Sensor Update Policies | Sensor Deployment and Maintenance | Documentation | Support and resources

Overview

Set up sensor update policies to control the update process for sensors on all your hosts. No restart is required during these in-place updates. Each host is assigned to a sensor policy, based on its host group. There are separate sensor update policies for separate platforms (Windows, Mac, and Linux).

Use sensor update policies to:

- Lock host groups to a specific sensor version
- Control whether the cloud manages sensor version updates
- Protect sensors from unauthorized uninstallation by end users
- Deploy new sensor versions to host groups for testing and validation

You can revert a sensor to a previous version, but only to a version released in the last 180 days. Because of our 180-day support window, we strongly recommend that you test and update to the latest sensor version as soon as possible.

> **Note: Falcon Container does not support sensor update policies for pods.** For info on updating the Falcon Container sensor, see Falcon Container Sensor for Linux .

Falcon offers several settings to give you better control over the maintenance and updating of your sensors.

- **Update schedules:** Use sensor update policies to automatically update test and production hosts to the appropriate versions.
- **Sensor and channel update throttling:** Throttle sensor update speeds to conserve bandwidth on slower networks.
- **Sensor uninstall protection:** Control whether an end user with local admin permissions can manually update or uninstall the sensor.

We also recommend these general best practices:

- Update your hosts' sensors monthly to keep them on a recent version. Even for organizations with more restrictive change control policies, we recommend not letting sensors age more than 60 days after their release.
- Create a policy with Managing sensor maintenance and uninstallation enabled for most hosts.

- Create one policy used for handling sensor uninstallation and maintenance. If you need to change or uninstall the sensor from hosts, move host groups to this policy with **Uninstall and maintenance protection** disabled and **Sensor version updates** off.

  Tip: Use this policy to uninstall, upgrade, or downgrade host groups.

For info about configuring content update policies, which control when CrowdStrike-initiated channel files are deployed to your sensors, see Content Update Policies .

Requirements

- **Subscriptions supported:** Falcon Prevent, Falcon Insight XDR
- **Default roles:** Falcon Administrator, Endpoint Manager

Sensor version management

Update your hosts' sensors monthly to keep them current. If sensors can't be updated monthly, avoid letting sensors age more than 60 days after their release. We recommend that you test internally before deploying to your entire environment, particularly if you run custom or uncommon applications. Testing can be done using fixed sensor versions, or automated.

- **Fixed:** Sensor is set to a specific version number, and will remain on this build
  - Organizations preferring a more "hands on" testing process manually assign specific sensor versions to test and production groups.
  - After a version has been tested, production sensor update policies are manually updated.
- **Automated:** Sensor is set to one of four Auto policy options
  - **Auto - Early Adopter**: When an early adopter build is available for testing, hosts with this setting update to the build. For more info, see Testing sensor builds as an early adopter

    Note: You must enable the **Early adopter sensor builds** setting to select early adopter builds for your policy.
  - **Auto - Latest**: When a scheduled release happens, hosts with this setting update to the newest version. For hosts designated for sensor testing.
  - **Auto - N-1**: When a scheduled release happens, hosts with this setting update to the second-newest version
  - **Auto - N-2**: When a scheduled release happens, hosts with this setting update to the third-newest version

  Note: In the event the latest sensor build is rolled back or removed from service, hosts on **Auto - N-1** and **Auto - N-2** will not revert to a previous build of the sensor. These policies are already set to a known stable sensor version and will remain there until it makes sense within the policy rules to move to the next available build.

Creating a sensor update policy

1. Go to Host setup and management > Deploy > Sensor update policies .
2. Click **Create policy**.
3. Enter a **Policy name**.
4. Select an operating system from the **Platform** dropdown menu.
5. Optional. Enter a **Description** for your policy.
6. Click **Create policy**.
7. On the **Sensor settings** tab, select a sensor version for your policy:
    - **Auto - Early Adopter**: When an early adopter build is available for testing, hosts with this setting update to the build. For more info, see Testing sensor builds as an early adopter

