

Getting started with Palo Alto Networks Cortex integration in Chrome Enterprise Core



Table of Contents

The value of the Chrome browser and Palo Alto Networks Cortex integration	04
Set up Chrome Enterprise Reporting Connector within Palo Alto Networks Cortex	05
Set up the Palo Alto Networks Cortex configuration in the Google Admin console	06
View Chrome events in Palo Alto Networks	07



Resources

This document will guide you through the process of setting up the reporting integration between Chrome Enterprise Core and Palo Alto Networks Cortex solution. Note that this feature requires devices to be enrolled into Chrome Enterprise Core.

Here are some useful links:



[Setting up Chrome Enterprise Core](#)



[Best practices for using Chrome Enterprise Core](#)



[Help Center article for Chrome Enterprise Connectors Framework](#)



The value of the Chrome browser and Palo Alto Networks Cortex integration

The integration between Palo Alto Networks Cortex and Chrome browser provides valuable insights into unsafe behavior and potential attackers targeting your enterprise. Through the Palo Alto Networks Cortex 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.

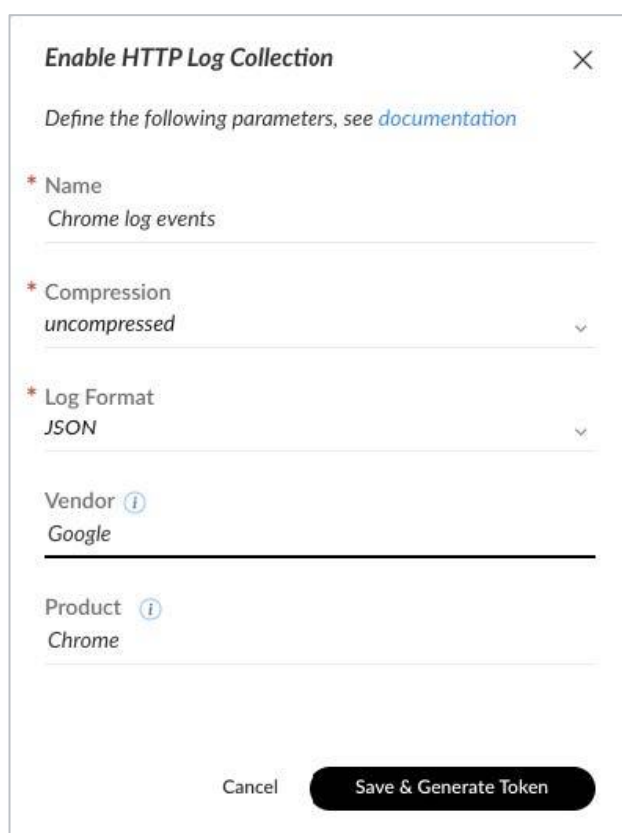
Once the integration is set up, the data is sent from the Chrome browser to Palo Alto Networks Cortex. Additionally, the data is logged in the Google Admin console under Reporting > Audit and Investigation > Chrome log events. For more information and the full list of available security events, please review this [Help Center article](#).



Set up Chrome Enterprise connectors within Palo Alto Networks Cortex

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

- 1 Under **Settings > Configurations > Custom Collectors**, click the **Add Instance** button (or click on an instance of a HTTP log collector) 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

Cancel **Save & Generate Token**

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 copy the token that is generated. You will need to enter this into the admin console in the following section.

Set up the Palo Alto Networks configuration in the Google Admin Console

- 1 Log in to 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 event reporting is turned on, click on the blue hyperlink *Reporting connector provider configurations* to take you to the connector provider configurations, or it can be 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’ to use as the hostname in the admin console e.g. `https://chrome.xdr.us.paloaltonetworks.com/logs/v1/event`
- 8 Press the *Add configuration* to save.
- 9 Select the *Organizational Unit* that has reporting events enabled 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 Cortex

Events will begin sending to Palo Alto Networks Cortex once the changed policy is applied to the enrolled machines in Chrome Enterprise Core. 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 Cortex, 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 Help Center article](#).

Chrome data protection events are available only for customers who have purchased [Chrome Enterprise Premium](#). For more information, visit [this Help Center article](#).

