



GigaVUE V Series Applications Guide

Product Version: 6.14

Document Version: 1.0

(See Change Notes for document updates.)

Copyright © 2026 Gigamon Inc. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. No part of this publication may be reproduced, transcribed, translated into any language, stored in a retrieval system, or transmitted in any form or any means without the written permission of Gigamon Inc.

Trademark Attributions

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 Inc.
3300 Olcott Street
Santa Clara, CA 95054
408.831.4000

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
6.14	1.0	07/10/2026	The original release of this document with 6.14.00 GA.

Contents

GigaVUE V Series Applications Guide	1
Change Notes	3
Contents	4
GigaVUE V Series Application Guide	8
Overview of GigaVUE V Series Applications	9
Supported V Series Applications	10
Application Intelligence	14
Points to Note for Application Intelligence	14
Application Visualization	17
Configure Application Visualization for Virtual Environment	17
Configure Filtering and Metadata Export for Selected Applications in Application Visualization	19
View Application Statistics for Application Visualization	20
User Defined Application	21
Create Rules for User Defined Application	27
Application Filtering Intelligence	29
Configure Application Filtering Intelligence for Virtual Environment	29
View Application Statistics for Application Filtering	34
Application Metadata Intelligence	35
Configure Application Metadata Intelligence for Virtual Environment	35
View Application Statistics for Application Metadata	44
Application Metadata Exporter	45
Application Metadata Exporter Deployment Options	46
Application Metadata Exporter - Export Scenarios	49
Prerequisites for Application Metadata Exporter	57
Rules and Notes	61
Configure Application Metadata Exporter	62
Configure Metadata Export Filter for AMX	71
Deploy Application Metadata Exporter in VMware ESXi using Third Party Orchestration	72
Deploy Application Metadata Exporter in VMware ESXi using FM Orchestration	91
Deploy Application Metadata Exporter (AMX) on KVM Hypervisor	113
View Application Metadata Exporter Statistics	114
Attributes for GigaVUE Enriched Metadata for Mobile Networks	118

Attributes for GigaVUE Enriched Metadata for Cloud Workloads	124
Supported Element Types for NetFlow Integrator Element Mapping	130
Troubleshoot AMI/AMX Deployment	133
Scenario 1: AMI not exporting IPFIX/CEF records (exporter side)	134
Scenario 2: AMX not receiving AMI/NetFlow records (ingestor side)	134
Scenario 3: AMX not exporting JSON records (exporter side)	135
GigaSMART NetFlow Generation	136
Create NetFlow Session for Virtual Environment	136
Examples- Configuring Application Intelligence Solution with Other Applications	141
Slicing and Masking with Application Filtering Intelligence	141
De-duplication with Application Metadata Intelligence	142
De-duplication	144
Feature Overview	144
Configure De-duplication Application	144
Distributed De-duplication	146
Limitations	147
What's Next	147
GENEVE Decapsulation	149
What's Next	149
Header Stripping	151
Limitation	152
Configure Header Stripping Application	152
Create Custom Port Template	154
Load Balancing	156
Enhanced Load Balancing	158
What's Next	161
Masking	162
What's Next	164
SSL Decrypt	165
Supported Protocols, Algorithms, and Ciphers for SSL Decrypt	166
Configure SSL Decrypt	168
Upload SSL Key Pairs	168
Create SSL Service	170
Key Mapping	170
SSL Key Pair Store	171
Add SSL Decrypt to Monitoring Session	171
PCAPng Application	174
Create Link Between UDP-in-GRE Tunnel and PCAPng Application	174
Create Link Between PCAPng Application and Other Destinations	175
Ericsson vTAP Domain Tagging Support	175

Configure the PCAPng Application for Domain Tagging	176
What's Next	177
5G-Service Based Interface Application	178
Ericsson vTAP	178
Ericsson vTAP Domain Tagging	179
How SBI Application works	180
Supported Platforms:	181
Rules and Notes	181
5G-Ericsson vTAP Packet Processing (5G-EVP)	182
Solution Architecture	182
Recommended VM Specifications	183
Recommended VM Specifications (DTLS)	183
Supported Deployment Combinations	184
Supported Platforms	184
Licensing	184
Overview of Packet Ordering	184
DTLS Support	185
NTP Time Synchronization	185
Multiple Egress IP Addresses	186
Rules and Notes	186
PCAPNG Processing and Flow Tracking	186
Egress Tunnels and VLAN Tag Insertion	187
End-to End Solution Overview and Configuration:	188
Upgrade and Migration	188
Configure PCC Traffic Flow	188
Monitoring Sessions Required	189
Prerequisites	189
End to End Configuration	189
Recommended VM Specifications	203
FHA Dashboards for 5G Applications	204
Upgrade and Migration Steps	204
Configure SCP Traffic Flow	204
Monitoring Sessions Required	205
Prerequisites	205
End to End Configuration	206
Recommended VM Specifications	215
FHA Dashboards for 5G Applications	216
Upgrade and Migration Steps	216
5G-Cloud Application	216
Supported Platforms	217
5G-Cloud Casa vTAP Support	217
GVHTTP2 Application	218

5G-Cloud Application	218
Configuration of 5G-Cloud Casa vTAP	218
Limitations	224
Rules and Notes	224
5G-Cloud Oracle and Nokia SCP Support	225
Oracle SCP	225
Nokia SCP	225
GVHTTP2 Application	226
5G-Cloud Application	226
Configuration of 5G-Cloud Oracle/Nokia SCP	227
Limitations	236
Rules and Notes	237
FHA Dashboards for 5G-Cloud Applications	238
5G-Cloud Ericsson SCP Support	238
Ericsson SCP	239
How Ericsson SCP Solution works	240
Configuration of 5G-Cloud Ericsson SCP	242
V Series Node 1:	242
V Series Node 2:	243
FHA Dashboards for 5G-Cloud Applications	245
5G Cloud Nokia HEP3 Support	248
Supportability Table	249
5G Cloud Nokia IMS Solution (Non-SBI)	249
5G Cloud Nokia HEP3 CMM Solution (SBI and Non-SBI)	262
Slicing	274
What's Next	275
Appendix - Casa vTap Statistics	276
GVHTTP2 Application	276
5G-Cloud Application	280
Appendix-5G Cloud Nokia HEP3 Support (SBI)	282
GRE-In-UDP Tunnel Decapsulation	283
Additional Sources of Information	285
Documentation	285
How to Download Software and Release Notes from My Gigamon	288
Documentation Feedback	288
Contact Technical Support	289
Contact Sales	290
Premium Support	290
The VUE Community	290
Glossary	291

GigaVUE V Series Application Guide

This guide describes the list of supported V Series Applications and how to add the V Series Applications to monitoring session and configure it.

- [Supported V Series Applications](#)
- [Application Intelligence](#)
- [De-duplication](#)
- [GENEVE Decapsulation](#)
- [Header Stripping](#)
- [Load Balancing](#)
- [Masking](#)
- [SSL Decrypt](#)
- [PCAPng Application](#)
- [5G-Service Based Interface Application](#)
- [5G-Cloud Application](#)
- [Slicing](#)

Overview of GigaVUE V Series Applications

GigaVUE V Series Node is a virtual machine running in the customer's infrastructure which processes and distributes network traffic. It plays the same role as an HC Series appliance in a physical deployment, running many of the same GigaSMART applications and feeding data to tools in a similar manner. Because GigaVUE V Series nodes reside in a virtual environment, inbound and outbound traffic is tunneled (because there are no physical device ports).

GigaVUE V Series Applications run on GigaVUE V Series Nodes. All these applications use Volume- Based License. Refer to [Volume-Based License](#) for more detailed information.

You can use these applications to optimize the traffic sent from your instances to the monitoring tools. GigaVUE Cloud Suite supports the following applications:

- [Application Intelligence](#)
- [De-duplication](#)
- [GENEVE Decapsulation](#)
- [Header Stripping](#)
- [Load Balancing](#)
- [Masking](#)
- [SSL Decrypt](#)
- [PCAPng Application](#)
- [5G-Service Based Interface Application](#)
- [5G-Cloud Application](#)
- [Slicing](#)

Refer to the [Supported V Series Applications](#) table for more information on the platforms in which these applications will be supported.

Supported V Series Applications

The following table summarizes GigaSMART feature support across GigaVUE Cloud Suite platforms, covering packet operations, tunnel handling, application intelligence, and 5G capabilities.

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (VMware vCenter)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Nutanix
Masking	✓	✓	✓	✓	✓	✓
Slicing	✓	✓	✓	✓	✓	✓
De-duplication	✓	✓	✓	✓	✓	✓
Application Metadata Exporter	✓	✓	✓	✓	✓ (Only when deploying GigaVUE V Series Node using Third party Orchestration)	✓
L2GRE Tunnel Encapsulation Refer to <i>Create Ingress and Egress Tunnels</i> section on the retrospective GigaVUE Cloud Suite Deployment Guide.	✓	✗	✓	✓	✓	✓
VXLAN Tunnel Encapsulation Refer to <i>Create Ingress and Egress Tunnels</i> section on the retrospective GigaVUE Cloud Suite Deployment	✓	✓	✓	✓	✓	✓

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (VMware vCenter)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Nutanix
Guide.						
L2GRE Tunnel Decapsulation Refer to <i>Create Ingress and Egress Tunnels</i> section on the retrospective GigaVUE Cloud Suite Deployment Guide.	✓	✗	✓	✓	✓	✓
VXLAN Tunnel Decapsulation Refer to <i>Create Ingress and Egress Tunnels</i> section on the retrospective GigaVUE Cloud Suite Deployment Guide.	✓	✓	✓	✓	✓	✓
ERSPAN Tunnel Decapsulation Refer to <i>Create Ingress and Egress Tunnels</i> section on the retrospective GigaVUE Cloud Suite Deployment Guide.	✓	✗	✓	✓	✓	✓
UDPGRE Tunnel Decapsulation Refer to <i>Create Ingress and Egress Tunnels</i> section on the	✓	✗	✓	✓	✓	✗

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (VMware vCenter)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Nutanix
retrospective GigaVUE Cloud Suite Deployment Guide.						
GENEVE Decapsulation	✓	✗	✗	✗	✓	✗
Header Stripping	✓	✓	✓	✓	✓	✓
Adaptive Packet Filtering (APF) without RegEx	✓	✓	✓	✓	✓	✓
Application Session Filtering (ASF)	✓	✓	✓	✓	✓	✓
Application Filtering Intelligence	✓	✓	✓	✓	✓	✓
Application Metadata Intelligence	✓	✓	✓	✓	✓	✓
GigaSMART NetFlow Generation	✓	✓	✓	✓	✓	✓
Application Visualization	✓	✓	✓	✓	✓	✓
Load Balancing	✓	✓	✓	✓	✓	✓
SSL Decrypt	✓	✓	✓	✓	✗	✓
5G-Service Based Interface Application	✗	✗	✓	✓	✓	✗
5G-Cloud Application	✗	✗	✓	✓	✗	✗

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (VMware vCenter)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Nutanix
Secure Tunnels Encapsulation	x	✓	x	✓	✓	✓
Secure Tunnels Decapsulation	x	✓	x	✓	✓	✓
GRE-In-UDP Tunnel Decapsulation	x	x	✓	✓	x	x

Application Intelligence

Application Intelligence provides a comprehensive solution that:

- identifies the applications contributing to the network traffic.
- isolates preferred application-specific traffic and directs it to the appropriate tools.
- exports relevant application metadata for further analytics and analysis.

Application Intelligence provides the following capabilities for virtual nodes:

- [Application Visualization](#)
- [Application Filtering Intelligence](#)
- [Application Metadata Intelligence](#)
- [Application Metadata Exporter](#)

Points to Note for Application Intelligence

Point to note when configuring Application Intelligence:

1. For a monitoring domain, the following application can be configured only once, and all these applications must be configured in a single monitoring session.
 - a. Application Visualization
 - b. Application Filtering
 - c. Application Metadata
2. For GigaVUE V Series Node version lesser than 6.3.00, Application Visualization, Application Filtering, Application Metadata, and Application Metadata Exporter (AMX) applications are not supported in the Monitoring Session.

