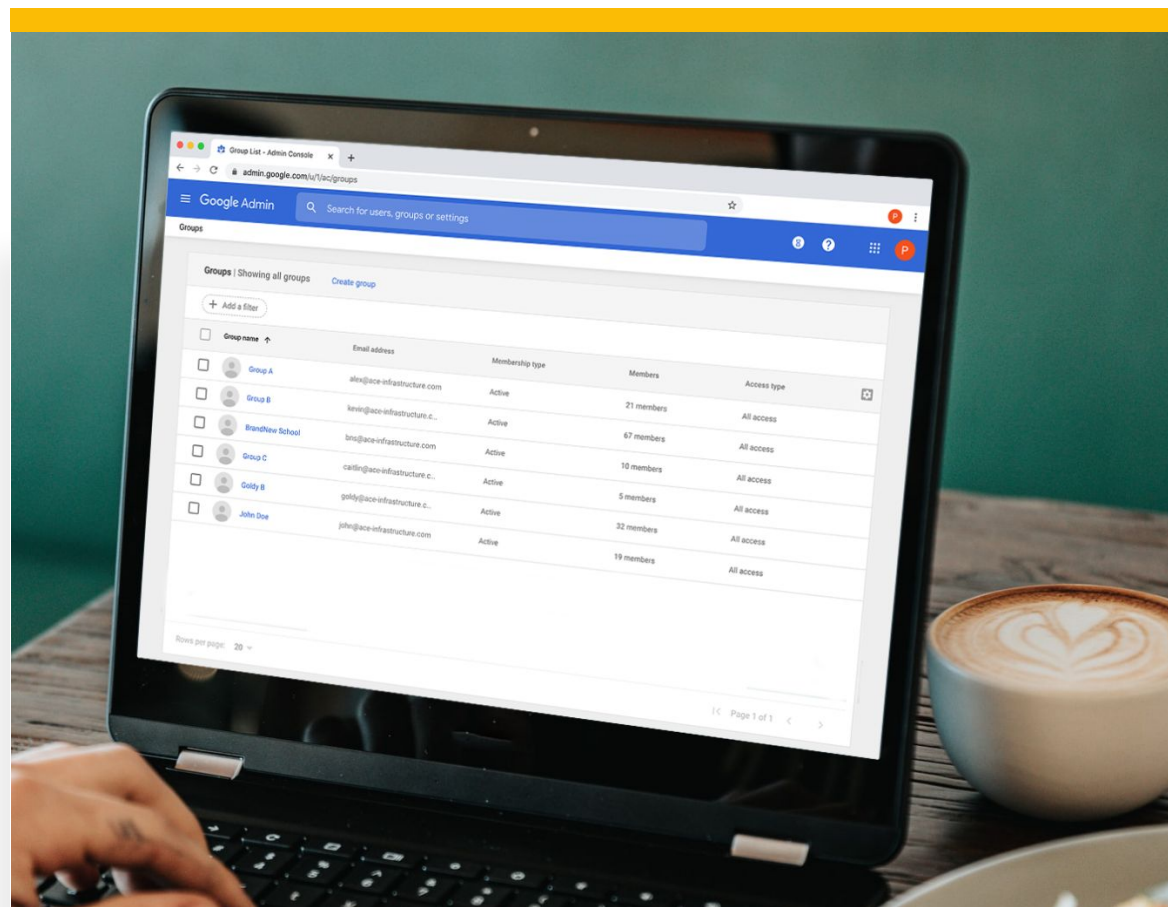



# Getting started with the Splunk integration in Chrome Browser Cloud Management



# Contents

What data gets sent to Splunk from Chrome browser 

---

Install the Google Chrome Add-on for Splunk 


---

Set up Chrome Enterprise Reporting Connector within Splunk 

---

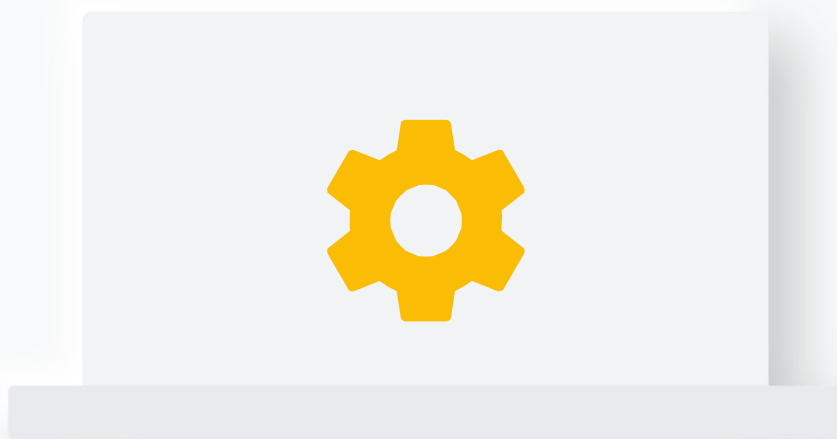
Create the HEC for the Chrome Enterprise Reporting Connector 

---

Set up the Splunk configuration in the Google Admin console 

---

View Chrome events in Splunk 



## 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:

- [Sending security events from Chrome browser to Splunk setup video](#)
- [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](#)

## What data gets sent to Splunk from Chrome browser

The following data is sent from Chrome browser to Splunk 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 each one:

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

## Install the Google Chrome Add-on for Splunk

The first step is to install the [Google Chrome Add-on](#) for your Splunk instance.



More details about the install process is [located via this link](#).



Steps for installing addons for Splunk Cloud, refer to [Install apps in your Splunk Cloud Deployment](#).



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](#).

## Set up Chrome Enterprise connectors within Splunk

In order to set up the connection between the Google Admin console and Splunk you first need to make sure that you enable HTTP Event Collector. Enabling an HEC (HTTP Event Collector) is completed through the Global Settings dialog box in Splunk.



1. Log into your Splunk instance.
2. Click Settings > Data Inputs.
3. Click HTTP Event Collector.
4. Click Global Settings.
5. In the All Tokens toggle button, select Enabled.
  - a. (Optional) Choose a Default Source Type for all HEC tokens. You can also type in the name of the source type in the text field above the drop-down list box before choosing the source type.
  - b. (Optional) Choose a Default Index for all HEC tokens.
  - c. (Optional) Choose a Default Output Group for all HEC tokens.
  - d. (Optional) To use a deployment server to handle configurations for HEC tokens, click the Use Deployment Server check box.