        Note: You must enable the **Early adopter sensor builds** setting to select early adopter builds for your policy.
    - **Auto - Latest**: When a scheduled release happens, hosts with this setting update to the newest version. Recommended for sensor testing.
    - **Auto - N-1**: When a scheduled release happens, hosts with this setting update to the second-newest version shortly after the release.
    - **Auto - N-2**: When a scheduled release happens, hosts with this setting update to the third-newest version shortly after the release.
    - **Specific version number**: Sensors upgrade or downgrade to the selected version and remain on it until you select a new version.
    - **Sensor version updates off**: Sensors can be on different versions and the cloud won't push any version changes.
8. Optional. Schedule time blocks during which to block sensor updates. For more info, see Schedule sensor cloud update exclusions .
9. Configure **Uninstall and maintenance protection**:
    - When enabled, the sensor is protected from unauthorized uninstallation and can't be uninstalled without providing a maintenance token.
    - If disabled, the sensor can be uninstalled by end users.
    - For more info, see Managing sensor maintenance and uninstallation .
10. Click **Save**, then click **Save** again to confirm your policy settings.

You can have a total of 100 custom sensor update policies.

Assigning a sensor update policy to a host group

1. On the **Sensor update policies** page, click the sensor update policy that you want to modify.
2. Click the **Assigned host groups** tab.
3. Click **Assign host groups**.
4. Select the groups that you want to assign to the policy, then click **Assign groups**.

You can only select groups that aren't yet assigned to a policy.

Deleting a sensor update policy

Before deleting a sensor update policy, you first have to disable it.

When you disable a policy, the policy stops affecting online hosts. When any offline hosts come back online, the cloud disables the policy on those hosts.

When you delete a policy, the hosts from that group will be reassigned another policy based on your policy precedence. For more info, see Policy precedence . You do not need to wait for offline hosts before deleting the policy.

Occasionally the default rate at which sensors update isn't suitable for every environment. If cloud-based sensor updates and channel file updates are using too much network bandwidth or taking too long to complete, you can adjust the rate at which updates are initiated.

To disable and then delete a sensor update policy:

1. On the **Sensor update policies** page, click the sensor update policy that you want to delete.
2. Click **Disable policy**, then click **Disable policy** again to confirm.
3. Click **Delete policy**, then click **Delete policy** again to confirm.

Testing sensor builds as an early adopter

CrowdStrike makes new sensor builds available for testing prior to their official production release. You can opt in to test early adopter builds to help validate them and provide feedback to CrowdStrike. Early adopter builds are available for testing purposes 4 days prior to the general availability of that build as **Auto - Latest**.

To opt in to include early adopter builds for a sensor update policy, on the **Sensor settings** tab, select **Show early adopter sensor builds**.

With this setting enabled, you can specify the sensor update policy to auto-update hosts in your test environment with the latest early adopter sensor version.

To provide feedback about any early adopter sensor build, click **Start Survey**.

Schedule sensor cloud update exclusions

Schedule exclusions to prevent hosts from receiving Falcon sensor cloud updates during specified time blocks. This is helpful in cases where you have maintenance windows that you don't want to disrupt with sensor updates.

> **Note:** You can only specify one time block per day of the week.

Important: Hosts can't receive sensor updates unless they are online. Some hosts, such as VMs and laptops, may only be online periodically. Be careful when creating sensor update exclusion time blocks to not exclude the only times these types of hosts are online because they won't have an opportunity to receive sensor updates. Changes to a sensor update policy that are made during an exclusion window will not be reflected in the **Host Management** table until the exclusion period is over and the updated policy is applied. Also, be aware that because of sensor update throttling, creating sensor update exclusion time blocks that drastically narrow the times during which sensors can receive updates may result in some hosts not receiving updates.

Enabling scheduled exclusions

Before specifying one or more time blocks to block updates, you must enable scheduled exclusions.

1. Go to **Host setup and management > Deploy > Sensor update policies** .
2. Create a new policy or select an existing policy.
3. On the **Sensor update schedule** tab, select **Enable sensor update schedule**.
4. Create at least one time block. For more info, see Adding a time block .

Adding a time block

After enabling scheduled exclusions, you can add a time block to a sensor update policy that will block updates from being applied during the specified time. Sensor cloud updates and policy assignments, as well as changes to already assigned policies, are not applied to hosts during the time block specified.