3. When undeploying and redeploying the Monitoring session which has the Application Intelligence application, ensure to follow the steps given below:
 - a. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears. Select the Monitoring Session for which you enabled Secure Tunnels. Click **Actions > Undeploy**. The monitoring session is undeployed.
 - b. Select the Monitoring Session for which you enabled Secure Tunnels. Click **Actions > Edit**. The **Edit Monitoring Session** Canvas page appears.
 - c. Add the Application Intelligence applications.
 - d. Modify the Number of Flows as per the below table:

Cloud Platform	Instance Size	Maximum Number of Flows
VMware	Large (8 vCPU and 16GB RAM)	200k
AWS	AMD - Large (c5n.2xlarge)	300k
	AMD - Medium (t3a.xlarge)	100k
	ARM - Large (c7gn.2xlarge)	100k
	ARM - Medium (m7g.xlarge)	200k
Azure	Large (Standard_D8s_V4)	500k
	Medium (Standard_D4s_v4)	100k
Nutanix	Large (8 vCPU and 16GB RAM)	200k

- Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k..
 - If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.
- e. Click **Deploy**.
 4. After adding the above-listed applications and deploying the Monitoring Session, you cannot edit the Number of flows and Fast Mode. For more detailed information on Number of flows and Fast Mode, refer to [Number of Flows](#) and [Fast Mode](#).
 5. Once the Number of flows is added in any of the above-listed applications, the same value is applied to all the above-listed applications configured in that Monitoring Session. You cannot change it.
 6. Once Fast Mode is enabled in any of the above-listed applications, then it is enabled for all the above-listed applications configured in that Monitoring Session. You cannot change it.

7. You can also configure Application Intelligence with Precryption, prefiltering, and secure tunnels. Refer to Precryption, Prefiltering, and Secure Tunnels topics in the respective cloud deployment guides for more detailed information on how to configure these features.
8. Small Form Factor for VMware ESXi is not supported when using applications like Application Visualization, Application Metadata, Application Filtering. Refer to *Configure GigaVUE V Series Nodes for VMware ESXi* section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) for more detailed information on how to deploy GigaVUE V Series Node, where you select the Form Factor.

Application Visualization

Application Visualization identifies and monitors all applications contributing to the network traffic and reports on the total applications and the total bandwidth they consume over a select period. Application Visualization allows you to identify more than 3,200 applications. It displays the traffic statistics in bytes and packets.

Refer to the following topics for more detailed information on how to configure the application and view the statistics:

- [Configure Application Visualization for Virtual Environment](#)
- [Configure Filtering and Metadata Export for Selected Applications in Application Visualization](#)
- [View Application Statistics for Application Visualization](#)

Configure Application Visualization for Virtual Environment

Application Visualization can be configured in the **Edit Monitoring Session** Canvas Page. To add an Application Visualization application to the canvas, follow the steps given below:

1. Drag and drop **Application Visualization** from **APPLICATIONS** to the graphical workspace.
2. Click the Application Visualization application and select **Details**. The Application quick

view appears.

3. In the Application quick view, enter or select the following details:

Parameter	Description																							
Name	Enter a name for the application.																							
Description	Enter the description.																							
Export Interval	The time interval in seconds at which the export must be done. The export interval is set to 300 seconds. It cannot be modified.																							
Advanced Settings																								
Number of Flows	The number of flows supported by the application. Refer to the following table for the maximum number of flows supported for VMware, AWS, Nutanix, and Azure platforms. <table border="1"> <thead> <tr> <th>Cloud Platform</th><th>Instance Size</th><th>Maximum Number of Flows</th></tr> </thead> <tbody> <tr> <td>VMware</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr> <tr> <td rowspan="4">AWS</td><td>AMD - Large (c5n.2xlarge)</td><td>300k</td></tr> <tr> <td>AMD - Medium (t3a.xlarge)</td><td>100k</td></tr> <tr> <td>ARM - Large (c7gn.2xlarge)</td><td>100k</td></tr> <tr> <td>ARM - Medium (m7g.xlarge)</td><td>200k</td></tr> <tr> <td rowspan="2">Azure</td><td>Large (Standard_D8s_v4)</td><td>500k</td></tr> <tr> <td>Medium (Standard_D4s_v4)</td><td>100k</td></tr> <tr> <td>Nutanix</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr> </tbody> </table> ▪ Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k.. ▪ If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.	Cloud Platform	Instance Size	Maximum Number of Flows	VMware	Large (8 vCPU and 16GB RAM)	200k	AWS	AMD - Large (c5n.2xlarge)	300k	AMD - Medium (t3a.xlarge)	100k	ARM - Large (c7gn.2xlarge)	100k	ARM - Medium (m7g.xlarge)	200k	Azure	Large (Standard_D8s_v4)	500k	Medium (Standard_D4s_v4)	100k	Nutanix	Large (8 vCPU and 16GB RAM)	200k
Cloud Platform	Instance Size	Maximum Number of Flows																						
VMware	Large (8 vCPU and 16GB RAM)	200k																						
AWS	AMD - Large (c5n.2xlarge)	300k																						
	AMD - Medium (t3a.xlarge)	100k																						
	ARM - Large (c7gn.2xlarge)	100k																						
	ARM - Medium (m7g.xlarge)	200k																						
Azure	Large (Standard_D8s_v4)	500k																						
	Medium (Standard_D4s_v4)	100k																						
Nutanix	Large (8 vCPU and 16GB RAM)	200k																						
Monitoring	You can use this option, enable or disable the Application Visualization application functionality.																							
Fast Mode	Enable the Fast Mode option for performance (less CPU cycles and less memory utilization) improvement. When the Fast Mode is enabled, some or all of the attributes of the applications will be disabled. If all the attributes of the application are disabled then the application itself is disabled. Refer to Fast Mode section for more information on the benefits and limitations of the Fast Mode. Note: This option is disabled for NetVUE Base Bundle License.																							

4. Click **Save**.

Configure Filtering and Metadata Export for Selected Applications in Application Visualization

This section describes how to perform filtering and exporting metadata for selected applications when configuring Application Visualization. Refer to the following steps for more detailed information:

- [Filter Traffic for Selected Applications](#)
- [Export Metadata for Selected Applications](#)

Filter Traffic for Selected Applications

1. Click the Application Visualization application in the Monitoring Session Canvas page and select **Details**. The Application quick view appears.
2. Click on **STATISTICS** tab.
3. Click on the drop-down menu that displays **Top 10** and select the **All**.
4. Select the applications for which you want to filter traffic.

NOTE: Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each application.

5. Click **Actions > Filter Selected Applications**. The **Filter Selected Applications** dialog box opens.
6. In the **Filter Selected Applications** dialog box, Select the existing Application Filtering map or New Map from the **Send to Map** drop-down menu.
 - **New Map:** Select this option if you wish to create a new application filtering map, to filter the traffic from the applications.
 - **Existing map:** Select this option if you have already configured an application filtering map and you wish to send the traffic for filtering to that map.
7. Under the **Applications** section, choose the traffic as pass or drop for the selected applications.
8. Click **Send to Map**.

NOTE: If the **New Map** option is selected from the **Send to Map** drop-down menu. Then, the map quick view appears. Refer to step 3, 4, 5, 6, and 7 in [Configure Application Filtering Intelligence for Virtual Environment](#) section for more detailed instructions on how to configure Application Filtering.

Export Metadata for Selected Applications

1. Click the Application Visualization application and select **Details**. The Application quick view appears.
2. Click on **STATISTICS** tab.

3. Click on the drop-down menu that displays **Top 10** and select the **All**.
4. Select the applications for which you want to export metadata.

NOTE: Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each application.

5. Click **Actions > Export Metadata for Selected Applications**. The **Export Metadata for Selected Applications** dialog box opens.
6. In the **Export Metadata for Selected Applications** dialog box, Select the existing Application Metadata application or New Exporter from the **Send to Exporter** drop-down menu.
 - **New Application Metadata:** Select this option if you wish to create a new application metadata, to export metadata from the applications.
 - **Existing Application Metadata Application:** Select this option if you have already configured an Application Metadata Intelligence application and you wish to send the traffic for exporting metadata from the applications.
7. Click **Export**.

NOTE: If the **New Application Metadata** option is selected from the **Send to Exporters** drop-down menu. Then, the application quick view appears. Refer to steps 3 and 4 in [Configure Application Metadata Intelligence for Virtual Environment](#) section for more detailed instructions on how to configure Application Metadata application.

View Application Statistics for Application Visualization

To view the application Statistics for the Application Visualization application, follow the steps given below:

1. Click **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select a monitoring session from the list view, click **Actions > Edit**. The Edit Monitoring Session page appears.
3. Click the application and select **Details**. The Application quick view appears.
4. Click on **STATISTICS** tab.

5. You can view the following in the statistics page:
 - a. **Total Traffic:** Displays the total traffic of the network. Use the drop-down menus to change the parameters. You can use the **Select Tags** filter option to filter the traffic related to the selected application tags.
 - b. **Total Applications :** You can view all the applications and their bandwidth in the network. You can also perform filtering and exporting metadata for selected applications. Refer to [Configure Filtering and Metadata Export for Selected Applications in Application Visualization](#) for more detailed information on how to perform filtering and exporting metadata for selected applications.
 - c. **Top 10 Applications:** Click on the drop-down menu that displays **All** and select the **Top 10** . Displays the Top 10 applications running in the network based on the metrics.
 - d. **Top 10 Application Families:** You can view a graphical representation of top 10 applications running in the network based on the metrics. When you hover over the Pie-chart, GigaVUE-FM shows the application families in the network.

You can view the statistics for past hour, past 24 hours, or past 7 days. GigaVUE-FM also allows you to view statistics for a particular period by selecting the date and time. The selected data and time must be within the past 7 days.

GigaVUE-FM takes more than five minutes to display the application statistics since the export interval is fixed at five minutes. For the first fifteen minutes after creating the solution, if GigaVUE-FM receives traffic, it will show real-time data. If there is no traffic during this time, it will take at least eleven minutes to display the statistics once traffic is received.

User Defined Application

This feature allows you to identify unclassified TCP, UDP, HTTP, and HTTPS applications and extract their application name and ID.

Refer to the following topic for more detailed information:

- [Supported Protocols and Attributes](#)
- [Mindata](#)
- [Supported RegExp Syntax](#)
- [Limitations](#)
- [Create Rules for User Defined Application](#)

Supported Protocols and Attributes

The DPI engine will match the rules defined based on the following protocols and attributes within the first 500 bytes of a packet payload.

For supported Regex patterns, refer [Supported RegExp Syntax](#)

Protocol	Attributes	Attribute Labels	Description	Direction	Supported Data Type	Example Value
http	cts-uri	Request URI	Partially Normalized URL (path + request)	Client to Server Only	REGEXP	\fupload\(create_file new_slice upload_slice)\?.*upload_token=.*
	cts-server	Server Name	Web Server Name from URI or Host	Client to Server Only	REGEXP	(.*\.)?gigamon\.com
	mime_type	MIME Type	Content type of Request or the Web page	Both, Client to Server or Server to Client	REGEXP	http
	cts-user_agent	User Agent	Software / Browser used for request	Client to Server Only	REGEXP	mozilla
	cts-referer	Referer URI	Source address where client got the URI	Client to Server Only	REGEXP	http://gigamon.com/
	stc-server_agent	Server Agent	Software used for the server	Server to Client Only	REGEXP	NWS_TCloud_PX
	stc-location	Redirect Location	Destination address where the client	Server to Client Only	REGEXP	.*\football\.*

			is redirected to			
	cts-cookie	Cookie (Raw)	Raw value of the HTTP Cookie header line	Client to Server Only	REGEXP	.*tEstCoOkie.*
	content	Content	Message body content	Both, Client to Server or Server to Client	REGEXP	.*GIGAMON.* mindata = 206 Refer Mindata
http2	cts-uri	Request URI	Partially Normalized URL (path + request)	Client to Server Only	REGEXP	\/fupload\/(create_file new_slice upload_slice)\?.*upload_token=.*
	cts-server	Server Name	Web Server Name from URI or Host	Client to Server Only	REGEXP	(.*\.)?gigamon\.com
	cts-user_agent	User Agent	Software / Browser used for request	Client to Server Only	REGEXP	mozilla
	cts-referer	Referer URI	Source address where client got the URI	Client to Server Only	REGEXP	http:\/gigamon.com\/
ssl	common_name	Domain Name	Domain name from Client		REGEXP	(.*\.)?gigamon\.com

			Hello message or the certificate			
	stc-subject_alt_name	Subject Alt Name(s)	List of host names which belong to the same certificate	Server to Client Only	REGEXP	(.*\.)?gigamon\.com
rtmp	cts-page_url	Page URL	URL of the webpage where the audio/video content is streamed	Client to Server Only	REGEXP	http://www.music.tv/recorded/1234567
tcp	stream	Payload Data	Data payload for a packet, excluding the header.		REGEXP	.*GIGAMON.* mindata = 70 Refer Mindata
	port	Server Port	Server (listen) port number		UINT16 RANGE as REGEXP String	80-4350
udp	stream	Payload Data	Data payload for a		REGEXP	.*GIGAMON.* mindata = 100

			packet, excluding the header			Refer Mindata
	port	Server Port	Server (listen) port number		UINT16 RANGE as REGEXP String	80-4350
sip	user_agent	User Agent	Software used	Both, Client to Server or Server to Client	REGEXP	GVUE-release 6.2.0
icmp	code	Message Code	Code of the ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	200
	typeval	Message Type	Type of ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	10
ip	address	Server IP Addresses	IP address of the server		IPV4 as REGEXP String	62.132.12.30\24
	dscp	DSCP Value	DSCP from Different		UINT8 as REGEXP	33

			ia ted Service (DS) Field in IP header		String	
	resolv_ name	DNS Name	Server's DNS name		REGEXP	gigamon.com
ipv6	address	Server IP Addres s	IP address of the server		IPV6 as REGEXP String	2001:0:9d38:6ab8:307b:16a 4:9c66:5f4 2001:0:9d38::9c66:5f4/64
	dscp	DSCP Value	DSCP from Different ia ted Service (DS) Field in IP header		UINT8 as REGEXP String	43

Mindata

The mindata value is the number of payload bytes to buffer and match a given pattern. You can configure mindata value for HTTP content, TCP stream, and UDP stream. The buffer size is calculated from the start of the payload and the default buffer size is different for each protocol (HTTP - 206, TCP - 67, and UDP - 48.)