  - e. (Optional) To have HEC listen and communicate over HTTPS rather than HTTP, click the Enable SSL checkbox.
  - f. (Optional) Enter a number in the HTTP Port Number field for HEC to listen on. Confirm that no firewall blocks the port number that you specified in the "HTTP Port Number" field, either on the clients or the Splunk instance that hosts HEC. You can do this by creating a firewall rule to allow requests with User Agent set to 'Google Chrome Enterprise Reporting Connector.
6. Click Save.

## Create the HEC for the Chrome Enterprise Connector



1. Log into your Splunk instance.
2. Click Settings > Add Data.
3. Click Monitor.
4. Click HTTP Event Collector.
5. In the Name field, enter a name for the token, enter Chrome.
  - a. (Optional) In the Source name override field, enter a source name for events that this input generates.
  - b. (Optional) In the Description field, enter a description for the input.
  - c. (Optional) In the Output Group field, select an existing forwarder output group.
  - d. Leave indexer acknowledgment disabled.
6. Click Next.
7. Under source type, click Select and choose google:chrome:json for the source type.
  - a. Note this option will not show up if you do not have the Google Chrome Add-on installed.
8. Leave the App Context and Select Allowed indexes as the default.
  - a. Note this selection will not show up unless you have the Chrome Add-on installed.
9. Click Review.
10. Confirm that all settings for the endpoint are what you want.
11. If all settings are what you want, click Submit. Otherwise, click < to make changes.
12. Copy the token value that Splunk Web displays and paste it into another document for reference later. This will be used when setting up the connector in the Google Admin console.

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



1. Log into the Google Admin console at [admin.google.com](https://admin.google.com).
2. Navigate to Devices>Chrome>Users and browsers. Add a filter for “security events reporting”.
3. Under Security events reporting, select Allow selected events. 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.

## 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](#).

