Gigamon®

Application Metadata Intelligence with Splunk (CEF) Integration Guide

Document Version: 1.0

(See Change Notes for document updates)

Change Notes

When a document is updated, the document version number on the cover page will indicate a new version and provide a link to the Change Notes table, which describes the updates.

Document Version	Date Updated	Change Notes
1.0	03-17-2026	The original release of this document.

Contents

Application Intelligence Solution Integration with Splunk

This guide provides step-by-step instructions for monitoring application metadata from Gigamon using Splunk.

***Note**:*

- *The guide is intended for customer deployments, and it requires familiarity with basic GigaVUE-FM and Splunk administration.*
- *The integration flow outlined in this guide is based on GigaVUE-FM 6.12, Gigamon Deep Observability App 2.3.1, and Splunk10.0.0. Menu labels and UI layouts may change slightly across releases. Always refer to the latest GigaVUE Documentation Library and Splunk documentation for UI details.*

Prerequisites

Before you start with the integration, ensure the following are in place:

- AMI solutions are deployed. For instructions, refer to:
  - Create Application Metadata Intelligence for Physical Environment
  - Create Application Metadata Intelligence for Virtual Environment
  - Apply Threshold Template (SplunkMetadata Template).
- Access to the Splunk UI.

Configure Splunk to ingest CEF data

To configure in Splunk:

1. Log in to Splunk using your Splunk URL and credentials.
2. Go to **Settings** > **Data** > **Data Inputs**.
3. Under **Local inputs,** select **Add new** UDP input.
4. Enter details in the following:
   a. Set the port to 10514. The port value can be changed if needed, but you must use the **same port** on the AMI exporter that sends CEF to Splunk.
   b. Source name override: Enter a source name.
   c. Only accept connection from: Optional (Default)
5. Click **Next**. In **the Input Settings** page:
   a. Select **Custom** > cefevents as Source Type.
   b. **App Context**: Gigamon Metadata Application for Splunk
   c. **Method**: IP
   d. **Index**: Default

***Note**:*

The Source Type-cefevents is specific to your add-on. To ensure it appears in the Source Type selection list, you must include it as part of the add-on package. Refer to the Source Type

creation guidelines for more information. When defining a Source Type, you also specify the category under which it is classified.

6. Under the **Review** page, verify the configurations and click **Submit**.

Configure Splunk details in GigaVUE-FM and Deploy

Before you begin, ensure AMI Monitoring Session is deployed and running.

To set up Splunk details in GigaVUE-FM:

1. Sign in to GigaVUE-FM.
2. Navigate to **Traffic** > **Virtual** > **Orchestrated Flows** and select your platform.
3. Open the monitoring session that contains the AMI node, and then open Traffic Processing.
4. Select the AMI node in the monitoring session to open its configuration panel.
5. To configure the Exporter, select the AMI Node, click on **Menu** > **Details**. Open **Exporters Section**.
6. In the Exporters section do the following configuration:
    a. Click the **Actions** dropdown, select **Add Exporter** and then provide an **Exporter name**.
    b. In the **Template**, click on **Apply Template** and select **SplunkMetadata Template**. (Ensure the threshold template is applied in AMI Exporter).
    c. Click **save** to apply the configuration.

***Note**:*

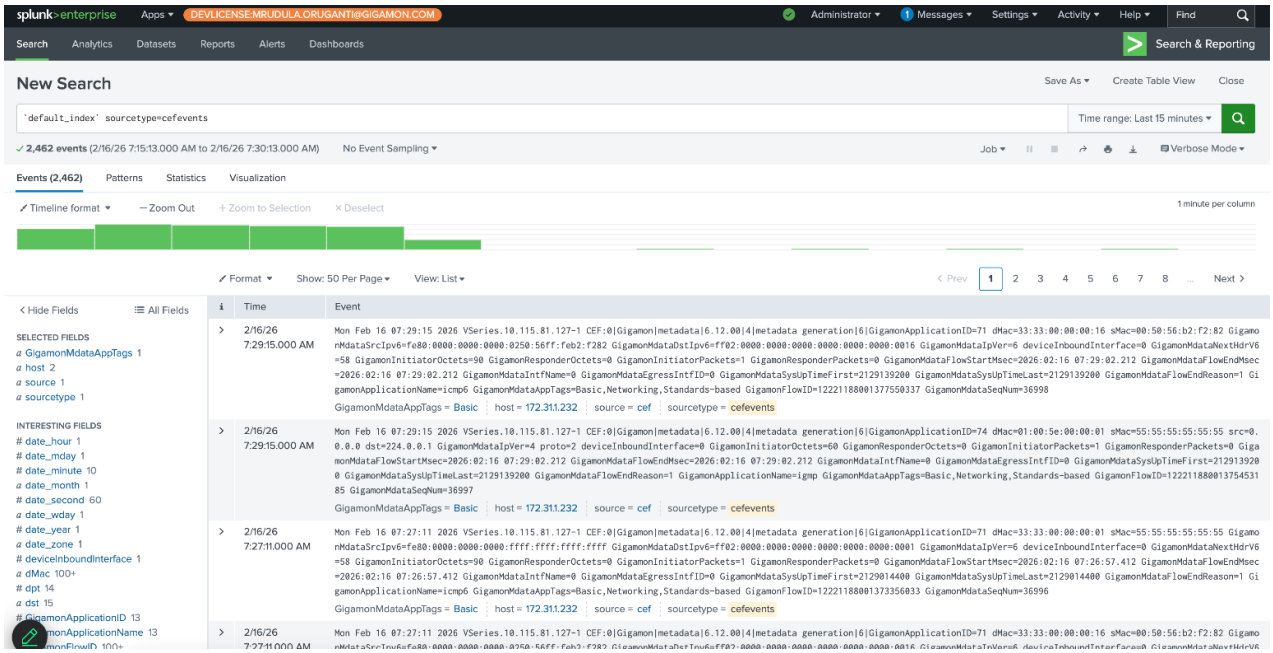
*To add more Application attributes to export metadata in Splunk, users can click on **Modify Applications+** and choose the required attributes from the Application Family.*

7. To configure the Tunnel, add a **New Tunnel** in the canvas:
    a) Enter an **Alias**, for example, SplunkCEF.
    b) In the **Type** drop-down list, select UDP port.
    c) Enter the IP address in the **Destination Address**.
8. Link the AMI exporter to the newly configured tunnel.
9. Click **Actions > Deploy** the Monitoring Session.

Verify the Integration

To verify integration is successful:

1. In the Splunk UI, click on Gigamon Deep Observability App - CEF. Select **Search and Reporting**.
2. In the search bar, run a query in the **Source** field in the format: ` default_index` sourcetype=cefevents and click **Save**.



Visualize the Dashboards Using Gigamon Deep Observability App

You must install predefined dashboards to visualize the application metadata in your Splunk instance. To install the predefined dashboards:

1. Go to **Apps** > **Find more Apps** from your Splunk Environment.
2. Search for "Gigamon".
3. Install the **Gigamon Deep Observability App – CEF** app.
4. Open the installed app and verify whether the dashboards are populated based on the ingested traffic.

Gigamon Inc. 3300 Olcott Street

Santa Clara, CA 95054 408.831.4000