1. On the **Sensor update policies** page, click the policy that you want to modify.
2. Click the **Sensor update schedule** tab.
3. Select a time zone for the scheduled exclusion. The default value for time zone is acquired from your browser's time zone setting.

   Important: The exclusion will apply at the specified time in the time zone that you select, regardless of the time zone that the hosts are located in. For example, if you create an exclusion during a time block of 04:00 - 06:00 and select a UTC+10:00 time zone, the exclusion applies to the hosts from 04:00 - 06:00 UTC+10:00 rather than their local time.

4. In the **Day** dropdown menu, select the day you want this time block to apply to.

   Note: You can only create one time block per day of the week.

5. Select a duration for your time block.
   1. For time blocks lasting less than a full calendar day, select a **Start time** and **End time**. Time blocks must be at least one hour long and one hour apart.
   2. If you want to schedule your time block for the entire day, select **All day**.

      Important: It is possible to create a schedule that might be too restrictive, thus

blocking sensor updates on targeted hosts. Additionally, newly provisioned hosts targeted by a restrictive update policy might not receive the assigned sensor update policy and will therefore indicate **No Policy** in the **Host Management** table. When you create a sensor update schedule, keep in mind the total time wherein sensor updates are blocked each week. You can find this info on the **Sensor update schedule** tab, next to **Total blocked duration**.

6. Click **Add time block**, then click **Save**.
7. In the **Save policy changes** dialog, click **Save**.

All scheduled exclusions for the week are represented in a chart on the **Sensor update schedule** tab. Hover the bar for each day to show the exact time that the exclusion is scheduled for.

Editing a time block

1. On the **Sensor update schedule** tab, click **Edit** The time block Edit button next to the time block that you want to edit.
2. Make your changes, then click **Add time block**.
3. Click **Save**.
4. In the **Save policy changes** dialog, click **Save**.

Deleting a time block

1. On the **Sensor update schedule** tab, click **Delete** The time block Delete button next to the time block that you want to delete.
2. Click **Remove**.

   Note: If you delete all time blocks and want to save your changes, you must deselect **Enable sensor update schedule** before saving.

Disabling scheduled exclusions

1. On the **Sensor update policies** page, click the policy that you want to disable scheduled exclusions for.
2. Click the **Sensor update schedule** tab.
3. Deselect **Enable sensor update schedule**.
4. Click **Save**.
5. In the **Save policy changes** dialog, click **Save**.

When this setting is disabled, existing time blocks remain but are ignored. Sensor cloud updates are applied regardless of the time blocks specified.

Sensor update throttling

For cloud-based sensor updates managed through Falcon, you can adjust how many sensor updates are initiated per minute.

- If sensor updates are consuming too much network bandwidth, you can decrease the number of sensor updates initiated per minute
- If sensor updates are taking too long, you can increase the number of sensor updates initiated

per minute

Updates are pushed to sensors each minute based on the limit you select. Even if the first batch of updates hasn't completed, the next batch of sensors starts the following minute. As a result, the number of sensors updated each minute might be fewer than the limit you selected. For example, if your sensor update rate is set to 50 sensors per minute, it can take up to 20 minutes to update 1000 sensors with an available network bandwidth of 1000mbps.

> **Note:** The default update rate is 50 sensors per minute. We strongly recommend making and testing incremental changes to the next step up or down, then see how it affects network performance. If adjustments are still needed, make another adjustment.

Throttle sensor update throttling rate

Adjust the sensor update rate:

1. Go to Support and resources > Resources and tools > General settings .
2. Click **Throttle updates**.
3. Use the **Sensor update rate** menu to select how many hosts receive sensor updates per minute.
4. Click **Save**.

Channel file update throttling

Channel file updates push dynamic content from the cloud to the sensor, including updates to policy and configuration settings. Most channel file updates are relatively small, ranging from 1K to 2MB in size. Because there are variations in update size, it's important to understand the range of channel file update sizes compared to the number of sensors in your environment. For example, if you have 100,000 sensors in your environment and a channel file update is 2MB, 200GB of channel file updates are downloaded.