For example, for pattern ".*TEST.*" that may be present within the first 67 bytes of TCP payload, you can specify the mindata value as 4 (which is the length of the input string) or as 67 (which is the default buffer size of TCP payload). In case, the pattern is present in between 65 to 68 bytes of the payload and the mindata is specified as 4 or 67, it will not match. For this case, you must specify the mindata value as 68.

Supported RegExp Syntax

Pattern	Description
.	Matches any symbol
*	Searches for 0 or more occurrences of the symbol or character set that precedes it

+	Searches for 1 or more occurrences of the symbol or character set that precedes it
?	Searches for 0 or 1 occurrence of the symbol or character set that precedes it
()	Groups a series of expressions together
[]	Matches any value included within the bracket at its current position Example: [Dd]ay matches Day and day
 [<start>-<end>]	Separates values contained in (). Searches for any one of the values that it separates. Example: The following expression matches dog or cat: (dog cat). Matches any value contained within the defined range (a hyphen indicates the range). You can mix character class and a hexadecimal range Example: [AaBbCcDdEeFf0-9]
\0 <octal_ number>	Matches for a direct binary with octal input
\x<hexadecimal- number>\x	Matches for a direct binary with hexadecimal input
\[<character- set>\]	Matches a character set while ignoring case. WARNING: Not performance friendly

Limitations

- The maximum number of user defined application that can be configured is 120 per GigaVUE-FM. These applications can be spread across one or more application intelligence sessions.
- The maximum number of rules that can be created per application is 8.
- The maximum number of protocols that can be configured per rule is 3.

Create Rules for User Defined Application

To create a new application:

You can create rules for User Defined Application in two ways:

1. Go to **Inventory > Resources > User-defined Applications**. Refer to User Defined Applications section in GigaVUEGigaVUE Fabric Management Guide for details.
2. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**. Follow the steps listed below:

- a. Select a Monitoring Session from the list view. Navigate to **TRAFFIC PROCESSING** tab. The GigaVUE-FM canvas page appears.
- b. In the canvas, click on the  icon on the left side of the page to view the traffic processing elements.
- c. Select **User Defined Applications** under **Options** menu.
- d. Enable the **User-defined Applications** toggle button.
- e. Click **New Application**. The New Application page appears.
- f. Enter the **User-Defined Application Name**.
- g. Enter **Priority**. The value must be between 1 and 120.

NOTE: The lowest value has the highest priority.

- h. In the Rules dialog box, select the following details:
 - Choose the **Protocol** from the list of protocols.
 - Choose the **Attributes** from the list of attributes.
 - Choose the **Values** from the list of values.

Using the **Actions** Button, you can perform the following actions:

- i. Click **Save**.

To add the created applications to the Monitoring Session:

1. In the **User Defined Applications** tab, click Add Application button.
2. Select the applications that must be added.
3. Click **Done**.

After creating rules for User defined Applications, you can add it to Application Filtering when configuring the applications. Refer to [Add Application](#) section for more detailed information on how to add User defined Application when configuring Application Filtering.

Application Filtering Intelligence

Application Filtering Intelligence allows filtering of traffic based on the application (such as YouTube, Netflix, Sophos, or Facebook) or application family (such as antivirus, web, erp, or instant-messaging) or application tags. Enables traffic filtering by layer 7 applications, which means you can filter out high-volume, low-risk traffic from reaching the tools and distribute high-risk network traffic of interest to the right tool at the right time.

Refer to the following topics for more detailed information and step-by-step instructions on how to configure Application Filtering Intelligence application and view the statistics:

- [Configure Application Filtering Intelligence for Virtual Environment](#)
- [View Application Statistics for Application Filtering](#)

Configure Application Filtering Intelligence for Virtual Environment

Application Filtering Intelligence (AFI) can be configured in the Monitoring Session Canvas. To add Application Filtering application to the canvas, follow the steps given below:

1. Drag and drop **New Map** from **New** to the graphical workspace.
2. Click the application and select **Details**. The Application quick view appears.
3. Enable **Application Filtering** in the **GENERAL** tab.

4. In the Application quick view, enter or select the following details in the **GENERAL** tab:

Parameter	Description
Name	Enter a name for the application.
Description	Enter the description.
Application Filtering Settings	
Bidirectional	Enable or Disable Bi-Directional Flow behavior. Bi-Directional is enabled by default. Disable this option for Uni-Directional Flow behavior.
Timeout	Specify the traffic flow inactivity timeout, in seconds. The session will be removed due to inactivity when no packets match.
Buffer	This option is enabled by default.
Buffer Count Before	Number of packets that should be buffered until the flow is identified. If the flow is not identified even after reaching the maximum number of packets buffered, then all the subsequent packets of this session will be dropped.
Protocol	Select the Protocol. The packet matching the selected protocol will be filtered. The default value is TCP-UDP.
Session Slicing	Enable or Disable session slicing to enter the Packet Count . Packet Count is disabled by default. The Packet Count limits the number of packets passed per flow to a configurable value in the range 2–100. Useful when tools only need the first few packets, such as TLS handshakes.
Session Fields	
Session Field	The Packet fields to be considered for creating the Session / traffic flow (Session key fields)
Action	Add or Remove 'VlanId' Packet field for creating the session / traffic flow.

Parameter	Description																							
Advanced Settings																								
Number of Flows	The number of flows supported by the application. Refer to the following table for the maximum number of flows supported for VMware, AWS, and Azure platforms.																							
	<table><tr><th>Cloud Platform</th><th>Instance Size</th><th>Maximum Number of Flows</th></tr><tr><td>VMware</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr><tr><td rowspan="4">AWS</td><td>AMD - Large (c5n.2xlarge)</td><td>300k</td></tr><tr><td>AMD - Medium (t3a.xlarge)</td><td>100k</td></tr><tr><td>ARM - Large (c7gn.2xlarge)</td><td>100k</td></tr><tr><td>ARM - Medium (m7g.xlarge)</td><td>200k</td></tr><tr><td rowspan="2">Azure</td><td>Large (Standard_D8s_V4)</td><td>500k</td></tr><tr><td>Medium (Standard_D4s_v4)</td><td>100k</td></tr><tr><td>Nutanix</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr></table>	Cloud Platform	Instance Size	Maximum Number of Flows	VMware	Large (8 vCPU and 16GB RAM)	200k	AWS	AMD - Large (c5n.2xlarge)	300k	AMD - Medium (t3a.xlarge)	100k	ARM - Large (c7gn.2xlarge)	100k	ARM - Medium (m7g.xlarge)	200k	Azure	Large (Standard_D8s_V4)	500k	Medium (Standard_D4s_v4)	100k	Nutanix	Large (8 vCPU and 16GB RAM)	200k
	Cloud Platform	Instance Size	Maximum Number of Flows																					
	VMware	Large (8 vCPU and 16GB RAM)	200k																					
	AWS	AMD - Large (c5n.2xlarge)	300k																					
		AMD - Medium (t3a.xlarge)	100k																					
		ARM - Large (c7gn.2xlarge)	100k																					
		ARM - Medium (m7g.xlarge)	200k																					
	Azure	Large (Standard_D8s_V4)	500k																					
		Medium (Standard_D4s_v4)	100k																					
Nutanix	Large (8 vCPU and 16GB RAM)	200k																						
- Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k.. - If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.																								
Fast Mode	Enable the Fast Mode option for performance (less CPU cycles and less memory utilization) improvement. When the Fast Mode is enabled, some or all of the attributes of the applications will be disabled. You can view the list of attributes/applications available in the fast mode by navigating to the app editor under AMI feature in the GigaVUE-FM. If all the attributes of the application are disabled then the application itself is disabled. Refer to Fast Mode section for more information on the benefits and Limitations of the Fast Mode.																							

- Click the **RULESETS** tab. Through the map, packets can be dropped or passed based on the highest to lowest rule priority. You can add 5 rule sets on a map. Each rule set can have only 25 rules per map and each rule can have a maximum of 4 conditions.

Enter the following details for each of the Rule Set created:

Parameter	Description
Priority	A priority determines the order in which the rules are executed. The priority value can range from 1 to 5, with 1 being the highest and 5 is the lowest priority.
AE ID	Application Endpoint ID will be used as source or destination object for creating or connecting links
Actions	Using this option, you can perform the following functions: • New Ruleset- Use to add a new Rule Set. Note: A maximum of 5 Rule Sets can be created. • New Rule- Use to add a New Rule Note: A maximum of 25 Rules can be created per rule set. • Delete this Ruleset- Use to delete the Ruleset
RULES	
Rule	Use the toggle button to Pass or Drop the traffic through the map.

Parameter	Description
Condition	Select any one of the conditions from the drop-down menu and search or select the attributes. Use the + and - buttons to add or remove a condition with a Rule. Click  and select Add Condition to add more conditions. Note: A maximum of 4 conditions can be created per Rule.
APPLICATION FILTERING Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each application.	
Add Application	Click on the Add Application button. The Add Application dialog box opens. Select a Type. The available options are: • Application Family: Each application is mapped only mapped to one Application Family ▪ Select an Application Family and the Applications that needs to be filtered from the traffic. ▪ In the Traffic Action column, select Pass or Drop to pass or drop the traffic. You can also use Pass All or Drop All to allow or drop the traffic for all the applications. • Application Tag: Each application can be mapped to one or more Application Tags. ▪ Select an Application Tag and the Applications that needs to be filtered from the traffic. ▪ In the Traffic Action column, select Pass or Drop to pass or drop the traffic. You can also use Pass All or Drop All to allow or drop the traffic for all the applications. User Defined Applications: To configure User Defined Applications for AFI, follow the steps given below. - Enable User Defined Applications toggle button in the Options page. Refer to User Defined Application topic for more detailed information on what is user defined applications and how to configure it. - In this Add Application dialog box, select User Defined Applications from the Application Family list.

- To pass or drop any remaining traffic in the network, enter the priority and AE ID in the default rule set available. Select **Pass** or **Drop** option for **Any Remaining Traffic** field.
- Click the **THRESHOLDS** tab. For more details on how to create and apply threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

8. To reuse the configuration, click **Add to Library**. Save the application filtering configurations using one of the following ways:
 - a. Select an existing group from the **Select Group** list or create a **New Group** with a name.
 - b. Enter a description in the **Description** field, and click **Save**.
 - c. The saved map can be found in the **Map Library** in the **Edit Monitoring Session** Canvas Page.
9. Click **Save**.

To edit a map, select the map and click **Details**, or click **Delete** to delete the map.

When using the Application Filtering application, you can either use a single tunnel, to tunnel all the filtered traffic from the application or use a separate tunnel for each rule configured.

View Application Statistics for Application Filtering

To view the application Statistics for the Application filtering application, follow the steps given below:

1. Click **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select a monitoring session from the list view, click **Actions > Edit**. The Edit Monitoring Session page appears.
3. Click the application and select **Details**. The Application quick view appears.
4. Click on **STATISTICS** tab.
5. You can view the following in the Application Filtering application statistics page:
 - a. Rules - Displays the rules created in this application.
 - b. Pass App (Bytes) - Displays the packet that pass through the applications selected.
 - c. Drop App (Bytes) - Displays the packets that are dropped by the applications selected.
 - d. Pass Rule (Bytes) - Displays the packet that pass through the rule sets configured.
 - e. Drop Rule (Bytes) - Displays the packets that are dropped by the rule sets configured.

Application Metadata Intelligence

Application Metadata Intelligence allows you to export metadata from applications that are detected in the network traffic. The records can be exported to a collector either in IPFIX or CEF format through the IP interface or the management interface. You can also use the application metadata attributes for purposes other than security, such as to determine the network or application health, to track the long-lived sessions seen in the network, and so on.

