

Google SecOps and Gigamon Application Metadata Intelligence

Deployment Guide

Contents

Prerequisite	2
Google SecOps:	2
Deploying Application Metadata Exporter (AMX) GigaVUE® V Series Node:	2
Configuration of Feed in SecOps	2
How to Configure Application Metadata Intelligence (AMI)	5
Configuring SecOps to Ingest JSON data:	7
Sample Dashboards	8

Prerequisite

Google SecOps:

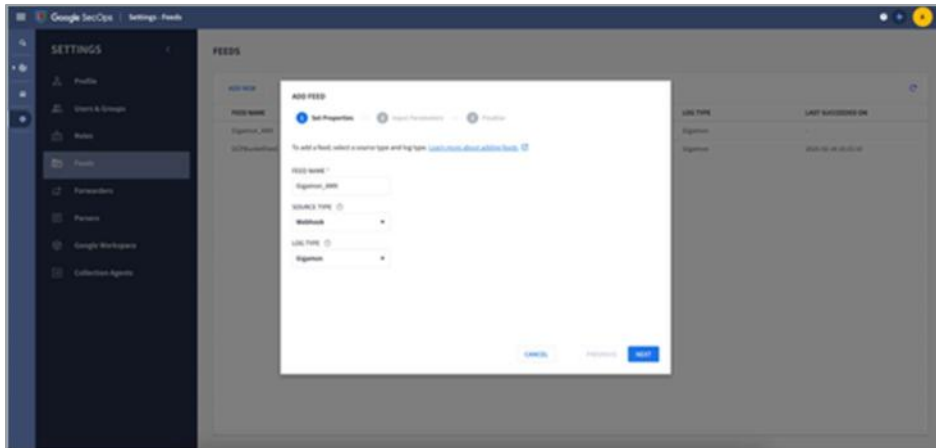
- Google SecOps and Google Cloud Platform (GCP) account must be mapped

Deploying Application Metadata Exporter (AMX) GigaVUE® V Series Node:

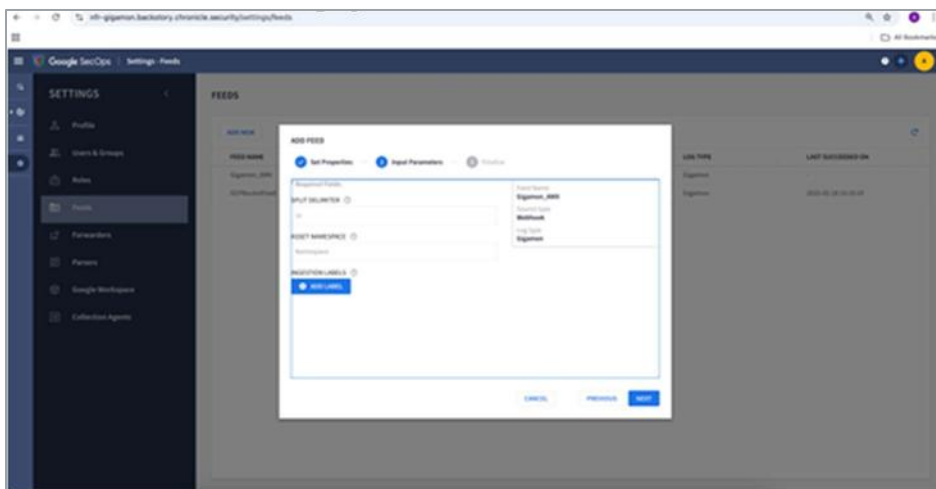
- Deploy a GigaVUE V Series node (for AMX) with traffic acquisition method as Customer Orchestrated Source
- And create a Monitoring Session (Rep1 (In) --->AMX --->Rep 2 (Out))

