Sensor Update Policies

Last updated: Dec. 19, 2023

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 versions
- 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 [/documentation/category/e65fa298/sensor-deployment-and-maintenance/linux-kubernetes-and-cloud/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 Uninstall and maintenance protection [/documentation/page/d2d629cf/sensor-update-policies#o075803c] 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.

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 [/documentation/page/d2d629cf/sensor-update-policies#idffc036]
    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 [/configuration/sensor-update/policies].
2. Click **Add New Policy**.
3. Enter a policy name, description, and platform.
4. Click **Apply** to create the policy.
5. Select a sensor version for this 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 [/documentation/page/d2d629cf/sensor-update-policies#idffc036]
     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
6. Optional: schedule time blocks during which to prohibit sensor updates. See Schedule sensor cloud update exclusions [/documentation/page/d2d629cf/sensor-update-policies#wb9ccacf].
7. 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, read Managing sensor maintenance and uninstallation [/documentation/page/d2d629cf/sensor-update-policies#o075803c]
8. Click **Save**, then click **Confirm** to save your prevention settings.

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

Assigning a sensor update policy to a group

On the Policy Settings page:

1. Click **Add Groups**
2. Choose the groups you would like to add to the policy
3. Click **Apply**

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

Deleting a sensor update policy

Deleting a sensor update policy is a two-step process: disable the policy, then delete it.

1. Go to **Policy Detail**
2. Disable the policy you want to delete
3. After disabling, click **Delete**

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 [/documentation/page/bd0f1c7f/detection-and-prevention-policies#ic6fb2c0]. 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.

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 in as **Auto - Latest**.

To opt in to include early adopter builds for a sensor update policy, enable **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. For more info about creating a sensor update policy, see Sensor version management [/documentation/page/d2d629cf/sensor-update-policies#hc3b9d34].

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. 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 prohibit updates, you must enable scheduled exclusions and specify a time zone:

1. Go to **Host setup and management > Deploy > Sensor update policies**.
2. Create a new policy or update an existing policy.
3. On the **Settings** tab of the sensor update policy, in the **Sensor update schedule** section, enable the **Prohibit sensor updates during the following time blocks** setting.
4. Specify a time zone for the scheduled exclusions. This time zone applies to all exclusion periods you create. The default value for time zone is acquired from your browser's time zone setting.
   Important: The time zone you specify is used for admin reference, it's not the time zone used for hosts the policy applies to. For example, if you specify an exclusion during a time block of 4:00 - 6:00 and specify the Pacific time zone, the exclusion applies to the hosts from 4:00 - 6:00 Pacific time, NOT their local time.

Managing time blocks

To specify a sensor cloud update exclusion time block:

1. Open a sensor update policy and click the **Settings** tab.

2. In the **Sensor update schedule** section, make sure the **Prohibit sensor updates during the following time blocks** setting is enabled and a time zone is specified. See [Enabling scheduled exclusions [/documentation/page/d2d629cf/sensor-update-policies#v97bb69c]](/documentation/page/d2d629cf/sensor-update-policies#v97bb69c).
3. In the **Active time blocks** section, click **Create new time block** or select the time block you want to edit.
4. In the T**ime range** section, specify a start time and an end time for the new block. Time blocks must be at least one hour long.
5. In the **Day(s)** applied section, select the days you want this time block to apply to.
   Note: You can only create one time block per day of the week.
6. Click **Save time block**.
7. At the top of the **Sensor update policy settings** section, click **Save** to save the policy.
8. In the **Confirm policy change** dialog, click **Confirm**.

Sensor cloud updates are not applied to hosts during the time block specified.

Deleting a time block

To delete an existing sensor cloud update exclusion time block:

1. Open a sensor update policy and click the **Settings** tab.
2. In the **Active time blocks** section, click **Delete** 🗑 for the applicable time block.
3. At the top of the **Sensor update policy settings** section, click **Save** to save the policy.
4. In the **Confirm policy change** dialog, click **Confirm**.

> **Note:** The **Prohibit sensor updates during the following time blocks** setting is automatically disabled if you delete all time blocks.

Disabling scheduled exclusions

To disable scheduled exclusions:

1. Go to **Host setup and management > Deploy > Sensor update policies**.
2. Open the applicable policy to edit.
3. On the **Settings** tab of the sensor update policy, in the **Sensor update schedule** section, disable the **Prohibit sensor updates during the following time blocks** setting.
4. At the top of the **Sensor update policy settings** section, click **Save** to save the policy.
5. In the **Confirm policy change** dialog, click **Confirm**.