You can control the size of channel file updates that are being applied to your sensors by time period: per second, minute, hour, and day

- If channel file updates are consuming too much network bandwidth, you can decrease the size of the updates per time period
- By default, channel file updates are not throttled

The throttling limitations are enforced based on the most restrictive size and rate.

> **Note:** We strongly recommend making small adjustments at a time. Start with a smaller number, and then see how this affects network performance. If adjustments are still needed, make another adjustment.

Adjust channel file update limits by time period

To adjust the rate at which channel file updates are downloaded:

1. Go to Support and resources > Resources and tools > General settings .

2. Click **Throttle updates**.
3. Use the **Channel file bandwidth limits** menu to adjust the size of the update limit per **second**, **minute**, **hour**, or **day**.

   Tip: To clear the throttling setting, delete the value.
4. Click **Save**.

Managing sensor maintenance and uninstallation

The **Uninstall and maintenance protection** setting in sensor update policies prevents unauthorized uninstallation of the sensor. Enabled by default for Mac and Windows policies, the setting controls whether a user with local admin permissions can manually update or uninstall the sensor. This setting also prevents unauthorized users from modifying sensor grouping tags.

We recommend keeping **Uninstall and maintenance protection** enabled for all your hosts, although occasionally a sensor needs to be manually upgraded, downgraded, or uninstalled. We recommend that you create a sensor update policy only used for temporary sensor maintenance and uninstallation. The policy should have **Uninstall and maintenance protection** disabled and **Sensor version updates off** selected. Move hosts to that policy when they require changes, then move the hosts back to their original sensor update policies when you're finished.

> **Important:** User mode of the Falcon sensor for Linux supports sensor maintenance and uninstallation protection for hosts running on ARM kernels that are version 6.0 and later only. Sensor maintenance and uninstallation protection is supported in user mode for all supported Linux kernel versions that are not ARM architecture. Sensor maintenance and uninstallation protection is supported in kernel mode for all supported Linux kernel versions and architectures.

For info about uninstalling and upgrading the sensor, read our deployment guides:

- Falcon Sensor for Windows Deployment
- Falcon Sensor for Mac Deployment
- Falcon Sensor for Linux

Making changes to a single host

If a host is offline, a Falcon Admin or Endpoint Manager can get a single-use, AID-specific maintenance token that allows the sensor to be uninstalled.

1. Go to the **Host management** page at **Host setup and management > Manage endpoints > Host management** .
2. Find and click a host to open its summary panel.
3. Click **Reveal maintenance token**.
4. Enter a reason for revealing the token.
5. Click **Reveal Token**.

The token doesn't change until the sensor has been uninstalled and reinstalled on the host.

Making changes to multiple hosts

If you manage sensor updates manually outside of Falcon through self-service sensor updating (through a tool like SCCM or JAMF) and have cloud updates turned off, a **Bulk maintenance mode** setting lets you use a single token to uninstall or upgrade *all* hosts in that policy. **Bulk maintenance mode** is available when **Uninstall and maintenance protection** is enabled and the sensor version is set to **Sensor version updates off**.

Sensors must either be connected to the cloud or have connected to the cloud after **Bulk maintenance mode** was enabled to receive the bulk maintenance token. Otherwise, the AID-specific token is effective.

> **Important:** The **Bulk maintenance mode** token doesn't change. We recommend using this mode only if there are multiple hosts that require changes to the sensor. If the token becomes compromised, open a ticket through the CrowdStrike Customer Center .

To enable **Bulk maintenance mode**:

1. Go to **Host setup and management > Deploy > Sensor update policies** .
2. Click the policy that you want to edit.
3. In the **Senor version** dropdown menu, select **Sensor version updates off**.
4. Make sure that **Uninstall and maintenance protection** is selected.
5. Select **Bulk maintenance mode**, then click **Save**.
6. Click **Reveal token**.
7. In the **Maintenance token for assigned host** dialog, click **Reveal token**.

When **Bulk maintenance mode** is enabled, sensor-specific tokens from the Host Management page are disabled.

Test and deploy sensor update policies

We recommend setting up groups to test sensor updates in your environment, then updating all your hosts when you're ready.