Configuration of Feed in SecOps

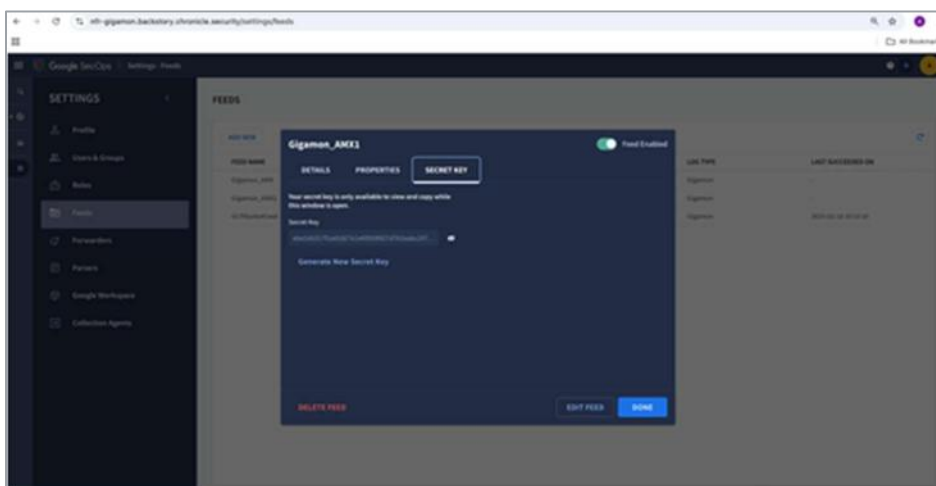
- Login to Google SecOps
- Go to Settings → Feeds
- Click Add New. Enter the Feed Name, Source type as Webhook and Log Type as Gigamon



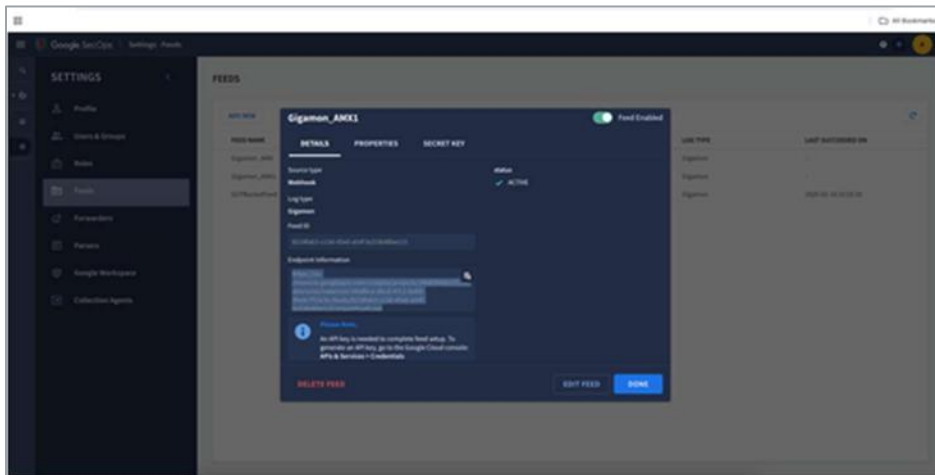
- Click Next. In the next page, leave the default values as such and click Next



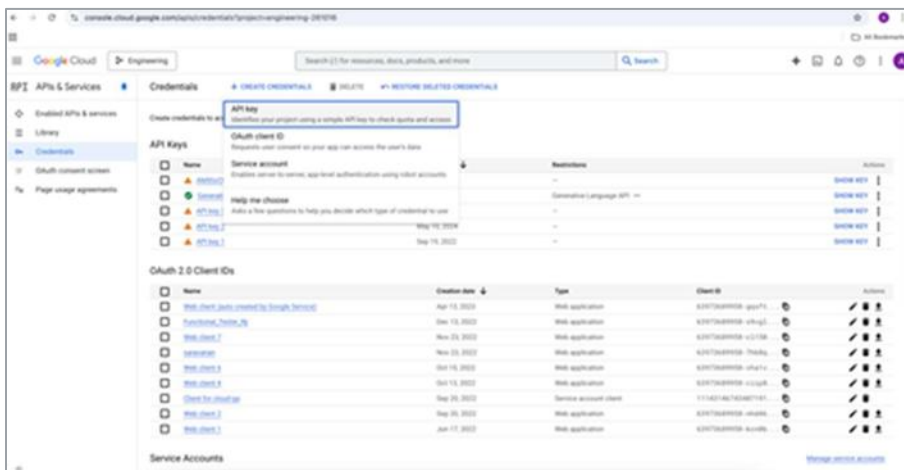
- Click Next. Finalize all the details and click SUBMIT
- Generate a new Secret key and copy the same.



