chrome enterprise

CROWDSTRIKE

# Getting started with the Crowdstrike Falcon Next-Gen SIEM integration in Chrome Enterprise Core

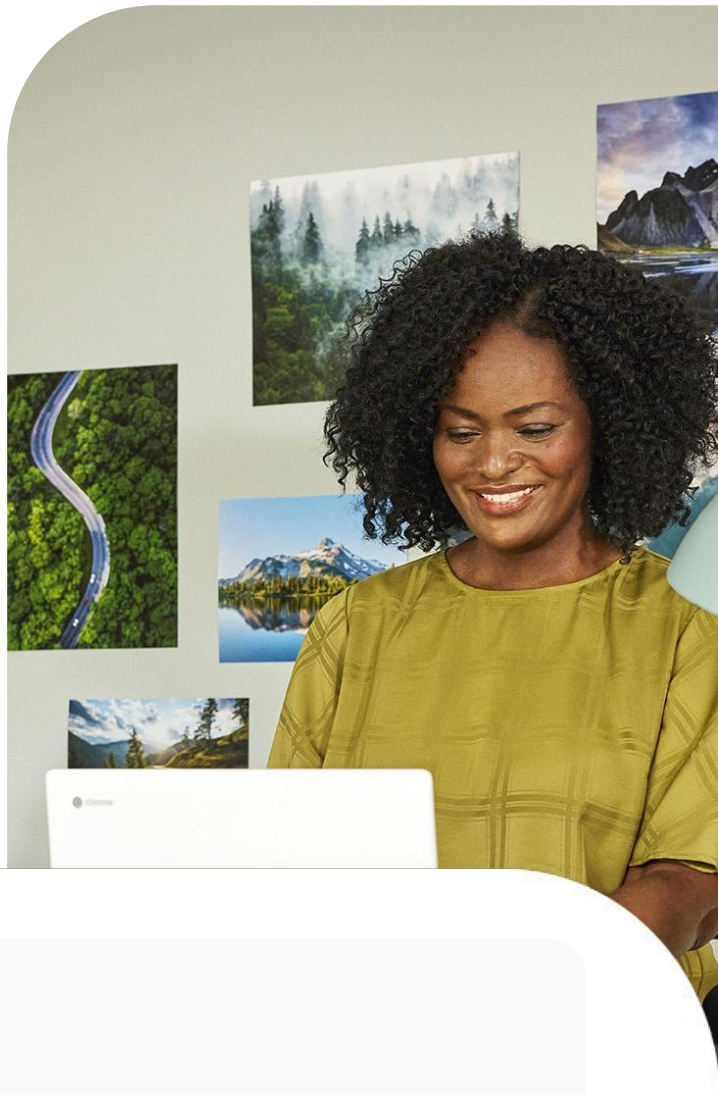
April 2025

# Resources

This document will guide you through the process of setting up the reporting integration between Chrome Enterprise Core and CrowdStrike Falcon Next-Gen SIEM. Note that this feature requires devices to be enrolled into Chrome Enterprise Core.

- Setting up Chrome Enterprise Core
- Best practices for using Chrome Enterprise Core
- Help Center Article for Chrome Enterprise Connectors Framework

# What data gets sent to CrowdStrike Falcon Next-Gen SIEM from Chrome browser?



The following data is sent from Chrome browser to CrowdStrike Falcon Next-Gen SIEM once the integration is set up. The data is also logged in the Google Admin console under Reporting>Audit and investigation>Chrome log events. For more information, please review this Help Center article.

**Here is a brief overview of just a few of the events captured:**

| Event value | Description |
|---|---|
| Malware transfer | The content uploaded or downloaded by the user is considered to be malicious, dangerous, or unwanted |
| Password changed | The user resets their password for the first-signed-in user account |
| Password reuse | The user has entered a password into a URL that's outside of the list of allowed enterprise login URLs |
| Unsafe site visit | The URL visited by the user is considered to be deceptive or malicious |

**For a complete list of all of the events that can be sent, please review this help center article.**

# Set up Chrome Enterprise connectors within CrowdStrike Falcon Next-Gen SIEM

1. Log into your CrowdStrike Falcon Next-Gen instance.
2. You will need to Set up a HEC/HTTP Event Data Connector to ingest your Google Chrome data. If you aren't sure how to do this, see HEC/HTTP Connector Guide.
3. Once you're in the Add new connector page, select the json (Generic Source) parser. Otherwise, follow the instructions within the guide in the previous step.
4. Once a banner is displayed stating the connector is ready to receive data, click on the Generate API Key button.
5. Save the API Key and API URL as you will be entering this into the admin console in the following section.

# Set up the CrowdStrike Falcon Next-Gen SIEM Configuration in the Google Admin Console

1. Log into the Google Admin console at admin.google.com and select the organizational unit that contains the enrolled browsers from which you want to send security events to CrowdStrike Falcon Next-Gen SIEM.
2. Navigate to Devices>Chrome>Users and browsers. Add a filter for “security events”.
3. Under Security events reporting, select Allow selected events. Under the additional settings you can also specify which events you want to send to CrowdStrike.
4. Now that the events are turned on, click on the blue hyperlink called “Reporting connector provider configurations” to take you to the connector provider configurations, or it can found under Devices>Chrome>Connectors.
5. Click the New Provider Configuration button and select CrowdStrike Falcon Next-Gen SIEM as the provider.
6. Enter the configuration name that you want this connector to display as in the Google Admin console.
7. Enter the hostname (API URL) of your CrowdStrike Falcon Next-Gen SIEM and the ingest token value (API Key) from step 4 of the last section.
8. Press the Add Configuration to save.
9. Select the Organizational Unit that the reporting events are turned on in and select the Chrome CrowdStrike Falcon Next-Gen SIEM connector that was created in the previous step and hit Save.

# View Chrome Events in CrowdStrike Falcon Next-Gen SIEM

Events will start being sent to CrowdStrike Falcon Next-Gen SIEM once the changed policy is applied to the enrolled machines in Chrome Enterprise Core.

**For more information about what events are sent to Crowdstrike Falcon Next-Gen SIEM, please review this Help Center article.**

Note that password events will only be sent if the feature is turned on. For more information about Password Alert, please review this blog.

Chrome Data Protection events are available only for customers who have purchased Chrome Enterprise Premium. For more information about Chrome Enterprise Premium and how to set it up, go to Protect Chrome users with Chrome Enterprise Premium Threat and Data Protection.