Falcon for Legacy Systems - Prevention Policy Settings

Last updated: Apr. 21, 2025

Overview

Falcon for Legacy Systems lets you see events from endpoints in your environment that use legacy Windows OS.

After deploying the sensor, use the Falcon console to configure prevention policies. Prevention policies consist of sensor settings that are applied to hosts based on assigned host groups.

For more info on deploying Falcon for Legacy Systems, see
Falcon Sensor for Legacy Systems Deployment [/documentation/page/j86ac82d/falcon-sensor-for-legacy-systems-deployment].

Prevention policy sensor settings

Falcon for Legacy systems' policies contain sensor settings that determine whether a detection or preventative action should be taken.

Recommended prevention policy settings

The table provides recommendations for prevention policy settings available for legacy Windows endpoints.

Type	Setting	Description	Recommendations
Cloud machine learning	Detection enabled	Detect malicious processes the moment they are executed.	Enable.
Cloud machine learning	Prevention enabled	Block malicious processes from starting and terminate malicious processes that are already running.	Disable for initial deployments, then enable after a period of detection triage and allowlisting as appropriate.
Sensor configuration	Disable sensor	Temporarily disable the sensor's monitoring and protection capabilities on assigned endpoints, typically used for troubleshooting purposes.	Do not enable this setting unless directed by Support, or if you need to diagnose any issues.

Managing policies

Configure sensor settings and assign host groups to policies.

Create a policy

Create prevention policies that are applied to host groups.

Create and enable a policy.

1. Go to **Endpoint security > Configure > Prevention Policies [/policies/prevention]**.
2. Enter a name, description and platform, and then click **Create Policy**.
3. Optional. To enable the policy you just created, click **Enable policy**.

Delete or duplicate a policy

Delete policies you no longer need or duplicate existing policies to create similar configurations quickly.

Delete or duplicate a policy. Policies must be disabled before they can be deleted.

If you want to keep a policy but not enforce it, disable the policy. You can also duplicate any policy you previously created.

> **Note:** The default policy can't be deleted.

1. Go to Endpoint security > Configure > Prevention Policies [/policies/prevention]
2. Find and click on the name of the policy you want to duplicate or delete.
3. If needed, click **Disable** to disable the policy.
4. Click **Delete policy** or **Duplicate policy**.

Configure sensor settings

Configure sensor settings to control how the sensor operates on your endpoints.

Enable or disable sensor settings based on the requirements of your environment.

Modifications are automatically saved and are pushed to devices immediately. For more information on the available settings, see Prevention policy sensor settings.

1. Go to Endpoint security > Configure > Prevention Policies [/policies/prevention].
2. Find the policy you want to configure and click on its name.
3. Enable or disable settings as needed.

Assign or remove host groups

The host groups assigned to a policy determine which hosts the policy is applied to.

1. Go to **Endpoint security > Configure > Prevention Policies**.
2. Find the policy to configure and click on the name of the policy**.**
3. Click the **Assigned host groups** tab.
4. To add a host group to the policy:
    a. Click **Assign host groups to policy**.
    b. Select each group from the menu.
    Tip: Type the group name in the text field to dynamically search for groups.
    c. Click **Assign groups**.
5. To remove a group from the policy:
    a. Find the group you want to remove and then click **Open menu** ⋮ , then click **Remove from policy**.

Click **Remove group from policy**.

‹ Falcon Sensor for Legacy Systems Deployment[/documentation/page/j86ac82d/falcon-sensor-for-legacy-systems-deployment]