- Go to the Details Tab and copy the Endpoint Information. Click DONE.



- Go to Google SecOps Console and click on APIs & Services → Credentials
- Click on Create Credentials → API Key. API key will be generated and copy the same.



How to Configure Application Metadata Intelligence (AMI)

Please refer to this public doc link: <https://community.gigamon.com/gigamoncp/s/docs> (Doc Library)

NOTE: Please choose the release configuration guide corresponding to the running GigaVUE-FM/V Series)

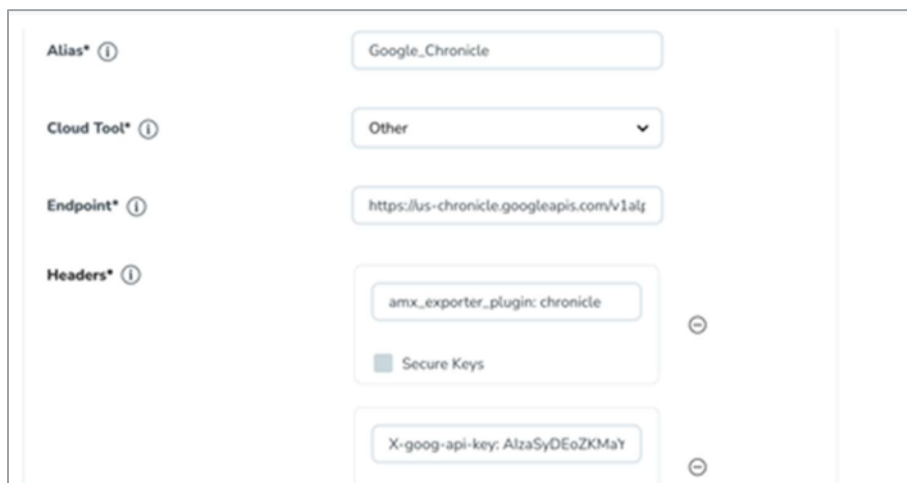
Below is the sample for v6.10 **Application Metadata Intelligence (AMI)**

Configuring Google SecOps Details in AMX:

Please refer to the doc guide for details related to AMX configuration for v6.10:

[6.10 AMX Deployment Guide](#)

- Edit the Monitoring Session, Click on AMX and give details.
- Go to Cloud Tools Exports:
 - Configure Alias as "Google SecOps or name as desired by the user"
 - Cloud Tool as "Other"
 - Configure the Endpoint obtained after configuring feeds in SecOps SIEM Add the below headers,
- amx_exporter_plugin: secops
- X-goog-api-key: XXXX
- X-Webhook-Access-Key: XXXX
 - Type as "AMI"
 - Enable Export
 - Make sure you provide max entries as 10
 - Others with default values.
- Below is a snapshot:



The screenshot displays a configuration form with the following fields and values:

- Alias*** (with an information icon): Google_Chronicle
- Cloud Tool*** (with an information icon): Other (dropdown menu)
- Endpoint*** (with an information icon): https://us-chronicle.googleapis.com/v1alg
- Headers*** (with an information icon):
 - amx_exporter_plugin: chronicle (with a minus icon to the right)
 - ☒ Secure Keys
 - X-goog-api-key: AlzaSyDEoZKMaY (with a minus icon to the right)

