chrome enterprise

Integrate Chronicle with Chrome Enterprise in Chrome Enterprise Core

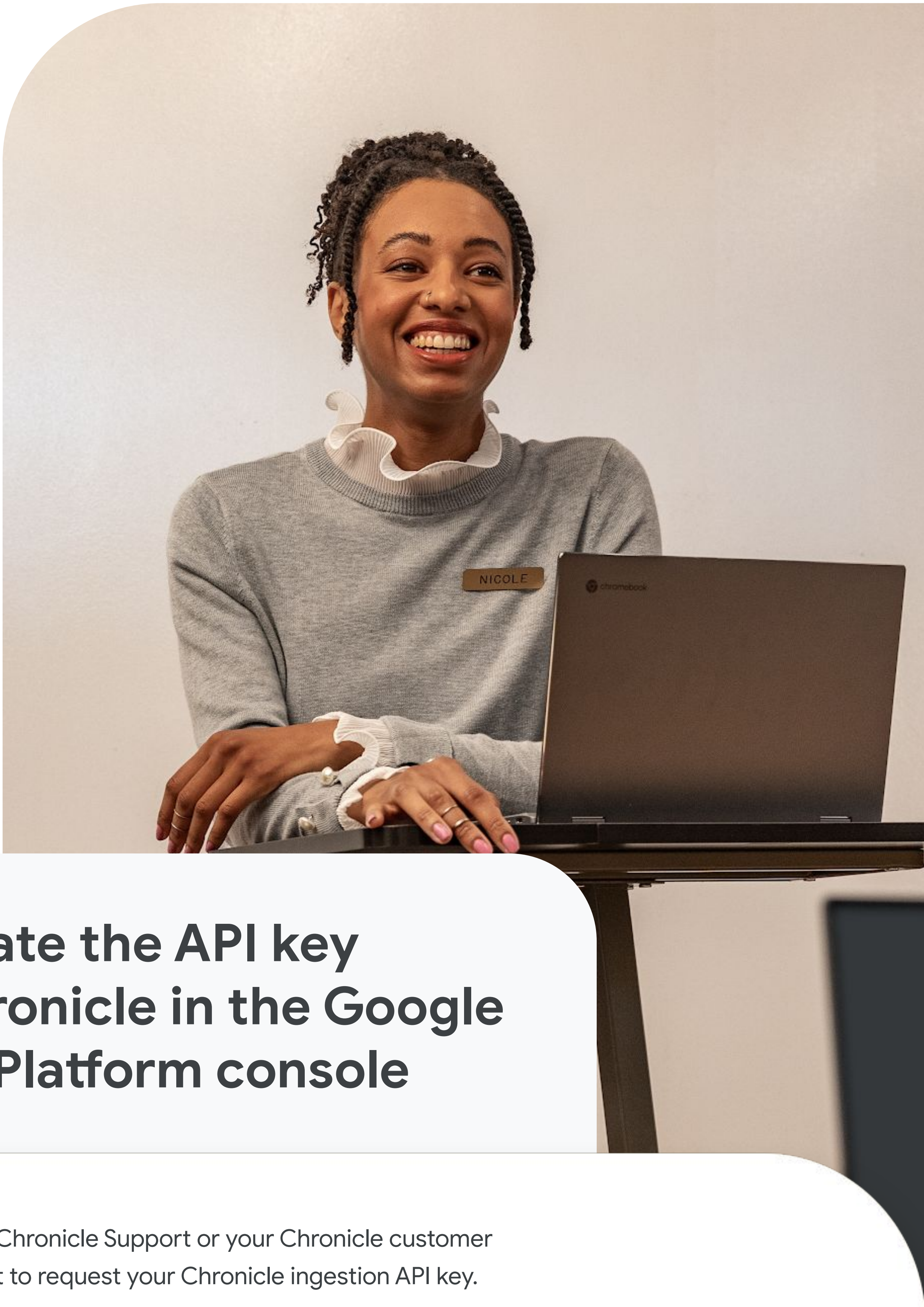
Table of Contents

Resources

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

Here are some useful links:

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



Generate the API key for Chronicle in the Google Cloud Platform console

Please contact Chronicle Support or your Chronicle customer point of contact to request your Chronicle ingestion API key.

Troubleshooting issues in Chrome Enterprise Core

The following data is sent from Chrome browser to Chronicle 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 Chronicle 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 “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 Chronicle.
4. Now that the events are turned on, click on this blue hyperlink 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 Chronicle as the provider.
6. Enter the configuration name that you want this connector to display as in the Google Admin console.
7. Enter the API key value you received from Chronicle.
8. Press the Add Configuration to save.
9. Select the Organizational Unit that the reporting events are turned on in and select the Chrome Chronicle connector that was created in the previous step, and hit Save.

chrome enterprise

View Chrome events in Chronicle

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

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

For more information about what events are sent to Chronicle, 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.