

Scheduling

- Task scheduling, on page 1
- Guidelines for scheduled tasks, on page 1
- Scheduled task types, on page 2
- Schedule a task, on page 7
- History for scheduling, on page 7

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.

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 patches, maintenance releases, and, starting at initial setup.
- A weekly task to perform a locally stored configuration-only backup of the Firewall Management Center, 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.

User role requirements

Admin or Maintenance

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.
- Bandwidth: Schedule tasks that require large amounts of bandwidth during periods of low network use.
- 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 **3.** Deploy Policies
Software upgrade	**1.** Download Latest Update **2.** Push Latest Update (devices only) **3.** Install Latest Update **4.** Deploy Policies **Note** For more information about software upgrades, including additional restrictions and recommended actions if an upgrade is unresponsive or fails, refer to the upgrade guide for your Firewall Management Center version: Secure Firewall Threat Defense upgrade guides for Firewall Management Center.
Recommended rules update	**1.** Cisco Recommended Rules **2.** Deploy Policies

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 the Firewall Management Center and managed devices. Initial setup schedules a weekly configuration backup of the Firewall Management Center, stored locally.

Options:

- **Backup Type**: Device or Firewall Management Center
- **Backup Profile**: Firewall Management Center backups require a backup profile. Refer to Create a backup profile.
- **Retrieve to Management Center**: Devices only. This option controls device backups irrespective of remote storage is enabled or not.
  - Enabled (default): If remote storage is configured, the backup files are saved to remote storage, else the device backup files are saved to the Firewall Management Center in `/var/sf/remote-backup/`.
  - Disabled: Saves device backups to the device in `/var/sf/backup/`.

  For more information about managing backup, refer to Manage backups and remote storage.

Guidelines:

- Supported devices: Some devices, such as devices in the public cloud, cannot be backed up. Refer to Requirements: backup and restore configuration.
- Prerequisite configurations: Firewall Management Center backups require a backup profile. Refer to Create a backup profile.
- 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.

Cisco recommended rules

Purpose: Generate rule state recommendations and modify intrusion policies based on network discovery data.

Options:

- **Policies**: The intrusion policies where you want to generate recommendations.

Guidelines:

- Licenses: IPS or Protection
- Prerequisite configurations: You must have at least one custom intrusion policy with recommendations enabled to schedule this task.
- Save changes before the task runs: If your intrusion policies have unsaved changes, recommendations are not applied. Discard your changes and commit the policy to apply recommendations.

- Deploy during a maintenance window to implement changes: Snort may need to restart. Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including devices configured for high availability or clustering.

Deploy policies

Purpose: Deploy configuration changes from the Firewall Management Center to managed devices. You may want to schedule a deploy after recommended rules, software, or VDB updates.

Options:

- **Device**: The devices where you want to deploy the policies.
- **Skip deployment for up-to-date devices**: Enabled by default to improve performance during the deployment process.

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.
- Concurrent deployments: Scheduled policy deployments do not run if a manual policy deployment is already in progress. You cannot deploy from the web interface while a scheduled deployment is running.

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.

Guidelines:

- Internet access: The Firewall Management Center must have internet access to download updates. Refer to Communication Ports and Internet Access.

Download latest update

Purpose: Download the latest maintenance releases, patches, and VDB update. Initial setup schedules a weekly download of the latest applicable updates.

Options:

- **Update Items**: Choose **Vulnerability Database**, **Software**, or both.

Guidelines:

- Supported software upgrade types: You can download maintenance updates and patches. Major upgrades are not supported.
- Required task order: To update the VDB or to upgrade the Firewall Management Center, download then install. To upgrade a managed device, download, push, then install. Each task must finish before the next begins.

- Internet access: The Firewall Management Center must have internet access to download updates. Refer to Communication Ports and Internet Access.
- Bandwidth: Consider scheduling downloads during periods of low network use.

Push latest update

Purpose: Push a downloaded software upgrade package to a managed device so that you can upgrade the device.

Options:

- **Device**: Choose a device or device group.

Guidelines:

- Supported upgrade types: You can push maintenance updates and patches. Major upgrades are not supported.
- Required task order: To upgrade the Firewall Management Center, download then install. To upgrade a managed device, download, push, then install. Each task must finish before the next begins.
- Bandwidth: Consider scheduling pushes during periods of low network use.

Install latest update

Purpose: Install a maintenance release, patch, or VDB update.

Options:

- **Update Items**: Choose **Vulnerability Database** or **Software**.
- **Device**: For software updates, you can choose the Firewall Management Center, a device, or a device group. For VDB updates, you must choose the Firewall Management Center.

Guidelines for VDB updates:

- 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.

Guidelines for software upgrades:

- Supported upgrade types: You can install maintenance updates and patches. Major upgrades are not supported.
- Required task order: To upgrade the Firewall Management Center, download then install. To upgrade a managed device, download, push, then install. Each task must finish before the next begins.

- Grouped devices: Use simple device groups to upgrade multiple devices with one scheduled task. The system upgrades the targets one at a time. In high availability or clustered deployments, devices use the normal upgrade behavior.
- Upgrade devices during a maintenance window due to effects on traffic inspection and flow: For high availability or clustered devices, traffic inspection and flow are not interrupted during upgrade. For standalone devices, interface configurations determine whether traffic is dropped or passed without inspection.
- Deploy during a maintenance window to implement changes: You must deploy after software upgrades. Snort typically restarts during this first deployment. Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including devices configured for high availability or clustering.

Nmap scan

Purpose: Nmap scans refresh static operating system, application, and server data previously supplied by Nmap. You can also use these scans to test for unidentified applications and servers.

Options:

- **Nmap Remediation**: The specific Nmap remediation to run.
- **Nmap Target**: The scan target.
- **Domain**: In a multidomain deployment, the domain whose network map you want to augment.

Guidelines:

- Prerequisite configurations: You must configure Nmap scanning to schedule this task. This includes creating an Nmap instance, scan target, and remediation. Refer to Nmap scanning guidelines for additional guidelines.
- Scan regularly: The system does not automatically update network map data replaced by Nmap unless you delete the scan targets from the network map and allow the system to rediscover them. Schedule regular scans to keep your network map current.
- Bandwidth: Consider scheduling expensive scans, such as portscans, during periods of low network use.

Report

Purpose: Schedule report generation.

Options:

- **Report Template**: Use a system-provided template or create your own to generate the report. To get reports by email, edit the report template. The scheduler email option sends only task status and does not send the report by email.
- **If report is empty, still attach to email**: Receive reports as email attachments even when reports have no data; for example, when no events of a certain type occurred during the report period.

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 **Integration** > **Other 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.
- Internet access: The Firewall Management Center must have internet access to download updates. Refer to Communication Ports and Internet Access.

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 1.
- 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 **System** (⚙) > **Tools** > **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.

History for scheduling

This table provides the feature history for the task scheduler.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Automatic software downloads and configuration backups.	6.5	Any	Initial setup schedules weekly tasks to: • Download the latest available software updates for the Firewall Management Center and its managed devices. • Perform a locally stored configuration-only backup. We recommend you review these tasks and adjust as necessary.
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**: Firewall Management Center vs device. Platform restrictions: Device must support on-demand backup. Refer to Requirements: backup and restore configuration.