Application Metadata Intelligence generates more than 6000 attributes for more than 4000 applications without impacting the users, devices, applications, or the network appliances. The feature identifies applications even when the traffic is encrypted.

Application Metadata Intelligence (AMI) is enabled to multi-collect protocols with more than one metadata attribute of the same type. The multi-collect feature supports additional protocols such as DNS, GTP, GTPV2, DHCP, HTTP, HTTPS, SSL, HTTP_PROXY, HTTP2, KERBEROS5, and DHCP6.

The generated metadata is exported in IPFIX (IP Flow Information Export) format and CEF (Common Event Format) to security analytics and forensics tools thereby providing greater visibility to enforce corporate compliance.

The output from the Application Metadata Intelligence in CEF format can also be converted to JSON format using Application Metadata Exporter (AMX) application. To learn more about AMX application refer to Application Intelligence—Application Metadata Exporter

Refer to following topics for more detailed information and step-by-step instructions on how to configure Application Metadata Intelligence and view the statistics:

- [Configure Application Metadata Intelligence for Virtual Environment](#)
- [View Application Statistics for Application Metadata](#)

You can convert the output from the Application Metadata Intelligence (AMI) which is in CEF format into JSON format and send it to the cloud tools and Kafka. Refer to [Application Metadata Exporter](#) for detailed information on AMX and how to configure it.

Configure Application Metadata Intelligence for Virtual Environment

Application Metadata Intelligence (AMI) can be configured in the Monitoring Session Canvas. To add Application Metadata Intelligence application to the canvas, follow the steps given below:

**Notes:**

- Ensure to create separate Monitoring Domains and Monitoring Sessions for Application Metadata Exporter (AMX) and Application Metadata Intelligence (AMI). Even when AMI is deployed virtually, it operates independently and requires its own Monitoring Session.
- Flow Direction/Behaviour under Application Metadata Settings must be configured as **Bidirectional** for exporting application Metadata. Each exporter can be configured to export application metadata for up to 256 applications, and up to 64 attributes can be exported for each application. GigaVUE-FM allows selecting metadata for applications that support exporting metadata. Applications which do not support exporting metadata are not listed in the GigaVUE-FM. By default, application name is exported for all such applications.

1. In GigaVUE-FM, go to **Traffic > Virtual > Orchestrated Flows**. Select the required cloud platform.
2. After creating a new Monitoring Session or on an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab. The GigaVUE-FM Monitoring Session canvas page appears.
3. Drag and drop **Application Metadata** from **APPLICATIONS** to the graphical workspace.
4. Click the Application Metadata application and select **Details**. The Application quick

view appears.

5. In the Application quick view, enter or select the following details in the **General** tab:

Parameter	Description
Name	Enter a name for the application.
Description	Enter the description.
Application Metadata Settings	
Flow Direction	Enable or Disable Bi-Directional Flow behavior. Bi-Directional is enabled by default. Disable this option for Uni-Directional Flow behavior.
Timeout	Specify the traffic flow inactivity timeout, in seconds. The session will be removed due to inactivity when no packets match.
Multi Collect	Enable: Enables the multi-collect of attributes within a given Metadata Store cache which means that if a configured attributes is seen in multiple packets within the same flow, each of these information is collected. Multi Collect is enabled by default, when a new cache is created. Multi Collect is enabled, when upgraded from an older release. Disable: Disables the multi-collect of attributes within a given Metadata Store cache. This option is disabled by default. Note: Do not enable this option if you are going to export the Application Metadata using the AMX application. There can be only one attribute in a JSON object, therefore Multi-collect is not supported when configuring the AMX application.
Data Link	If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the Data Link and enable the VLAN option.
Observation ID	Enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is 00 01 02 05 , and in Decimal is 66053 .
Enable DPI Packet limit	This field is used to restrict the number of packets in a particular session to be sent to the DPI engine instead of sending all the packets in order to improve the AMI performance. The value must range between 20 - 50 as the first 20 to 50 packets contains the most significant attributes.
Recurring Attributes	When enabled, exports TLS Server Name for the lifetime of new TLS flows. When disabled, the value is exported only once at the beginning of a flow.
Advanced Settings	
Number of Flows	The number of flows supported by the application. Refer to the following table for the maximum number of flows supported for VMware, AWS, and Azure platforms.

Parameter	Description		
	Cloud Platform	Instance Size	Maximum Number of Flows
	VMware	Large (8 vCPU and 16GB RAM)	200k
	AWS	AMD - Large (c5n.2xlarge)	300k
		AMD - Medium (t3a.xlarge)	100k
		ARM - Large (c7gn.2xlarge)	100k
		ARM - Medium (m7g.xlarge)	200k
	Azure	Large (Standard_D8s_v4)	500k
		Medium (Standard_D4s_v4)	100k
	Nutanix	Large (8 vCPU and 16GB RAM)	200k
	- Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k.. - If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.		
Fast Mode	Enable the Fast Mode option for performance (less CPU cycles and less memory utilization) improvement. When the Fast Mode is enabled, some or all of the attributes of the applications will be disabled. If all the attributes of the application are disabled then the application itself is disabled. Refer to Fast Mode section for more information on the benefits and Limitations of the Fast Mode.		
Aggregate Mode	Enable this option to export the minimum, maximum, and mean of RTT values for the following list of supported protocols and attributes and also the aggregate of TCP Lost byte values collected per export time interval.		
	Protocol	Attribute	
	http	rtt	
	icmp	rtt	
	icmp6	rtt	
	ssh	rtt	
	tcp	rtt	
	tcp	rtt_app	

Parameter	Description	
	telnet	rtt
	wsp	connect_rtt
	wsp	query_rtt

6. In the Application quick view, enter or select the following details in the **Exporters** tab:

Parameter	Description
Exporter Name	Enter a name for the Exporter.
Actions	Using this option, you can perform the following functions: • Add Exporter - Use to add a new Exporter to this Application Metadata Intelligence Application. A maximum of 5 exporters can be added. • Save as New Template - Use to save the current configuration as a new custom tool template. • Delete this Exporter - Use to delete the Exporter.
Template	Use to select the tool template. Refer to <i>Tool Templates</i> section in GigaVUE Fabric Management Guide for more information on tool templates and how to create custom tool templates.
Export Params	Select any one of the following options: • Application Name - Exports Application Name Attribute in AMI records. Enable this option to export Application Name attribute with network attributes • Application Family - Exports Application Family Attribute in AMI records. Enable this option to export Application Family attribute with network attributes • Application Tags - Exports Application Tag Attribute in AMI records. Enable this option to export Application Tag attribute with network attributes
Format	Select NetFlow or CEF
NetFlow: Select this option to use NetFlow	
Record / Template type	• Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. • Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool. Note: It is recommended to select Cohesive from the drop-down menu, as NetFlow exports network and transport parameters only.
Enable Maximum Packet Length	Enable this option to edit the interface MTU value.
Maximum Packet Length (This option appears only when Enable Maximum Packet Length option is enabled)	Using this field, you can configure the maximum length of the packet that can be exported. Enter this value less than or equal to egress interface MTU value to avoid fragmentation. The value can range between 1280 and 9001.
Active Timeout	Enter the active flow timeout value in seconds.
Inactive Timeout	Enter the inactive flow timeout in seconds.
Version	Select the NetFlow version. The supported versions are V5, V9, IPFIX(V10).
Template Refresh Interval	Enter the time interval at which the template must be refreshed in seconds

Parameter	Description
CEF: Select this option to use CEF	
Record / Template type	- Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. - Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active flow timeout value in seconds.
Inactive Timeout	Enter the inactive flow timeout in seconds.
APPLICATION & ATTRIBUTES: Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each of the application. (Not applicable when using NetFlow V5, V9, NetFlow IPFIX(V10), or CEF when the flow direction is Uni-Directional in the above Template drop-down menu.)	
NOTE: When you edit application attributes during an AMI deployment with background traffic, you may experience minor data loss until the update completes.	
Add Application	Click on the Add Application button. The Add Application dialog box opens. Select a Type. The available options are: Application Family: Each application is mapped only mapped to one Application Family - Select an Application Family and the Applications that needs to be filtered from the traffic. - Attributes for the selected application is displayed in the Attribute column. You can select the required attributes. Application Tag: Each application can be mapped to one or more Application Tags. - Select an Application Tag and the Applications that needs to be filtered from the traffic. - Attributes for the selected application is displayed in the Attribute column. You can select the required attributes. NOTE: The AMI exporter exports application metadata for the selected applications but exports the packet attributes for all applications. To export packet attributes only for the selected applications, filter the required traffic by using a flow map or AFI.
NETWORK & TRANSPORT PARAMETERS: Select the Network and the transport packet attributes with the respective parameters	
Data Link	Select any one of the parameters such as Source MAC address, Destination MAC Address and VLAN.
Interface	Select any one of the parameter such as Input Physical, Output Physical and Input Name.
IP	Select the parameter as Version if required.

Parameter	Description
IPv4	Select the required attributes. By default, Source Address, Destination Address, and Protocol are enabled.
IPv6	Select the required attributes. By default, Source Address, Destination Address, and Next Header are enabled.
Transport	Select the required attributes. By default, Source Port, Destination Port are enabled.
Counter	Select the Bytes, and Packets.
Timestamp	Select the required timestamp such as System Uptime First, Flow Start, System Uptime Last, and Flow End.
Flow	Select the parameter as End Reason if required.
GTP-U	Select the required parameters such as QFI and TEID.
Outer IPv4	Select any one of the parameter such as Source or Destination.
Outer IPv6	Select any one of the parameter such as Source or Destination.

NOTE: In the exporter record, the generator ID represents the hostname of the GigaVUE V Series Node. Any changes to the hostname after deploying the Monitoring Domain with the AMI application will not be reflected in the exporter record.

- Click **Save**.

After configuring the Application Metadata application, follow the below steps to create an egress tunnel:

- In the canvas page, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.
- Enter the **Alias**, **Description** and select **UDP** as **Type**.

NOTE: When using Application Metadata, if you create a tunnel to send the output to the tools, select UDP as the tunnel type.
You can either use a single tunnel to export all metadata from the application or configure separate tunnels for each exporter.

- Enter the **MTU** value.
- L4 Destination IP Address** - Enter the IP address of the tool port. If using Application Metadata Exporter (AMX), enter the data subnet IP address of the V Series Node where AMX application is deployed. Refer to [Application Metadata Exporter](#) for details.
- Source L4 Port** - The port from which the connection will be established to the target. For example, if A is the source and B is the destination, this port value belongs to A.

6. **Destination L4 Port** - The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B. The destination port must match the AMX ingestor port number to ensure seamless data forwarding from AMI to AMX.

NOTE: If the export format is CEF, the default value for L4 destination port is 514. If the export format is NetFlow, the default value for L4 destination port is 2055.

To deploy the configured Application Metadata Intelligence application, follow the below steps:

1. On the Monitoring Session canvas page, click **Deploy** from the **Actions** menu to deploy the Monitoring Session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on the V Series Node.
2. You can view the Monitoring Session Deployment Report in the **SOURCES** and **V SERIES NODES** tab. When you click on the Status link, the Deployment Report is displayed. If the Monitoring Session is not deployed properly, then one of the following errors is displayed in the Status column.
 - Success—The session is not deployed on one or more instances due to V Series Node failure.
 - Failure—The session is not deployed on any of the V Series Nodes or Instances.

After adding the Application Metadata application and deploying Monitoring Session, you cannot change the **Aggregate Round Trip time** option.

NOTE: To configure Application Metadata Intelligence in physical environment, refer to [Create an Application Intelligence Session in Physical Environment](#).

View Application Statistics for Application Metadata

To view the application Statistics for the Application Metadata application, follow the steps given below:

1. Click **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select a monitoring session from the list view, click **Actions > Edit**. The Edit Monitoring Session page appears.
3. Click the application and select **Details**. The Application quick view appears.
4. Click on **STATISTICS** tab.
5. You can view the following in the Application Metadata application statistics page:
 - Exporter Name - Displays the exporters created for this application.
 - Format - Displays the format as NetFlow or CEF, for the individual exporters.
 - Packet Sent/ Sec - Displays the count of packets sent per second for each exporter.

You can download the Exporter statistics using the following option:

Download Records (Exporter) - Select this option to download the PCAP file (for example, Pcap__e1_link3_2026-03-12_174220.pcapng) of the exporter records. You can download records for a single AMI exporter or for multiple exporters.

For more information on troubleshooting AMI exporter issues, refer to [Troubleshoot AMI/AMX Deployment](#).

For more information on health status of exporters, refer to [View Health Status](#).