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

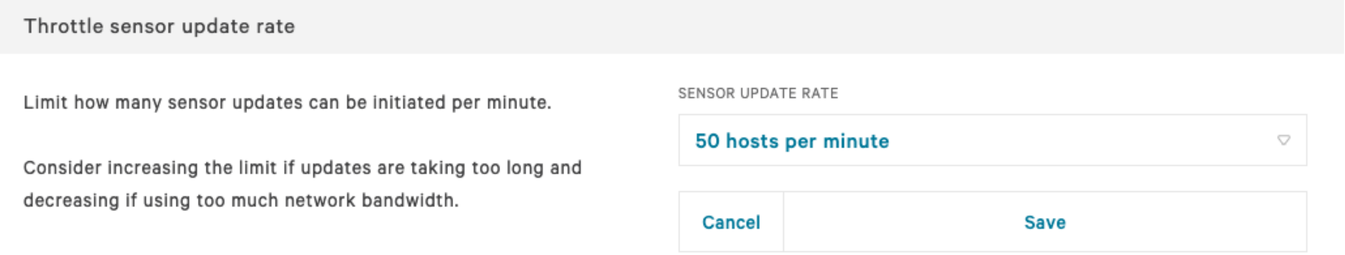
Sensor update throttling

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.

> 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 rate

Limit how many sensor updates can be initiated per minute.

Consider increasing the limit if updates are taking too long and decreasing if using too much network bandwidth.

SENSOR UPDATE RATE: 50 hosts per minute

Adjust the sensor update rate:

1. Go to Support and resources > Resources and tools > General settings [/configuration/general-settings] .
2. Use the **Sensor update rate** menu to select how many hosts receive sensor updates per minute.
3. Click **Save** when you're finished.

Channel file update throttling

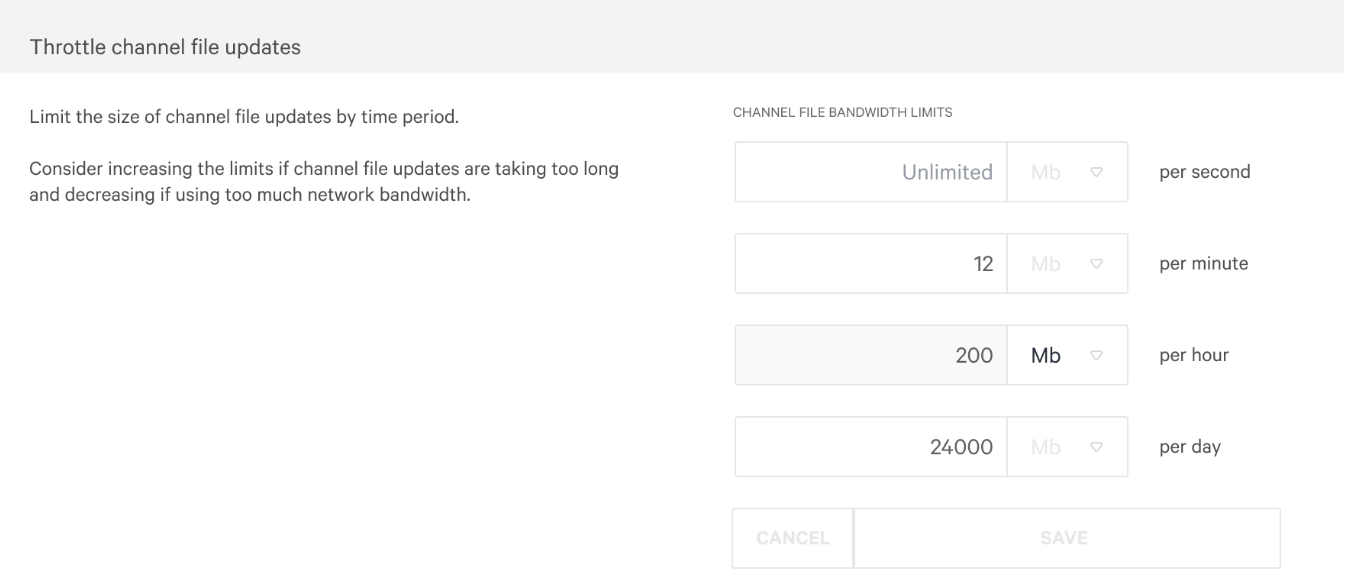
Channel file updates push dynamic content from the cloud to the sensor, including updates to policy and configuration settings. Most channel file updates are relatively small, ranging from 1K to 2MB in size. Because there are variations in update size, it's important to understand the range of channel 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.

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.



Throttle channel file updates

Limit the size of channel file updates by time period.

Consider increasing the limits if channel file updates are taking too long and decreasing if using too much network bandwidth.

CHANNEL FILE BANDWIDTH LIMITS

Unlimited Mb per second

12 Mb per minute

200 Mb per hour

24000 Mb per day

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

1. Go to Support and resources > Resources and tools > General settings [/configuration/general-settings].
2. 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.

