chrome enterprise

Google Security Operations

Integrate Google Security Operations with Chrome Enterprise in Chrome Enterprise Core

October 2025

Table of Contents

Resources

This document will guide you through the process of setting up the reporting integration between Chrome Enterprise Core and Google Security Operations. Note that this feature requires devices to be enrolled into Chrome Enterprise Core to send security events to Google Security Operations.

Here are some useful links:

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

What data gets sent to Google Security Operations from Chrome browser?

The following data is sent from Chrome browser to Google Security Operations 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.

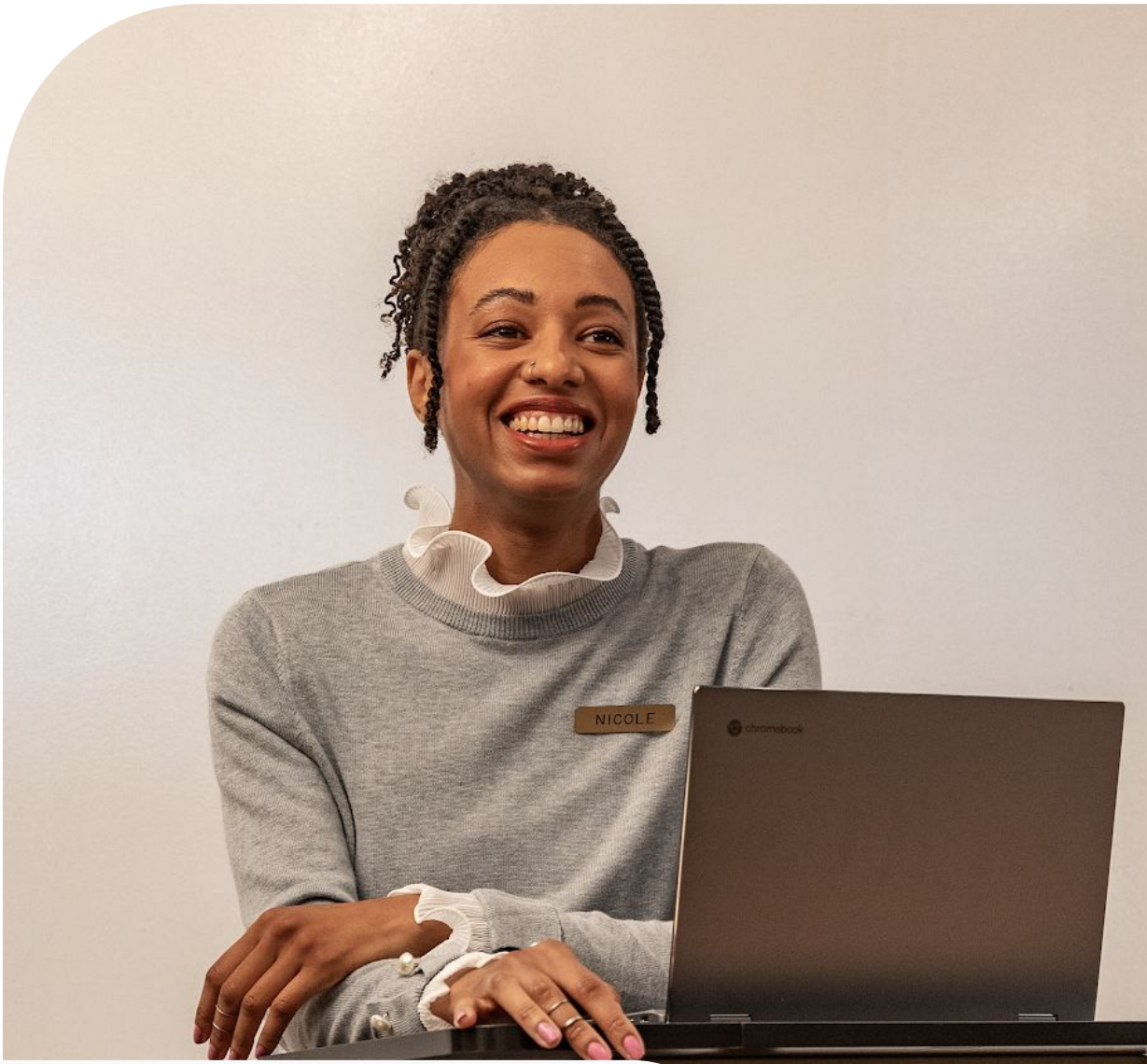
Here is a brief overview of just a few of the events captured:

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 the Google Security Operations 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 Google Security Operations.
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 Google SecOps.
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 Chrome browser>Connectors.
5. Click the New Provider Configuration button and select Google Security Operations (Keyless integration) as the provider.
6. Enter the configuration name that you want this connector to display as in the Google Admin console.
7. How you setup the configuration depends on how your Google Security Operations (SecOps) instance is set up relative to your Google Workspace domain:
    a. Your Google SecOps instance is within the same Google Cloud Platform (GCP) Organization as your Google Workspace domain–Select the “Use instance in associated GCP account” radio button. After that, select the relevant instance from the “SecOps Instance” dropdown.
    b. Your Google SecOps instance is located outside of your GCP organization–You’ll need to generate a token. Follow the instructions on the next page to obtain a token. Once generated, select the “Use instance outside of your organization” radio button and paste the token into the provided text field.
    c. A Google SecOps instance wasn’t found–You’ll need to generate a token. Follow the instructions on the next page to obtain a token. Once generated, paste it into the provided text field.
8. Press the Test connection button then press Add Configuration to save.
9. Select the Organizational Unit that the reporting events are turned on in and select the Google Security Operations connector that was created in the previous step and hit Save.



Generate a token in the Google Security Operations Platform

Follow the instructions here to generate a token in SecOps.
Then go back to the previous page and follow steps 7-9.

View Chrome events in Google Security Operations

Alerts from managed browsers will start being sent to Google Security Operations once the policy is applied in Chrome Browser Cloud Management. Ingested events include fields like accessed domain, downloaded file hash, and username. Each of these can be found within Google Security Operations using the following methods:

- **Search & Investigative Views**: Username, hash, domain, and IP values can be directly entered into Google SecOp's search bar, and results will be materialized in Google SecOp's respective investigative views
- Google SecOps **Detect**: Customers can create or enhance existing threat detection rules using Chrome alert data
- **Raw Log Scan**: Customers can use Google SecOp's Raw Log Scan capability to search over raw data

For more information about what events are sent to Google SecOps, please review this Help Center article and Google SecOps documentation

- 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.