Application Metadata Exporter

Application Metadata Exporter (AMX) is an Application Intelligence component that runs on GigaVUE V Series Nodes and works with Application Metadata Intelligence (AMI) and other telemetry sources to deliver standardized metadata to your monitoring and analytics tools.

GigaVUE-FM manages both AMX and AMI and provides a central point to deploy, configure, and monitor AMX across on-premises and cloud environments.

You can use AMX to:

- Transform and export application metadata in JSON and Parquet formats to cloud-native tools/data lakes.
- Transform and export NetFlow/IPFIX, and mobility metadata in JSON format to cloud-native tools and Kafka-based data pipeline.
- Enrich mobile-network metadata for 3G/4G/5G visibility and analytics.
- Enrich AMI records with cloud and Kubernetes workload metadata with host, environment, and container context to reduce Mean Time To Identification (MTTI) and Mean Time To Resolution (MTTR).
- Enrich AMI records with user identity information using Zscaler Private Access (ZPA), adding customer, user, and service details to help pinpoint performance issues and monitor the effectiveness and compliance of network access policies.

Refer to the following topics for more detailed information on the various deployment options and scenarios:

- [Application Metadata Exporter Deployment Options](#)
- [Application Metadata Exporter - Export Scenarios](#)

Application Metadata Exporter Deployment Options

The output from the Application Metadata Intelligence or GTP Correlation Engine is sent to the AMX application, which exports it to the tools in JSON format over HTTPS/Kafka. AMX application is always deployed in GigaVUE V Series Node. The GigaSMART application sending data to the AMX application can be on GigaVUE HC Series or the GigaVUE V Series Node. Based on where the GigaSMART applications reside, there can be four deployment methods:

NOTE: For exporting GigaVUE Enriched Metadata for Cloud Workloads, AMI should be deployed in GigaVUE V Series Nodes.

- **On-Premises**
 - Hardware (AMI)
 - Hardware (Control Plane Metadata)
 - Virtual (VMware, Nutanix, KVM)

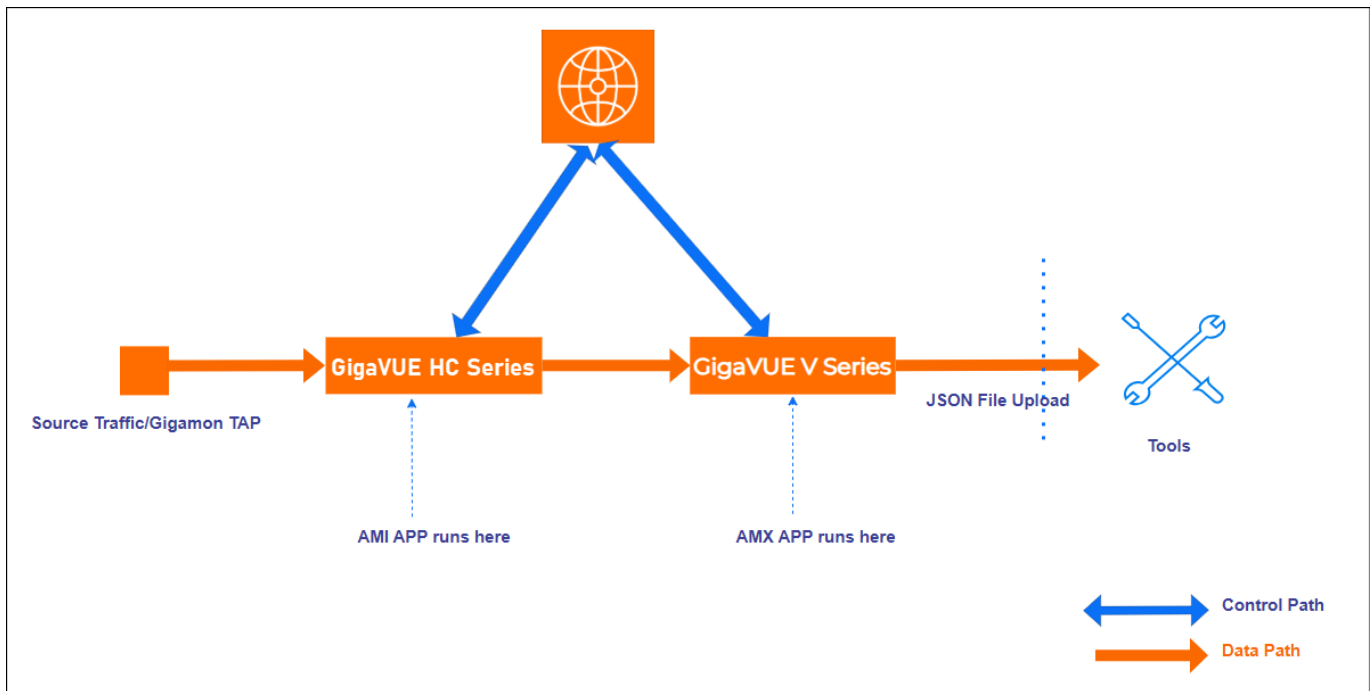
- **Public Cloud**

On-Premises

Hardware (AMI)

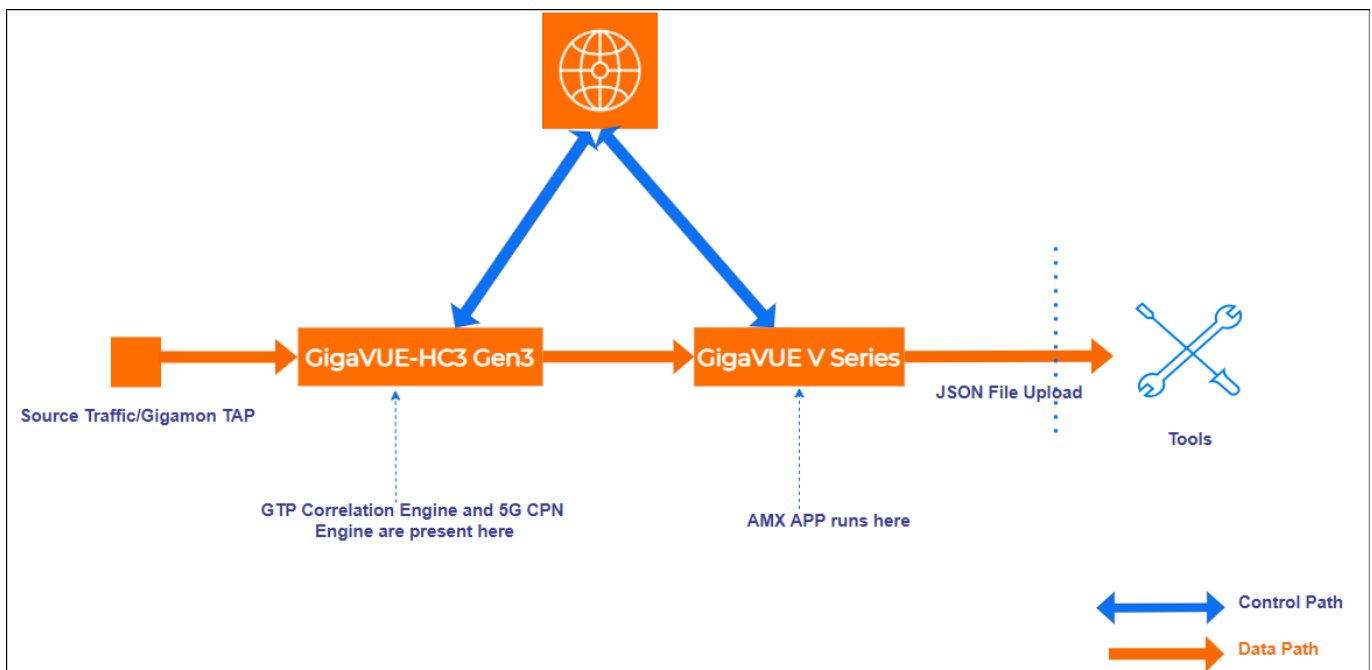
In hardware deployments, the Application Metadata Intelligence (AMI) runs on a physical node/cluster, and the AMX application is deployed on a GigaVUE V Series Node running on VMware ESXi, OpenStack, or Nutanix. The output from the AMI in CEF format is sent to the AMX application in GigaVUE V Series Node. GigaVUE-FM handles the orchestration of the configuration between the Gigamon devices. The following devices support the integration of AMX application:

- GigaVUE-HC1
- GigaVUE-HC3
- GigaVUE-HC1-Plus
- GigaVUE-HCT



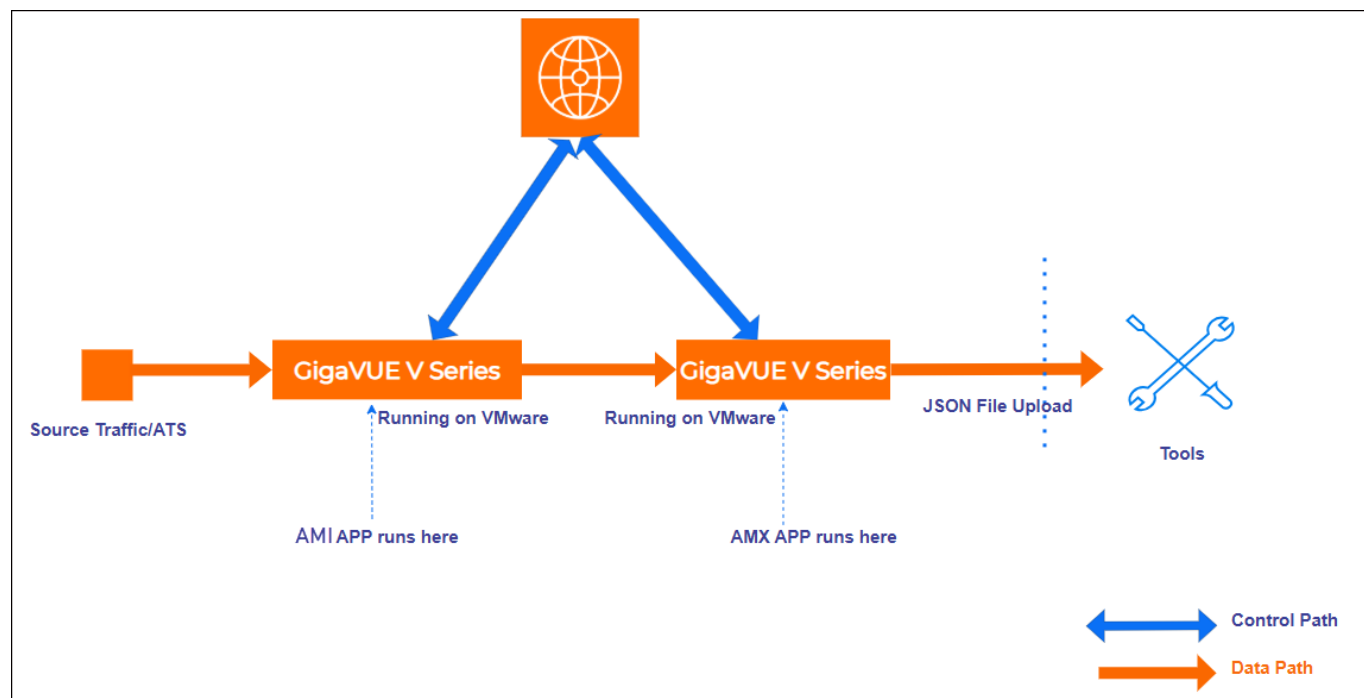
Hardware (Control Plane Metadata)

In hardware deployments, the GTP Correlation Engine runs on a physical node/cluster, and the AMX application is deployed on a GigaVUE V Series Node running on VMware ESXi/KVM and Nutanix. The output from the GTP Correlation Engine in Flat JSON format is sent to the AMX application in GigaVUE V Series Node. The performance of the device and the application is managed by GigaVUE-FM. The GigaVUE-HC3 Gen3 devices support the integration of AMX application.