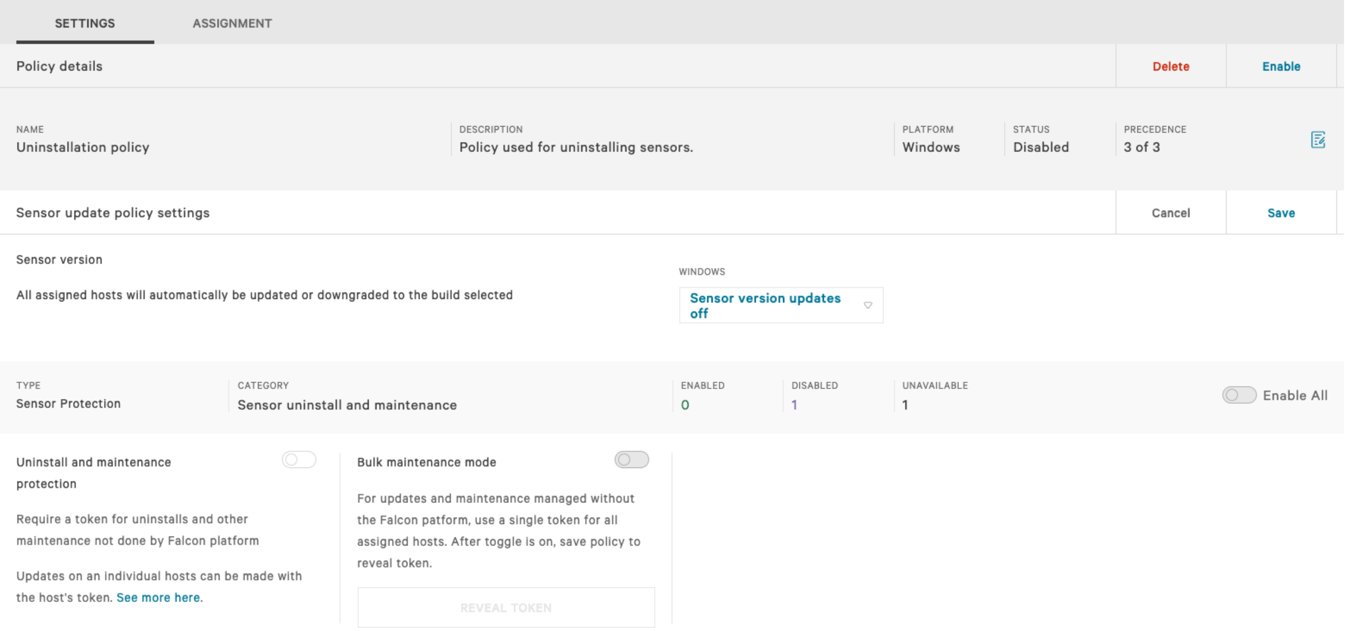
3. Click **Save** when you're finished.

Managing sensor maintenance and uninstallation

Windows and Mac sensor versions 5.10 and later

The **Uninstall and maintenance protection** setting within sensor update policies prevents unauthorized uninstallation of the sensor. Enabled by default, the setting controls whether an end user with local admin permissions can manually update or uninstall the sensor. For Windows sensor versions 6.42 and later, this setting also prevents unauthorized users from modifying sensor grouping tags.

Generally, 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.



Policy details

NAME: Uninstallation policy
DESCRIPTION: Policy used for uninstalling sensors.
PLATFORM: Windows
STATUS: Disabled
PRECEDENCE: 3 of 3

Sensor update policy settings

Sensor version

All assigned hosts will automatically be updated or downgraded to the build selected

WINDOWS: Sensor version updates off

TYPE: Sensor Protection
CATEGORY: Sensor uninstall and maintenance
ENABLED: 0
DISABLED: 1
UNAVAILABLE: 1
○ Enable All

Uninstall and maintenance protection ○

Require a token for uninstalls and other maintenance not done by Falcon platform

Updates on an individual hosts can be made with the host's token. See more here.

Bulk maintenance mode ○

For updates and maintenance managed without the Falcon patform, use a single token for all assigned hosts. After toggle is on, save policy to reveal token.

We also recommend disabling **Uninstall and maintenance protection** when downgrading a sensor update group from sensor version 5.10 or later to 4.28 or earlier to ensure the AID-specific maintenance token that allows for uninstallation is cleared before the hosts downgrade to the older version. You can enable **Uninstall and maintenance protection** again after updating the sensor update policy to 5.10 or later.

Single-use, AID-specific maintenance tokens allow for the sensor to be uninstalled if a host is offline or if time-sensitive changes are needed. Users with the Falcon Admin or Endpoint Manager role can reveal maintenance tokens.

