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

Overview

Content update policies control how content updates are deployed to your hosts.

Content updates contain content packages, which deliver configuration information from the CrowdStrike cloud to Falcon sensors. These packages are necessary to maintain security posture and sensor health.

Content updates consist of these categories:

- System Critical
- Sensor Operations
- Rapid Response
- Vulnerability Management

> **Note:** Vulnerability Management content packages are only available with the Falcon Exposure Management or Falcon Spotlight subscriptions.

Content updates differ and are deployed separately from sensor software updates.

Requirements

Subscription: Falcon Insight XDR, Falcon Prevent

Sensor support: All supported sensor versions

Default roles: Content Control Manager

CrowdStrike clouds: Available in all clouds

Content update categories

There are several content update categories that deliver specific types of content packages. You can configure the deployment of some CrowdStrike-initiated content packages with content update policies.

- System Critical, Sensor Operations, Rapid Response, and Vulnerability Management content packages are controlled by content update policies.
- Customer-initiated policy content packages, such as IOC Management, are deployed automatically when customer-initiated configuration changes are made. These changes can be

made using either the Falcon console or CrowdStrike APIs.

Content Package Category	Purpose	Includes
System Critical content packages	Required by the Falcon sensor for ongoing operating system stability.	• Operating system and sensor classification • Global allowlists and policy controls, ensuring that the sensor does not interfere with critical OS files
Sensor Operations content packages	Include Windows OS Feature Manager (OSFM) and Zero Touch Linux (ZTL) updates, which ensure the Falcon sensor's compatibility in response to vendor-provided operating system kernel updates for Windows and Linux. Keeping these packages up-to-date is important to avoid Reduced Functionality Mode (RFM).	• OS Feature Manager • Zero Touch Linux • Tampering protection • General sensor settings • OS and application compatibility settings for Falcon Exposure Management • OS and application compatibility settings for Falcon for Mobile
Vulnerability Management content packages	Provide the sensor with vulnerability definitions and data. **Note:** Vulnerability Management content packages are only available with the Falcon Exposure Management or Falcon Spotlight subscriptions.	• Vulnerability identification rules
Rapid Response content packages	Provide behavioral IOAs as well as telemetry, detection, and prevention logic to the Falcon sensor on an ongoing basis. Provide false positive/false negative mitigation updates for IOA and ML content.	• Behavioral IOA Content • IOC Data • Detection Configuration Settings • Tampering Protection • CrowdStrike-initiated allowlisting and blocklisting
Customer-initiated content packages	Customer-defined policies for Falcon modules based on the configurations made using the Falcon console or APIs. **Note:** These packages are deployed after	• Custom IOAs • Network containment • Real-Time Response • Allowlisting and blocklisting through

	customer-initiated configuration changes and aren't controlled by content update policies.	IOC management • Machine learning exclusions • Certificate-based allowlisting • IOA and sensor visibility exclusions • Sensor update and prevention policies • Falcon FileVantage policy • Falcon Data Protection policy • Falcon Identity Protection policy • On-demand scans • Falcon Exposure Management configuration assessment • Device control policy • Firmware analysis policy • Falcon Cloud Security policy

Content update deployment options

You can configure these deployment options:

- **GA** (strongly recommended): Receive content updates during general availability. General availability (GA) is a phased rollout after a successful deployment to early access hosts. When selecting **GA**, you have the option to specify a delay period. For example, if you select a 4 hour delay, you'll start receiving content updates for that category 4 hours after general availability is complete.

- **Early access**: Receive content updates following successful internal testing and deployment to all CrowdStrike assets. Early Access content has been fully tested by CrowdStrike and is considered stable and ready for production.

- **Pause** (not recommended): Your sensor won't receive content updates. The **Pause** option affects sensor performance in these ways:

    - If Sensor Operations content packages are paused, your sensors won't receive sensor configuration updates, which will impact operating system and application compatibility and may lead to reduced functionality mode (RFM) on Windows and Linux hosts.

    - If Rapid Response content packages are paused, your sensors won't receive behavioral IOA, allowlisting, and blocklisting updates generated by CrowdStrike threat researchers and analysts.

- If Vulnerability Management content packages are paused, your sensors won't receive updated vulnerability definitions and data.
- **Important:** This option isn't available for System Critical content packages.

Note: The behavior of paused content updates differs for newly installed sensors and existing sensors that check for content updates. For more info, see Behavior for New and Existing Sensors When Content Updates Are Paused .

Manage content update policies

Configure content package deployment options for your host groups.

Falcon Flight Control support

Content update policies are supported for Falcon Flight Control environments. Like all policies that support Flight Control environments in the Falcon console, content update policies configured in a parent CID are available in child CIDs. Content update policies can also be configured in a child CID. See our Falcon Flight Control documentation Managing policies .

