chrome enterprise

splunk>

# Getting started with the Splunk integration in Chrome Browser Cloud Management

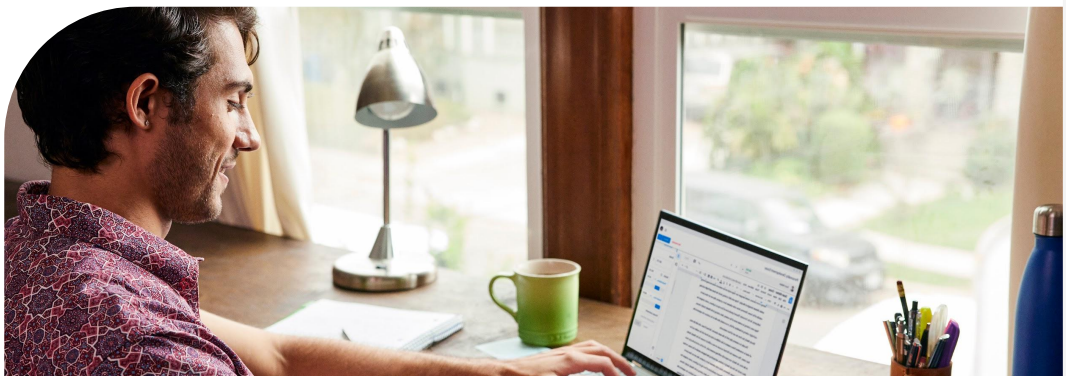
June 2023

# Resources

This document will guide you through the process of setting up the integration between Chrome Browser Cloud Management and Splunk. Note that this feature requires devices to be enrolled into Chrome Browser Cloud Management.

**Here are some useful links:**

- Setting up Chrome Browser Cloud Management
- Best practices for using Chrome Browser Cloud Management
- Google Chrome Add-on for Splunk
- Splunk Add-on installs as documented for a Single Server Install or a Distributed Environment Install.
- Help Center Article for Chrome Enterprise Connectors Framework
- Getting started with the Google Chrome app for Splunk



## The value of the Chrome browser and Splunk integration

The integration between Splunk and the Chrome browser provides valuable insights into unsafe behavior and potential attackers targeting your enterprise. Through the Splunk integration, Chrome offers insights into security events such as malware transfers, visits to unsafe sites, password reuse, and more. By having visibility into these events, you can gain even more confidence in detecting malicious activity and respond quickly to prevent possible breaches.

Once the integration is set up, the data is sent from the Chrome browser to Splunk. Additionally, the data is logged in the Google Admin console under Reporting > Audit and Investigation > Chrome log events. For more information, please review this Help Center article.

## Set up the Splunk configuration in the Google Admin console

1. Log into the Google Admin console at admin.google.com.
2. Navigate to Devices>Chrome>Users and browsers. Add a filter for “Events reporting”.
3. Under Events reporting, select Enable event reporting. Under the additional settings you can also specify which events you want to send to Splunk
4. Now that the events are turned on, click on this blue hyperlink to take use to the connector provider configurations, or it can found under Devices>Chrome>Connectors.
5. Click the New Provider Configuration button and select Splunk as the provider.
6. Enter the configuration name that you want this connector to display as in the Google Admin console.
7. Enter the domain name of your Splunk instance and the token id generated from the HEC Splunk creation process.
    a. Note that you only need to add your domain name, not the full path to your Splunk HEC. Entering the full path will result in an error, since the “services/collector/event” part of the HEC path is added programatically.
    b. For more information about sending data to a event collector, please refer to this Splunk documentation.
8. Press the Add Configuration to save.
9. Select the Organizational Unit that the reporting events are turned on in and select the Chrome Splunk connector that was created in the previous step and hit Save.

## Install the Google Chrome Add-on for Splunk

Install the Google Chrome Technical Add-on for your Splunk instance.

1. More details about the install process is located via this link.
2. For customer-managed deployments, refer to the standard methods for Splunk Add-on installs as documented for a Single Server Install or a Distributed Environment Install.
3. Steps for installing addons for Splunk Cloud, refer to Install apps in your Splunk Cloud Deployment.

## Getting started with the Google Chrome App for Splunk

The Google Chrome App for Splunk provides users with pre built dashboards and analytics to help investigate the most critical incidents of risky extension installs, malware transfer and unsafe site visits. The solution also includes incident response or automation-driven detections, simplifying the process of responding to critical incidents. View the most updated instruction on how to set up Google Chrome App for Splunk on the Splunk Lantern page.

# View Chrome events in Splunk

Events will start being sent to Splunk once the changed policy is applied to the enrolled machines in Chrome Browser Cloud Management.

The source name override you have specified during the setup of the HEC in Splunk is the keyword to search for Chrome events.

**For more information about what events are sent to Splunk, 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 BeyondCorp Enterprise. For more information about BeyondCorp and how to set it up, go to Protect Chrome users with BeyondCorp Threat and Data Protection.