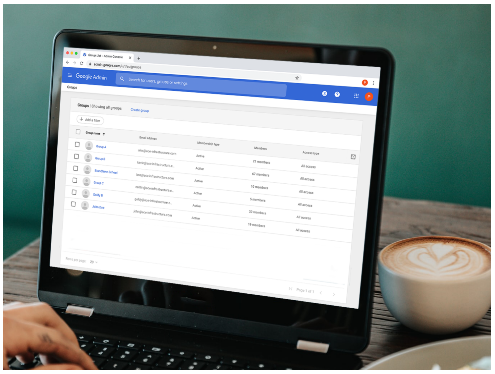
Getting started with Palo Alto Networks Integration in Chrome Browser Cloud Management

Last updated December 2022



This document will guide you through the process of setting up the reporting integration between Chrome Browser Cloud Management and Palo Alto Network's Cortex solution. 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
Help Center Article for Chrome Enterprise Connectors Framework

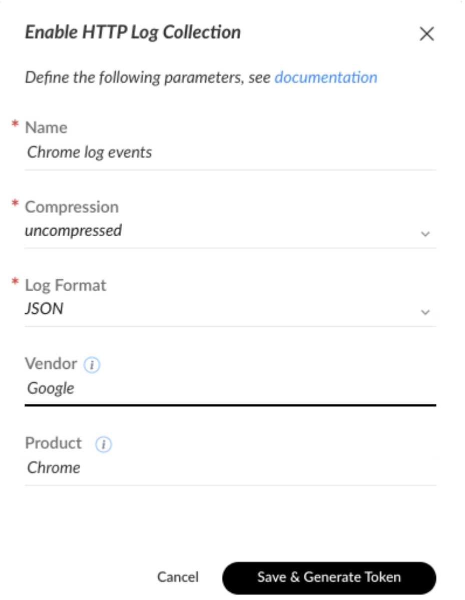
What data gets sent to Palo Alto Networks from Chrome browser

The following data is sent from Chrome browser to Palo Alto Networks 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.

Set up Chrome Enterprise connectors within Palo Alto Networks

Log into your Palo Alto Networks Cortex instance at https://cortex-gateway.paloaltonetworks.com.

1. Under Settings> Configurations>Custom Collectors, click the Add Instance (or click on an instance of a HTTP log collector) button to create a new repository or select an existing one that you want to send Chrome browser security events to.
2. When you create a new repository, you need to give it a name, select Json as Log Format, set the compression as uncompressed and enter the Vendor and Product names.



Enable HTTP Log Collection

Define the following parameters, see documentation

* Name
Chrome log events

* Compression
uncompressed

* Log Format
JSON

Vendor
Google

Product
Chrome

- Note: If you don't enter in a vendor or product Cortex XDR will label the dataset as "unknown_unknown_raw".

3. Click "Save & Generate Token"and retrieve the token that is generated. Save value as you will be entering this into the admin console in the following section.

Set up the Palo Alto Networks 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 Palo Alto Networks.
2. Navigate to Devices>Chrome>Users and browsers. Add a filter for “event reporting”.
3. Under Browser reporting> Event reporting, select Enable event reporting.
    a. Under the additional settings you can also specify which events you want to send to Palo Alto Networks .
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 Palo Alto Networks 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 of your Palo Alto Networks instance and the ingestion token value from step 3 of the last section.
    a. You can find your instance URL under Settings>Configurations>Data Collection>Custom Collectors and select the collector that you just created.
    b. Click the three dots and select Copy API URL
    c. Remove the https:// and anything after the .com like this example and use that as the hostname in the admin console.
        i. ~~https://~~chrome.xdr.us.paloaltonetworks.com~~/logs/v1/event~~
8. Press the Add Configuration to save.
9. Select the Organizational Unit that the reporting events are turned on in and select the Chrome Palo Alto Networks connector that was created in the previous step and hit Save.

View Chrome Events in Palo Alto Networks

Events will start being sent to Palo Alto Networks once the changed policy is applied to the enrolled machines in Chrome Browser Cloud Management. After Cortex begins receiving Chrome Events, Cortex automatically parses the logs and creates a dataset with the name <vendor>_<product>_raw. You can then use XQL Search queries to view logs and create new Correlations rules.

For more information about what events are sent to Palo Alto Networks, 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 Reuse, please review this HC.
- 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.