Note: If you're in a child CID and you're using the override feature, you can't apply an override to parent CID policies.

Create a content update policy

Create, configure, and assign host groups to a content update policy.

1. Go to **Host setup and management > Deploy > Content update policies** .
2. Click **Create policy**.
3. Enter a name for the policy and optional description.
4. Click **Create policy**.
5. On the **Settings** tab, configure content package deployment settings. If you select **GA** as the deployment option for any content category, you can optionally select a delay period.
6. Click **Save**, and then click **Save**.
7. Assign host groups.
    1. Click the **Assigned host groups** tab.
    2. Click **Assign host groups to a policy**.
    3. Select the host groups you want covered by the policy, and then click **Assign groups**.

       Host group changes are automatically saved.
8. To enable the policy, click **Enable policy**.

Duplicate a content update policy

Duplicate a policy's deployment settings. By default, duplicated policies are disabled and aren't assigned to any host groups.

1. Go to **Host setup and management > Deploy > Content update policies** .
2. Click the policy that you want to duplicate.
3. Click **Duplicate policy**.
4. Enter a name for the policy and optional description.

Click **Duplicate**.

Edit content update policy settings

Edit deployment settings, assigned host groups, or the name or description of the policy.

1. Go to **Host setup and management > Deploy > Content update policies** .
2. Find the policy to edit and click the policy name.
3. Edit policy settings as needed.
    - To edit the name or description, click **Edit name or description** .
    - To enable or disable a policy, click **Enable policy** or **Disable policy**.
    - To edit deployment settings, select settings as needed on the **Settings** tab, click **Save**, and then click **Save**.
4. Add or remove host groups as needed in the **Assigned host groups** tab.
    - To add groups, click **Assign host groups to policy**, select the groups, and then click **Assign groups**.
    - To remove a group, click the action menu for the group's entry, select **Remove from policy**, and then click **Remove from policy**.

      Host group changes are automatically saved.

Delete a content update policy

Delete a policy that's no longer needed. Policies must be disabled before they can be deleted.

1. Go to **Host setup and management > Deploy > Content update policies** .
2. Find the policy to delete and click the policy name.
3. If the policy is enabled, click **Disable policy**, and then click **Disable policy**.
4. Click **Delete policy** and then click **Delete policy**.

Edit content update policy precedence

Policy precedence determines which policy is applied if a host is assigned to multiple policies.

1. Go to **Host setup and management > Deploy > Content update policies** .
2. Click **Edit precedence**.
3. Drag and drop policies to the needed positions.

   Note: The default policy always has the lowest precedence and cannot be reordered.
4. Click **Save**.

Overriding deployment settings

You can override content update deployment settings for one or more policies at a time. This option either allows all content updates at general availability or it pauses updates for all categories including System Critical.

You can also revert the override applied to selected policies. The policy settings return to what was configured before the override was applied.

Consider these points when configuring overrides:

- If an override is applied to a policy, you can't modify that policy's individual deployment settings unless the override for that policy is reverted. You can see what the policy's deployment settings were configured to use before the override was applied by opening the policy on the **Content Update Policies** page.
- If you configure an override to allow all content updates, your sensors will receive updates at the GA delivery phase. For example, if one of the content categories in the policy is set to EA, sensors will instead receive updates at GA with the override enabled.
- If you pause content updates, your sensors' security posture is reduced and your Windows and Linux hosts could go into reduced functionality mode (RFM).
- If you use Falcon Flight Control and you're in a child CID, you can't apply an override to parent CID policies.

Apply override settings

Override policy settings to allow or pause content updates.

1. Go to **Host setup and management > Deploy > Content update policies** .
2. Select one or more policies.
3. Click **Override**.
4. Select whether to allow or pause content updates for hosts that belong to one or more groups the policies are applied to.
5. Click **Override policy**.

Revert override settings

Revert the override applied to one or more policies. The policy settings return to what was configured before the override was applied.

1. Go to **Host setup and management > Deploy > Content update policies** .
2. Select one or more policies.
3. Click **Revert overrides**.
4. Click **Revert policy overrides**.

Version pinning

Version pinning sets a specific version for a content update category in a content update policy. This ensures hosts with that policy applied stay at the specified version and don't receive updates for that category unless the version pin is removed or changed.

You can set or remove pinned versions only using the CrowdStrike API.

For more info, see Content Update Policy APIs .

You can view whether versions are pinned in these areas of the Falcon console:

- On the **Content update policies** page (**Host setup and management > Deploy > Content update policies**), the **Pinned categories** column shows whether any categories are pinned.
- In a content update policy, any category deployment settings that have a version pinned are read-only in the Falcon console. If you hover over a category with a pinned version, a tooltip opens showing the pinned version.
- On the **Host Management** page, the **Content update states** tab (**Host setup and management > Manage endpoints > Content update states**) displays whether a version is pinned to a host in the policy settings columns. You can also filter policy settings by **Pinned**.