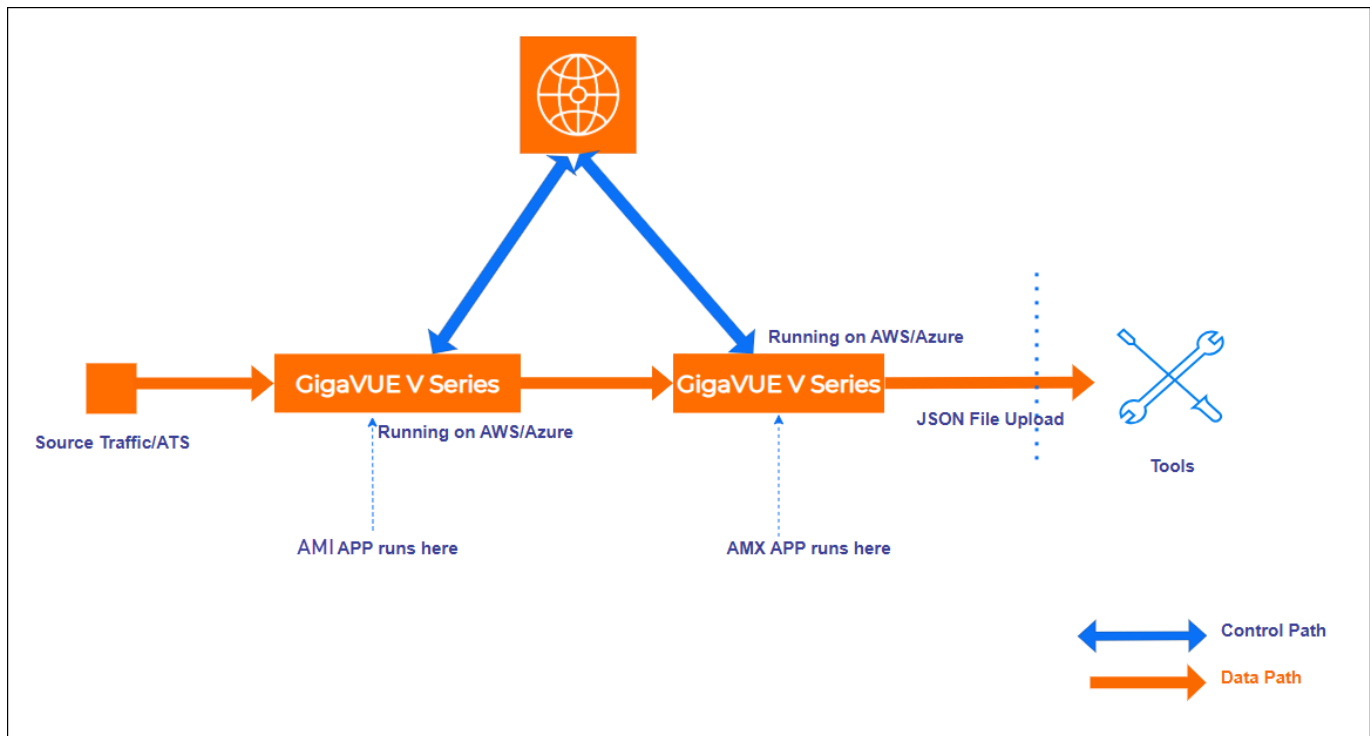
Private Cloud (VMware)

In the Private Cloud environment, the application is supported only on VMware ESXi/KVM and Nutanix and can be deployed in the VMware as shown in the diagram.



Public Cloud

In the Public Cloud environment, the application is supported on AWS and Azure platforms, and can be deployed as shown in the diagram:



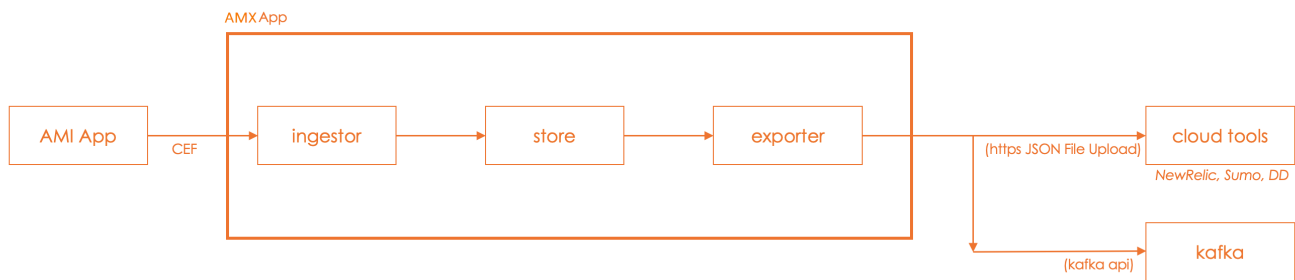
Application Metadata Exporter - Export Scenarios

Refer to the following topics for more detailed information on the various ways to configure AMX:

- Export Application Metadata in JSON format over HTTPS/Kafka
- Transform NetFlow/IPFIX records to JSON format and export over HTTPS/Kafka
- Export of 3G/4G/5G Control Plane Metadata by AMX
- Export GigaVUE Enriched Metadata for Mobile Networks and Export over HTTPS/Kafka
- Export GigaVUE Enriched Metadata for Cloud Workloads and Export over HTTPS/Kafka
- Identity Enrichment using Zscaler Private Access (ZPA)

Export Application Metadata in JSON format over HTTPS/Kafka

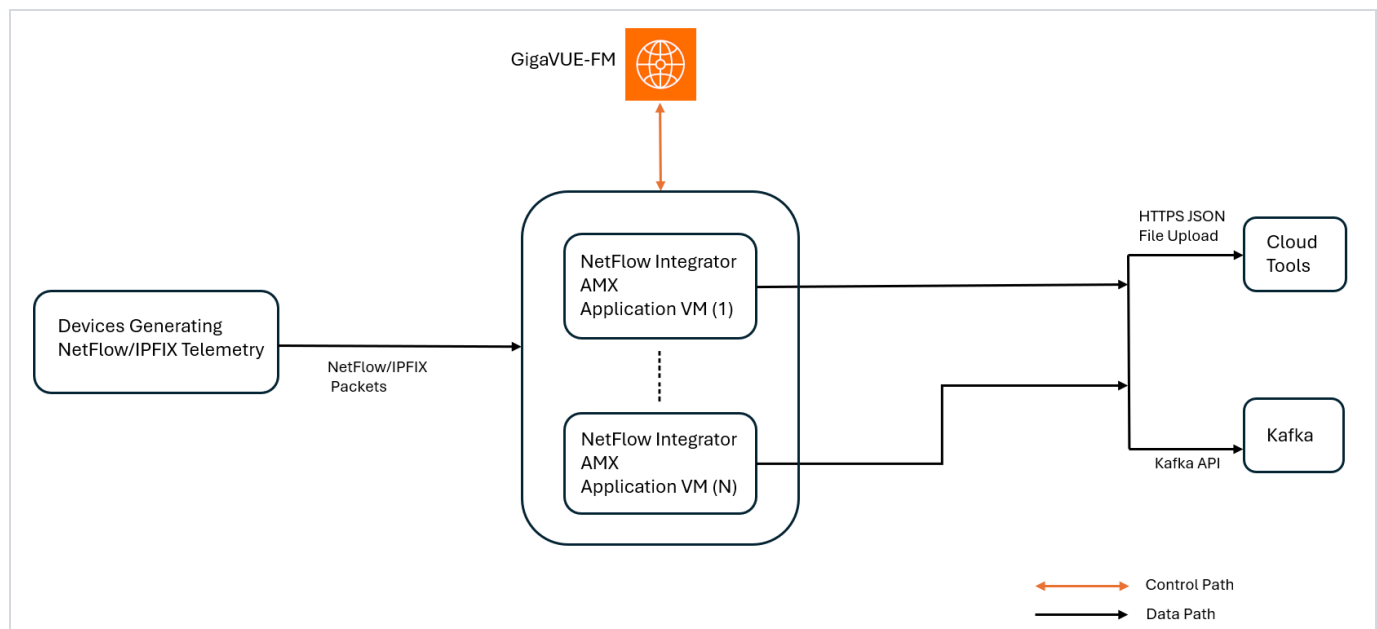
Application Metadata Exporter (AMX) application converts the output from the Application Metadata Intelligence (AMI) in CEF format into JSON format and sends it to the cloud tools and Kafka Consumers. The following image illustrates this end-to-end flow.



Transform NetFlow/IPFIX records to JSON format and export over HTTPS/Kafka

The AMX application with NetFlow Integrator functionality supports ingesting NetFlow/IPFIX flow records from various sources and devices, such as firewalls, routers, and switches, including AMI. It normalizes these records into JSON and exports them to external tools, providing a consolidated view of network traffic and NetFlow/IPFIX insights in a standard format compatible with most Network Performance Monitoring (NPM) tools.

The following image illustrates how the NetFlow Integrator collects NetFlow/IPFIX telemetry from network devices, converts it into JSON, and exports it over HTTPS or Kafka to external cloud tools. GigaVUE-FM acts as the central control system for AMX.



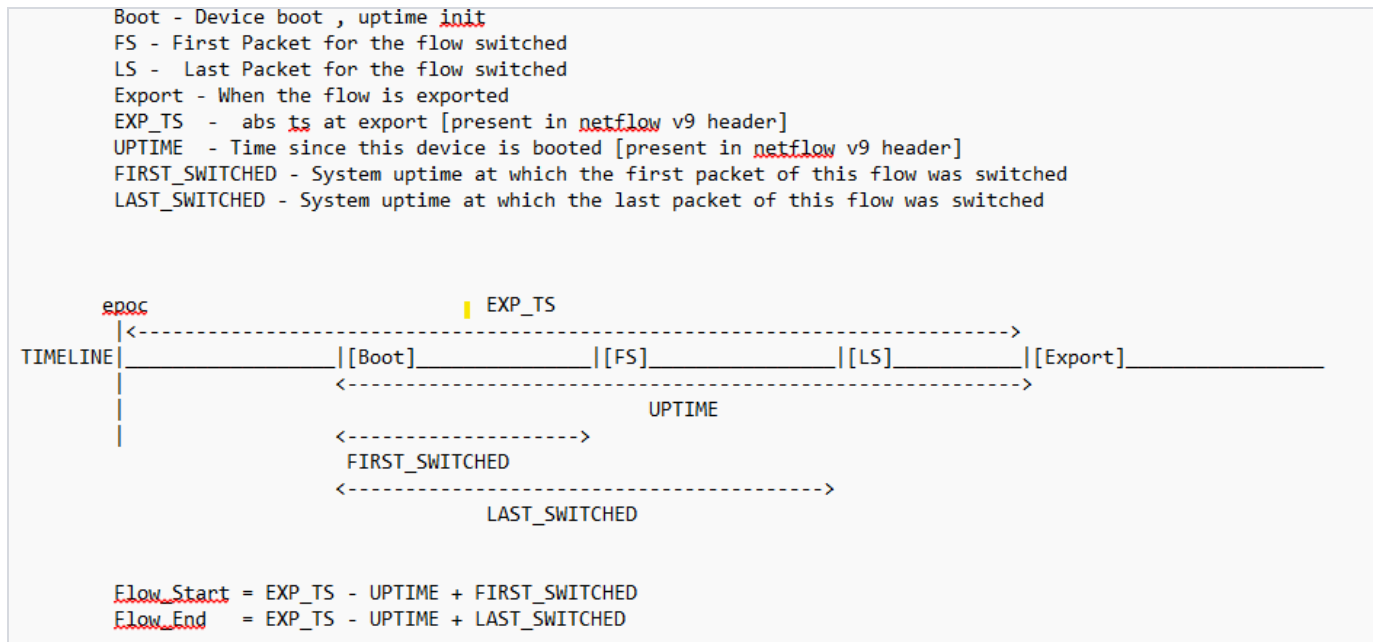
Supported Platforms

- VMware ESXi
- VMware NSX-T

Important Notes

- **NetFlow v9 and v5 Timestamps:**
 - The NetFlow header contains system uptime (in seconds) and an export timestamp.
 - Flow start time is derived using the following formula:
 - $\text{Flow_Start} = \text{Export Timestamp} - \text{System Uptime} + \text{First_Switched}$
 - Flow end time is derived using the following formula:
 - $\text{Flow_End} = \text{Export Timestamp} - \text{System Uptime} + \text{Last_Switched}$
 - The calculated start and end time are converted into nanoseconds.
 - Unsupported attributes such as flow start/end in milliseconds, microseconds, or nanoseconds will be ignored. Instead, the export timestamp is used as both the flow start and end times, which are then converted to nanoseconds.
- **NetFlow v10/IPFIX Timestamps:**
 - NetFlow v10/IPFIX directly incorporates timestamps without the need for system uptime.
 - Even if Flow start and end timestamps are available in seconds, milliseconds, microseconds, or nanoseconds, they are always converted to nanoseconds for output.
- **Missing Flow Start/End Attributes** - For records that do not include flow start or end attributes, AMX automatically assigns both values to the export timestamp.