1. Go to the **Sensor update policies** page at **Host setup and management > Deploy > Sensor update policies** .
2. Select an operating system from the **Platform** dropdown menu.
3. Click the default policy.
4. Select a target **Sensor version** for the default group. **We strongly recommend choosing a specific version**, not an `Auto` version, for the default group.
5. Go to the **Host groups** page at **Host setup and management > Manage endpoints > Host groups** to create your groups.
    1. Create a new custom group called "Test-QA Group." You should add a few hosts from each platform to the group that are not used in production. For more info, see Assign hosts to a host group .
    2. Create another new custom group called "Tech Pilot Group" that consists of more hosts from each platform, to include a limited number of non-critical production hosts.
    3. Create a third custom group called "Business Pilot Group" that contains a larger number of hosts, including production systems from multiple OUs, Departments, Sites, and so on. This allows you to determine if there are potential conflicts with specific applications/settings used by different OUs/Departments.

6. Return to the **Sensor update policies** page at **Host setup and management > Deploy > Sensor update policies** .
7. Set the "Test-QA Group" to the `Auto - Latest` version. This group always tests the latest available version.
8. Set specific builds for other groups, and create additional groups as needed.
9. After you feel comfortable with the build of your "Test-QA" group, configure your other groups to update to that version.

Best practices for sensor update policies

We recommend these general best practices for sensor update policies:

- We strongly recommend updating your hosts' sensors monthly to keep them on a recent version. If sensors can't be updated monthly, we recommend not letting sensors age more than 60 days after their release.
- To ensure that sensors function as expected, don't shut down or reboot the host while the sensor is being installed. Doing so can cause the host to repeatedly crash on boot or omit the uninstall option.
- Keep **Uninstall and maintenance protection** enabled for all sensor update policies, except for the one policy used for handling sensor uninstallation and maintenance. If you need to change or uninstall the sensor from hosts, move host groups to this policy with **Uninstall and maintenance protection** disabled and **Sensor version updates off** selected. This will ensure you can use this single policy to uninstall, upgrade, or downgrade host groups consisting even of hosts of different sensor versions.

Managing the DC sensor using a sensor update policy

Deploy or upgrade domain controller (DC) sensors quickly across your organization.

Requirements

- Falcon sensor
- Falcon Identity Threat Protection version 4.*x*

  > **Note:** Find your current Falcon Identity Threat Protection version at **Identity protection > Configure > Settings**.

To simultaneously update multiple DCs to the latest sensor version:

1. Go to **Identity protection > Configure > Identity configuration policies**.
2. Create a policy or edit the default policy. For more information about creating a policy and assigning host groups, see Creating a sensor update policy .

   > **Note:** The default policy is assigned to any device that's not assigned a higher-precedence policy. You can't assign host groups to the default policy.

   Update DC sensor Windows default policy
3. Optional. Test the DC sensor on a subset of DCs by clicking **Assigned host groups** and then

selecting the group that contains the relevant domain controllers.

> **Note:** Selecting the sensor update version directly on the default policy page rather than within a host group simultaneously deploys the DC sensor across all DCs covered by the default policy.

4. On the **Sensor Settings** tab, click **software updates off** and select the version that you want to deploy on DCs across your environment.

   Your changes are immediately implemented as long as the policy is enabled.

   Within 10 minutes, the sensors are installed on DCs assigned to the policy. No reboot is required.

   You can track the progress on the **Identity configuration policies** page.

   Note: Real Time Response session audit events are logged against your DC hosts from `cs_software_manager_distributor_identity_threat_detection@crowdstrike.com`.

Troubleshooting:

1. If the sensor isn't upgrading or deploying, confirm that the Falcon sensor is running on the DC.
   - For Windows, see Falcon sensor for Windows - Verify that the sensor is running .
   - For Linux, see Falcon sensor for Linux - Verify that the sensor is running .
   - For macOS, see Falcon sensor for Mac - Verify that the sensor is running .
2. On **Host setup and management > Manage endpoints > Host management**, locate the relevant DCs and review their assigned policies. In the **Real Time Response - High risk commands** section, confirm that **put** and **run** or **put-and-run** is enabled.
3. If the previous troubleshooting steps are not successful, create a Support ticket and provide the corresponding CSWinDiag collection. For more info see Using CSWinDiag for Falcon Sensor for Windows Diagnostics .