Version pinning considerations

Consider these points when pinning versions:

- To avoid compromising your security posture, we strongly recommend updating pinned versions to the latest available content for that category no more than 72 hours after that content is released.
- If you apply version pinning to the System Critical or Sensor Operations category, your sensors won't receive the latest available sensor configuration updates, which will impact operating system and application compatibility and might lead to reduced functionality mode (RFM) on Windows and Linux hosts.
- Pinning a content version that's older than what's currently installed on the sensor can result in content being downgraded to the pinned version. There are a few exceptions for certain channel files that don't support downgrades.
- You must actively track and manage content categories that are pinned. The Falcon console

won't provide reminders or notifications to update pinned content as it ages.

- If a content update policy has a version pinned to a content update category, you can't change that category's deployment setting or apply a policy override unless the pinned version is removed.
- If a content update policy has an override applied, you can't pin a version to the policy unless the override is removed.

Viewing which content updates are applied to hosts

The **Content update states** page in host management, at **Host setup and management > Manage endpoints > Content update states** , shows a list of your hosts and a timestamp of the last content package updates that have been applied for each content category. For more info, see View content update states .

View audit log entries for content update policies

You can filter the audit log to see when configuration changes were made to content update policies.

1. Go to **Audit logs > Audit logs > Falcon UI** .
2. Filter by **Service: Content update policy**.

Get notified of content update policy changes notifications

You can create Fusion SOAR workflows to send notification settings when a content update policy is created, edited, or deleted. Use these event trigger settings to configure your workflow:

- **Trigger: Audit event > Policy**

  Search for `policy` and then expand **Utilities**.
- **Type: Deleted**, **Created**, **Enabled**, **Disabled**, Updated, or **All**
- **Add a condition:**
  - **Parameter: Policy type**
  - **Operator: is equal to**
  - **Value: Content Update**

For more info about Fusion SOAR, including detailed instructions for configuring workflows, see Fusion SOAR .

Schedule maintenance windows with Fusion SOAR

Create a scheduled workflow with Falcon Fusion SOAR to automatically set content update settings for a policy. This feature helps you pause or enable content updates during a specified time frame.

Use the **Update content policy** action to configure these settings:

- **Policy type: Content update policy**
- **Policy:** Select the content update policy to apply the workflow to.
- **Content category:** Select the applicable content category. If the policy has settings for more than one content category, you must create a workflow for each.
- **Release schedule:** Select when you want content updates deployed.

For example, you can set content updates to pause Vulnerability Management content package updates on weekends and become active again during weekdays. For this example, create two workflows: one to enable content updates, and another to disable them. First, create a workflow with a trigger for Monday morning at 8:00 AM and use these **Update content policy** action settings:

- **Policy type: Content update policy**
- **Policy:** The name of your policy
- **Content category: Vulnerability Management**
- **Release schedule: General Availability**

Then, create another workflow with a trigger for Friday evening at 7:00 PM. Use the same settings as the first workflow except select the **Deployment phase** to **Pause**. Together these workflows create a time frame where sensors don't receive Vulnerability Management content package updates.

To quickly create a scheduled workflow to manage the content update policy, a new playbook is available called **Configure content update policy**. For more info, see Fusion SOAR Playbooks .

For more info about Fusion SOAR, including detailed instructions for configuring workflows, see Fusion SOAR .

View content package updates deployment status

Use the **Content quality dashboard** to get a global view of content package updates and their current statuses.

1. In the Falcon console, go to **Dashboards and reports > Dashboards > Content quality dashboard** .
2. For each release version, view the applicable content categories. Only content categories that are included in the deployment show a status. For each applicable content category, view the status for early access (EA) and general availability (GA). These statuses are available:
    - **Pending**: The deployment is ready to begin when the previous stage is complete.
    - **In progress**: The phased deployment of the content package updates has started. If a deployment is paused, its status remains in progress until it is started again and completed, or aborted.

- **Completed time stamp**: The deployment has completed rollout to all hosts for the applicable phase. The time stamp of completed deployment is displayed.

  > **Important:** The timestamp on the Content quality dashboard indicates when the phase was completed on all hosts. Individual hosts receive content updates as part of a gradual rollout. You can view when a specific host received a content update in host management. See View content update states .

- **Aborted**: The deployment has been aborted. An aborted deployment won't be restarted or completed but might be rectified by a subsequent release.

Throttling channel file updates

If your environment has limited bandwidth, you can throttle the rate at which channel files are downloaded. For more info, see Channel file update throttling .