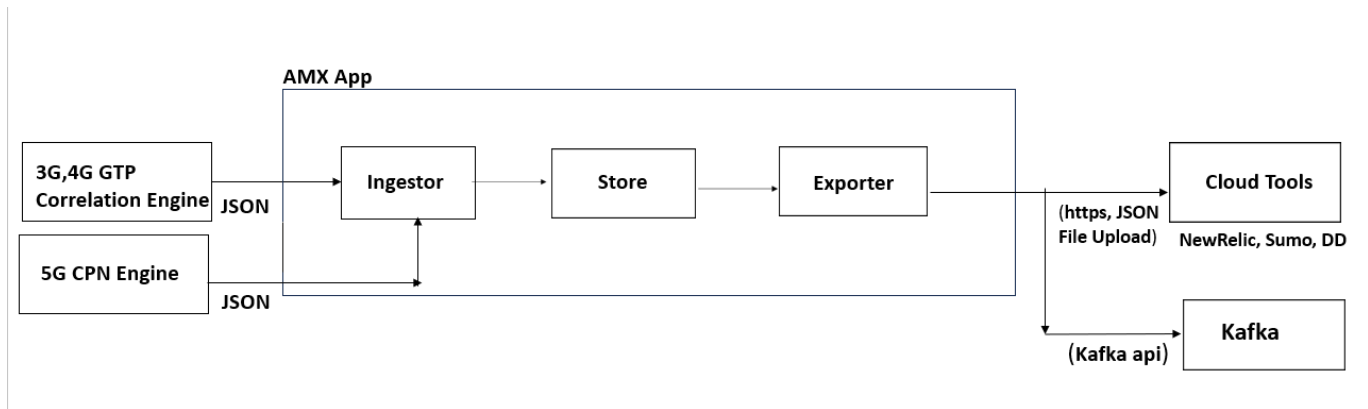
The image below explains how flow start and end times are calculated using system uptime, export timestamp and flow switch times.



Export of 3G/4G/5G Control Plane Metadata by AMX

The AMX application can also export the 3G/4G control plane metadata received from the GTP Correlation engine and 5G control plane metadata received from the 5G CPN engine to the cloud tools and Kafka in Flat JSON format.

The AMX application can be deployed only on a GigaVUE V Series Node and can be connected to a GTP Correlation / 5G CPN engine running on a physical node.



Export GigaVUE Enriched Metadata for Mobile Networks and Export over HTTPS/Kafka

The metadata enrichment enhances service provider analytics, by generating metadata on 5G/4G/3G network traffic. The AMX correlates the user plane metadata produced by AMI with the control plane metadata produced by the GTP/5G correlation mobility application to produce an enriched metadata feed for the mobile networks. This data feed helps with use cases like service personalization, planning, and many others by containing information about the:

- Subscriber Session
- Over the Top Application
- Handset Type
- Location
- Flow throughput calculation attributes - DL, UL bytes, and time stamps.
- Application Protocol
- Core Network Information
- User Tunnel Information

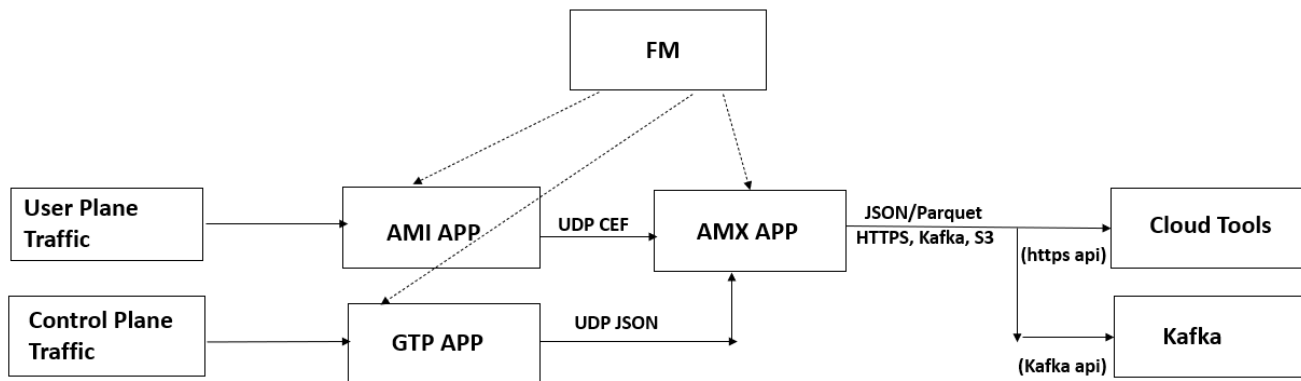
Export of GigaVUE Enriched Metadata for Mobile Networks is supported only for GigaVUE V Series Node deployed using Third Party Orchestration on VMware ESXi.

User Plane and Control Plane traffic from the following devices are supported for exporting GigaVUE Enriched Metadata for Mobile Networks:

- GigaVUE-HC3
- GigaVUE-HC1-Plus

NOTE: For GigaVUE-HC1-Plus, the AMI application must be configured on the built-in engine to efficiently handle higher traffic loads. The plug-in engine can be used for the Control Plane traffic.

For information on Control Plane Metadata, refer to [Control Plane Metadata](#).



Export GigaVUE Enriched Metadata for Cloud Workloads and Export over HTTPS/Kafka

GigaVUE Enriched Metadata for Cloud Workloads provides comprehensive situational awareness to address security and performance pain points in a timely manner. It enriches application metadata from N/S and lateral traffic with key host environment details that allow you to find critical information as follows:

- The location of the workloads hosted and their virtual network.
- The operational environment to which the workloads belong.
- The instance types used, images, and tags that the workload contains.
- The host name, the security associations like security group name, IAM instance profile name.

Export of GigaVUE Enriched Metadata for Cloud Workloads (Virtual Machines)

Export of GigaVUE® Enriched Metadata (GEM) for Cloud Workloads is supported on the following cloud platforms:

- AWS
- Azure

- VMware (ESXi and NSX-T)

This functionality works by using the inventory API which is queried in the following intervals.

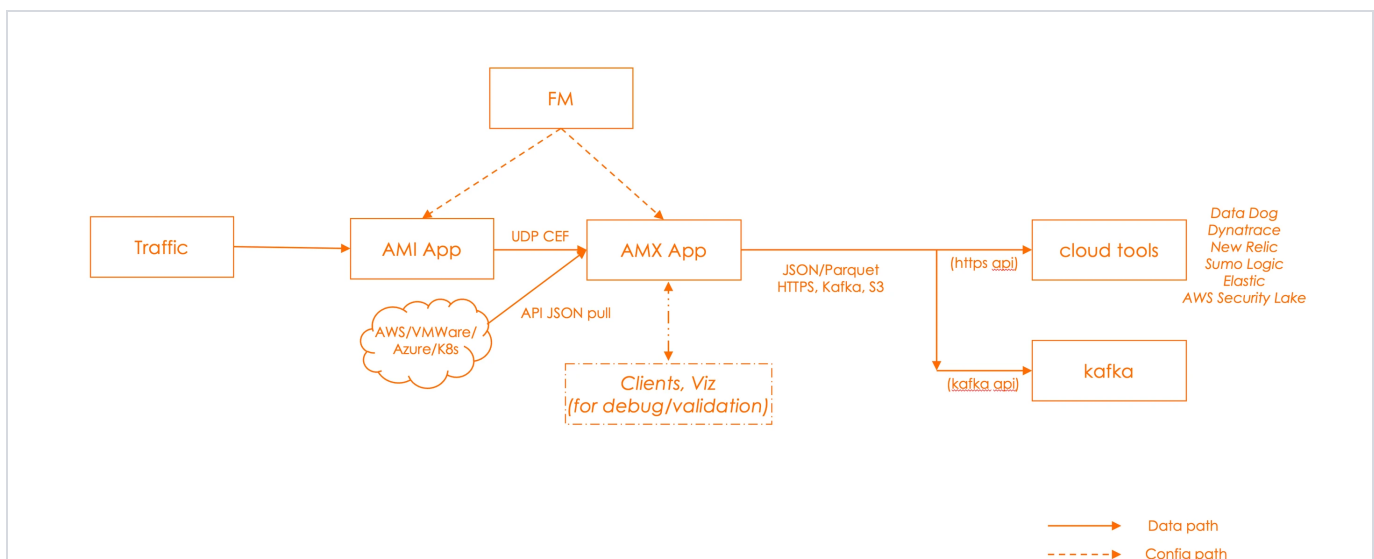
- VMware: 300 sec
- AWS: 30 sec
- Azure: 60 sec

The default inventory query interval should suffice in most cases, however the interval can be customized in extreme situations. [Contact Gigamon Support](#) for assistance.

In addition to these fixed inventory polling intervals, you can subscribe to optional services to receive automatic workload updates in AWS (Event Bridge)/Azure (Event Grid). For VMware, no additional configuration is required because dynamic updates are enabled by default.

AMX application performs the enrichment every 10 seconds. It picks the flow records, which are 15 seconds or older, to allow any delays in fetching the inventory details, and uses the IP address of the endpoints to enrich the records based on the selected attributes. Refer to the following figure for a high-level illustration of the solution. The solution can be deployed using GigaVUE-FM or Third Party Orchestration.

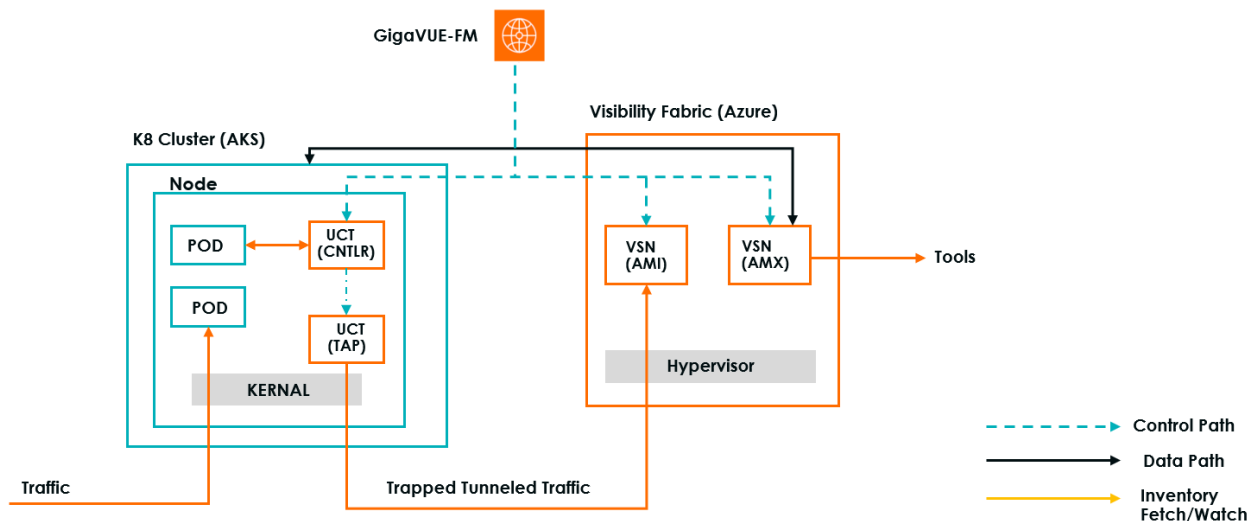
The following image illustrates how AMX exports GigaVUE Enriched Metadata for cloud workloads by converting flow records into JSON/Parquet format and streaming them over HTTPS or Kafka to cloud tools.



The enrichment supported depends on the type of platform. Refer to [Attributes for GigaVUE Enriched Metadata for Cloud Workloads](#) for more details.

Export of GigaVUE Enriched Metadata for Cloud Workloads Kubernetes containers - Azure Kubernetes Service (AKS)

This feature enables the enrichment of flow records with Kubernetes inventory data, unlocking deeper visibility and advanced use cases for containerized environments. In the current Kubernetes visibility solution for AKS, UCT-TAP ships tapped traffic (both east-west and north-south) to the AMI node deployed in Azure. The AMI node then forwards metadata to the AMX node, also deployed in Azure. With the new enhancement, the AMX node enriches the AMI metadata using Kubernetes inventory details fetched directly from the AKS cluster.



GigaVUE-FM queries the Kubernetes inventory every 300 seconds, which is the default interval for monitoring events between inventory fetches. The default inventory query interval should suffice in most cases; however the interval can be customized in extreme situations. Please contact Gigamon Support for assistance.

NOTE: In addition to sending regular queries every 300 seconds, GigaVUE-FM enables a watch mechanism that updates AMX with every event—create, delete, and modify.

For Kubernetes environments, GigaVUE-FM uses a controller with access to the Kubernetes API. The controller subscribes to cluster events and pushes updates in near real-time. No built-in optional services are required.

Refer to [Prerequisites for Export of GigaVUE Enriched Metadata for Cloud Workloads](#) for more detailed information.