X-Webhook-Access-Key: 05e9a17

Secure Keys

Type
ami

MORE OPTIONS

Source IP Address ⓘ
Optional

Enable Export ⓘ
☒

Format ⓘ
JSON

Zip ⓘ
☐

Interval (sec) ⓘ
30

Parallel Writers ⓘ
4

Export Retries ⓘ
4

Max Entries ⓘ
10

Backoff Reset Window ⓘ
0

Max Entries ⓘ
10

Backoff Reset Window ⓘ
0

Request Timeout ⓘ
10

Labels ⓘ
Add

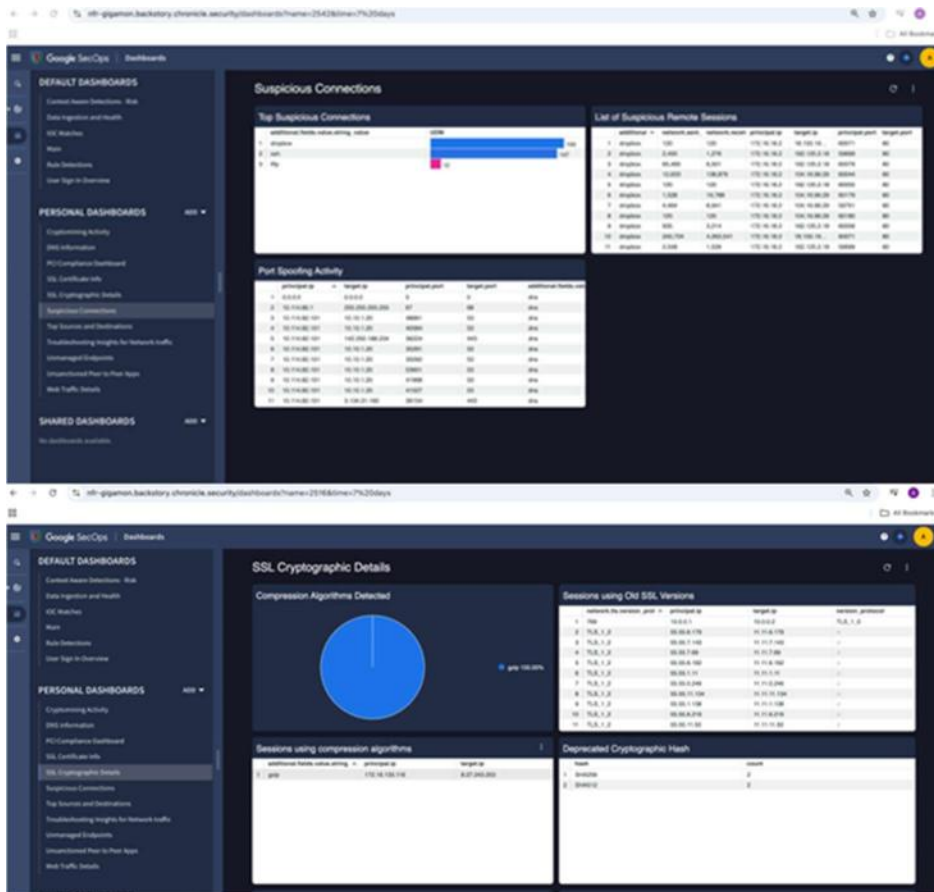
- Now click save and deploy the monitoring session.
- The configuration part is done, now you can test by sending traffic.

Configuring SecOps to Ingest JSON data:

- Login to Google SecOps. Enter the Search term Gigamon and in the raw log search select the start date/end date. Click Search. UDM events generated can be viewed.

The screenshot displays the Google Security Operations (SecOps) interface. At the top, the 'Google Security Operations' logo is visible. Below it, a search bar contains the term 'Gigamon'. A modal window provides instructions on how to use the search bar, including a note about the search scope and a 'Search' button. The main interface shows a 'Raw Log Search' view with a table of results. The table has columns for 'Time', 'Event', and 'Asset'. The first row shows a timestamp of '2020-02-12 11:44:00' and an event type of 'NETWORK_DNS'. The right sidebar contains a 'Procedural Filtering' section with various filters like 'Event Type', 'Event Source', and 'Network Connection Status'.

Sample Dashboards



Gigamon® Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com

© 2025 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.