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

- Windows Deployment Guide [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment]
- Mac Deployment Guide [/documentation/page/e261a9b7/falcon-sensor-for-mac-deployment]
- Linux Deployment Guide [/documentation/category/86/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.

On the Host Management page [/hosts/hosts]:

1. Find the host
2. Open its summary panel
3. Click **Reveal maintenance token**
4. Enter a reason for revealing the token (recorded in the Audit Log [/investigate/events/en-US/app/eam2/audit_app?earliest=-14d&latest=now&form.analyst_tok=*&form.service_tok=*&form.customer_tok=*])
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 [https://supportportal.crowdstrike.com/s/login_page/?startURL=%2Fs%2F&ec=302].

On the Sensor Update Policies [/configuration/sensor-update/policies] page:

1. Find the policy, then click **Edit policy**
2. Set the **Sensor version** to **Sensor version updates off**
3. Make sure **Uninstall and maintenance protection** is enabled
4. Enable **Bulk maintenance mode**, then click **Reveal**
5. Enter a reason for revealing the token (recorded in the Audit Log [/investigate/events/en-US/app/eam2/audit_app?earliest=-14d&latest=now&form.analyst_tok=*&form.service_tok=*&form.customer_tok=*])
6. Click **Reveal Token**

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

> Sensor version 4.28 and earlier

Cloud-managed uninstall protection is not supported until 5.10.

Best practices for 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 **Sensor Update Policies**.
2. Click **Edit** icon on the default policy page.
3. Set a target version for the default group. **We strongly recommend choosing a specific version**, not an `Auto` version, for the default group.
4. Go to Host groups [/hosts/groups-new] (**Host setup and management** > **Manage endpoints** > **Host groups**) to create your groups.
    - 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.
    - 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.
    - 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.
5. Return to **Sensor Update Policies**.
6. Set the "Test-QA Group" to the `Auto` version. This group always tests the latest available version.
7. Set specific builds for other groups, and create additional groups as needed.
8. After you feel comfortable with the build of your "Test-QA" group, configure your other groups to update to that version.

We also recommend these general best practices:

- If possible, 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

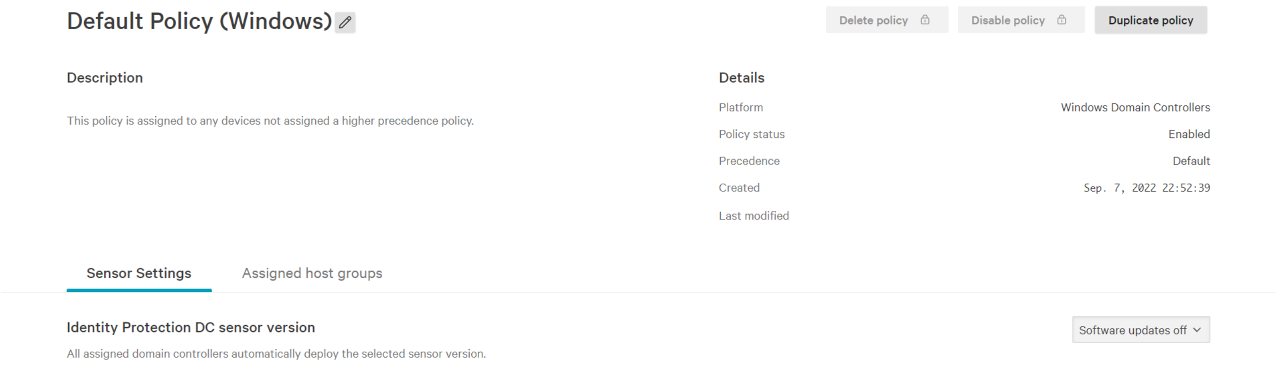
Deploy or upgrade domain controller (DC) sensors quickly across your organization.

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 [/documentation/page/d2d629cf/sensor-update-policies#od687218].
   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.



Default Policy (Windows)

Description

This policy is assigned to any devices not assigned a higher precedence policy.

Details

Platform	Windows Domain Controllers
Policy status	Enabled
Precedence	Default
Created	Sep. 7, 2022 22:52:39
Last modified	

Identity Protection DC sensor version

All assigned domain controllers automatically deploy the selected sensor version.

Software updates off

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 [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#ee039a51].
   - For Linux, see Falcon sensor for Linux - Verify that the sensor is running [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#ee039a51].
   - For macOS, see Falcon sensor for Mac - Verify that the sensor is running [/documentation/page/ecc97e75/falcon-sensor-for-windows-deployment#ee039a51].

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 [https://supportportal.crowdstrike.com/s/article/Using-CSWinDiag-for-Falcon-Sensor-for-Windows-Diagnostics]

   .

< Cloud IP Addresses and FQDNs[/documentation/page/e87d1418/ Sensor Health Monitoring > [/documentation/page/cf07afb6/sensor-health-monitoring]