bandwidth: If you are transferring backup files, consider scheduling backups during periods of low network use.

Download CRL

Purpose: Download certificate revocation list (CRL) updates. The system automatically schedules daily CRL updates when you configure user or audit log certificates in the system configuration. Use the scheduler to change the update interval or run a one-time update. Disabling the configurations removes the task.

Download latest update

Purpose: Download the latest VDB update. Initial setup schedules a weekly download of the latest applicable updates.



Note Use **Administration** > **Upgrades & updates** > **Product Upgrades** to upgrade software. Scheduled software upgrades are not supported, although the web interface allows configuration.

Options:

- **Update Items**: Choose **Vulnerability Database**.

Guidelines:

- Required task order: To update the VDB, download then install. Download must finish before install begins.
- Bandwidth: Consider scheduling downloads during periods of low network use.

Push latest update



Note Use **Administration** > **Upgrades & updates** > **Product Upgrades** to upgrade software. Scheduled software upgrades are not supported, although the web interface allows configuration.

Install latest update

Purpose: Install a VDB update.



Note Use **Administration** > **Upgrades & updates** > **Product Upgrades** to upgrade software. Scheduled software upgrades are not supported, although the web interface allows configuration.

Options:

- **Update Items**: Choose **Vulnerability Database**.
- **Device**: Choose the Cloud-Delivered Firewall Management Center.

Guidelines:

- Required task order: To update the VDB, download then install. Download must finish before install begins.

- 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.
- Deploy during a maintenance window to implement changes: Snort typically restarts during the first deployment after VDB update. Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including devices configured for high availability or clustering.

Queue intrusion policy apply

Purpose: Deploy intrusion policy changes from the Cloud-Delivered Firewall Management Center to managed devices.

Options:

- **Intrusion Policy**: The policy you want to deploy.
- **Device**: The device where you want to deploy the policy.

Guidelines:

- Traffic inspection and flow: 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. Refer to Snort restart traffic behavior and Configurations that restart the snort process when deployed or activated.

Update URL filtering database

Purpose: Obtain the latest URL filtering data from Cisco. By default, when you enable URL filtering, automatic updates are enabled. However, if you need to control exactly when these updates occur, use the scheduler.

Guidelines:

- Licenses: URL Filtering
- Prerequisite configurations: You must enable URL filtering to schedule this task. Disable automatic updates on **Integrations** > **Cloud Services**.
- Update size, duration, and bandwidth: Daily updates are typically small. With longer intervals, expect larger downloads and additional time for the changes to propagate, and consider scheduling during periods of low network use.

Schedule a task

Before you begin

Before you schedule a task:

- Review the guidelines and prerequisites for scheduled tasks in general: Guidelines for scheduled tasks, on page 2.
- Review the guidelines and prerequisites that apply to your task: Scheduled task types, on page 2.

- (Optional) Set up an email relay server to get task status messages: Configure a mail relay host and notification address.

Follow these steps to schedule a task.

Procedure

Step 1 Choose **Administration** > **Advanced** > **Scheduling** and click **Add Task**.

Step 2 Choose a **Job Type** and configure the task-specific parameters.

Refer to Scheduled task types, on page 2 for the specific options and restrictions for each task.

Step 3 Specify the schedule details: once or recurring, start time, and frequency.

Step 4 Enter a name for the task, and optionally, a comment and email addresses for status notifications.

You can see comments when you view task details in the calendar.

Step 5 Click **Save**.

Your task is scheduled and will run at the configured time.