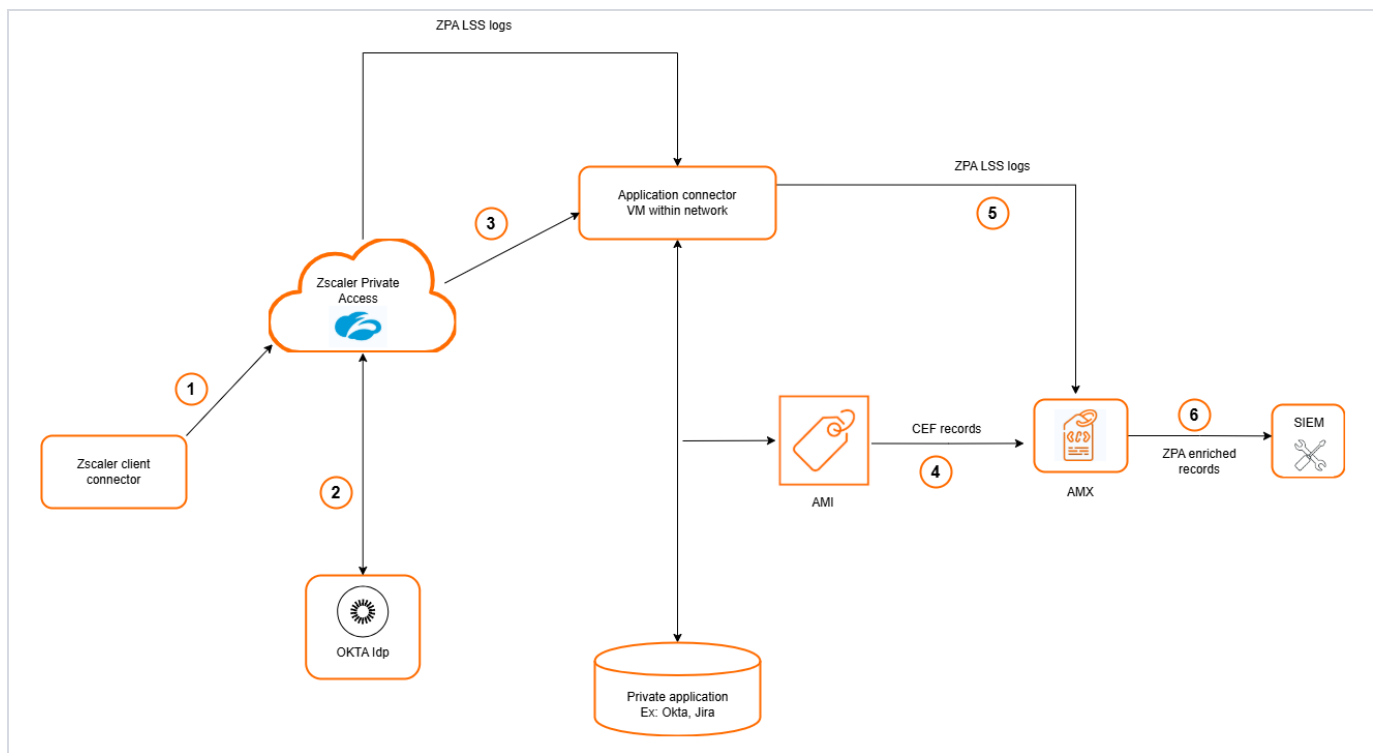
Identity Enrichment using Zscaler Private Access (ZPA)

Zscaler Private Access (ZPA) is a cloud-delivered Zero Trust Network Access (ZTNA) platform that brokers users' access to private applications without putting users on a flat VPN network.

With this feature, GEM enriches application metadata with user details such as username, location, network access policy, etc., AMX ingests Zscaler User Activity Logs through the ZPA Log Streaming Service (LSS), correlates them with application metadata from AMI, and exports the enriched records to tools (for example, SIEM or Observability tools). To reduce tool-side ingestion costs, enrichment is exported at the start of a flow, not for the entire session.

This enrichment can be combined with GEM for Cloud Workloads for VMware, enabling a unified identity enrichment strategy across both ZPA-brokered access and virtualized cloud environments.

The following image shows the ZPA deployment architecture.



The workflow of the ZPA enriched data export is given as follows:

1. A user launches a private application for example OKTA, Jira, which the Zscaler Client Connector identifies as ZPA-protected traffic.

2. The client establishes a tunnel to the ZPA cloud, where the user is authenticated through the IdP and access policies are evaluated.
3. If access is permitted, ZPA selects an appropriate Application Connector with connectivity to the private application, and the Application Connector proxies the traffic to the application.
4. Gigamon physical or virtual taps mirror the traffic to Application Metadata Intelligence, which generates application metadata in CEF format.
5. For the same sessions, ZPA produces LSS User Activity Logs and streams them over TCP to Application Metadata Exporter on the configured listening port.
6. AMX correlates the application metadata with the ZPA User Activity logs using the following 5-tuples, enriches with the selected attributes, and exports records to tools.
 - o Connector IP
 - o Connector Port
 - o Server IP
 - o Server Port
 - o IP Protocol

Prerequisites for Application Metadata Exporter

Prerequisites for Deploying GigaVUE V Series Applications Using GigaVUE-FM

AWS

Prerequisites to follow when creating a monitoring domain and deploying a GigaVUE V Series Node in AWS:

- Select **Traffic Acquisition Method** as Customer Orchestrated Source. Refer to [Create a Monitoring Domain](#).
- Select **Instance type** with three or more NICs. Select one subnet to receive the mirrored GRE or VXLAN tunnel traffic and one other for tools subnet. Refer [Configure GigaVUE Fabric Components in GigaVUE-FM](#) for more detailed information on how to deploy a GigaVUE V Series Node.
- When the **Traffic Acquisition Method** is selected as Customer Orchestrated Source, the Volume Size field appears on the **AWS Fabric Launch Configuration** page. Enter the Volume Size as 80GB.

Azure

Prerequisites to follow when creating a monitoring domain and deploying GigaVUE V Series node in Azure:

- Select **Traffic Acquisition Method** as Customer Orchestrated Source. Refer *Create Monitoring Domain* section in the respective GigaVUE Cloud Suite Deployment Guide for more detailed information on how to create a monitoring domain.
- Select **Size** with three or more NICs. Select one subnet to receive the mirrored GRE or VXLAN tunnel traffic and one other for tools subnet. Refer to [Configure GigaVUE Fabric Components in GigaVUE-FM](#) for more detailed information on how to deploy a GigaVUE V Series Node.
- When the **Traffic Acquisition Method** is selected as Customer Orchestrated Source, the **Disk Size** field appears on the **Azure Fabric Launch Configuration** page. Enter the Disk Size as 80GB.

VMware

Prerequisites to follow when creating a monitoring domain and deploying GigaVUE V Series Node in VMware:

- Select **Traffic Acquisition Method** as Customer Orchestrated Source. Refer *Create Monitoring Domain for VMware ESXi* section in *GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)* for more detailed information on how to create a monitoring domain and deploy GigaVUE V Series Nodes.
- When the **Traffic Acquisition Method** is selected as Customer Orchestrated Source, select the **Form Factor** field as 80GB on the **VMware Configuration** page. Refer to *Configure GigaVUE Fabric Components using VMware ESXi* section in *GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)* for more detailed information on how to deploy GigaVUE V Series Node.
- When uploading the OVF files for GigaVUE V Series Node deployment using third party orchestration, ensure to select the OVF files with 80GB disk space. Refer to the following topics for more detailed information.
 - Deploying GigaVUE V Series Node using Third Party Orchestration (VMware ESXi): *Configure GigaVUE Fabric Components using VMware ESXi* section in *GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)*
 - Deploying GigaVUE V Series Node using Third Party Orchestration (VMware vCenter): *Configure GigaVUE Fabric Components using VMware vCenter* in *GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration*.

Prerequisites for Deploying GV-Cloud V Series Applications Using Third Party Orchestration

Prerequisites to follow when creating a monitoring domain and deploying a GigaVUE V Series Node in Third Party Orchestration:

- Select **Traffic Acquisition Method** as Customer Orchestrated Source. Refer to [Create a Monitoring Domain](#).

- Select **Instance type** with three or more NICs. Select one subnet to receive the mirrored GRE or VXLAN tunnel traffic and one other for tools subnet. Refer [Deploy Fabric Components using Generic Mode](#) for more detailed information on how to deploy a GigaVUE V Series Node.
- When the **Traffic Acquisition Method** is selected as Customer Orchestrated Source, enter the Volume Size, Disk Size, or Form Factor as 80 GB, depending on the selected platform.

Prerequisites for Export of GigaVUE Enriched Metadata for Cloud Workloads

This section provides the detailed steps that need to be performed in each platform for exporting the enriched metadata from cloud workloads.

AWS:

The following section describes how to setup IAM roles with least privileges for exporting GigaVUE Enriched Metadata for Cloud Workloads:

1. Create two IAM roles.
 - First one is for AMX instance that gets launched to let it access assume role (sts) service. (AMXEC2Role)
 - Second one is with **ec2ReadOnlyAccess** permission. (AMXToAssumeRole)
2. Map the instance role to an assume role that has AmazonEC2ReadOnlyAccess permissions.
 - a. Copy arn name of the AMXEC2Role.
 - b. Click **AMXToAssumeRole > Trust Relationships > Edit Trust Policy**.
 - c. Click **Add a principal**.
 - d. Select IAM role as Principal Type. Paste the AMXEC2Role arn that was copied. This is the critical step of mapping two IAM roles.
 - e. Click **Add principal > Update Policy**
3. Add the arn of AMXToAssumeRole in AMX ingestion configuration options.
 - a. Copy the arn and add as aws_assume_role_arn in AWS ingestion configuration.
 - b. If aws_assume_role_arn is configured, there is no need to provide token and keys.
4. (optional) Create an SQS queue. Refer to [Create a queue using the Amazon SQS console](#) in AWS documentation for more detailed information.
5. (optional) Create an EventBridge Rule. In the **Select Target** field, select the SQS queue created in the previous step. Refer to [Creating rules that react to events in Amazon EventBridge](#) in AWS documentation for more detailed information.
6. (optional) Add SQS URL in AMX ingestion configuration options.

Copy the url and add as aws_sqs_url in AWS ingestion configuration.

Azure:

The following instructions need to be configured in Azure for exporting enriched metadata from Azure workloads:

1. Create a Storage Account under the Resource Group. Refer to [Create an Azure storage account](#) in Azure documentation for more detailed information.
2. Create a Storage Queue under the Storage Account. Refer to [Quickstart: Create a queue and add a message with the Azure portal](#) in Azure Documentation for more detailed information.
3. Under the Storage Account > Access Control (IAM). Select “Storage Queue Data Contributor” and select your ID to add the IAM role. Refer to [Assign Azure roles using the Azure portal](#) for more detailed information on how to assign roles.
4. (optional) Create an Event subscription. Refer to [Create an event subscription](#) section in Azure documentation.
5. In the Storage queue, switch the **Authentication method** to **Access key**.

The following section describes how to setup IAM permissions in Azure for exporting GigaVUE Enriched Metadata for Cloud Workloads:

Register an application and assign a role to the application with the following set of minimum IAM permissions. Refer to [Register an application with Microsoft Entra ID and create a service principal](#) and [Assign a role to the application](#) in the Azure documentation for more detailed information.

Minimum IAM permission required:

```
Microsoft.Network/virtualNetworks/read
Microsoft.Network/publicIPAddresses/read
Microsoft.Network/networkSecurityGroups/read
Microsoft.Compute/virtualMachineScaleSets/read
Microsoft.Compute/virtualMachines/read
Microsoft.Compute/images/read
Microsoft.Network/networkInterfaces/read
Microsoft.Resources/subscriptions/read
Microsoft.Resources/subscriptions/resourceGroups/read
```

VMware:

Refer to [Deploy Application Metadata Exporter in VMware ESXi using Third Party Orchestration](#) for prerequisite and predeployment checklist.

Kubernetes (AKS)

The following are the prerequisites required:

1. GEM for Kubernetes requires configuring an Ingestor in GigaVUE-FM to set up the source for Kubernetes containers. You must upload the `k8s_kubeconfig` file during the initial setup. GigaVUE-FM does not allow viewing or editing the uploaded file. However, you can upload a new file to overwrite the existing one.
2. Each ingestor must have a separate `k8s_kubeconfig` file. If you need to configure multiple clusters, create a dedicated `k8s_kubeconfig` file and a corresponding Ingestor for each cluster. You can configure up to four Ingestors.
3. Ensure that the user credentials specified in the `kubeconfig` file have the following sufficient read permissions to access the required Kubernetes resources.
 - Pods
 - Nodes
 - Namespace
 - Endpoints
 - Services
4. If DNS/FQDN is not configured, map the cluster name (as specified in the `server` field of the `kubeconfig` file) to a valid IP address in the `/etc/hosts` file.

Rules and Notes

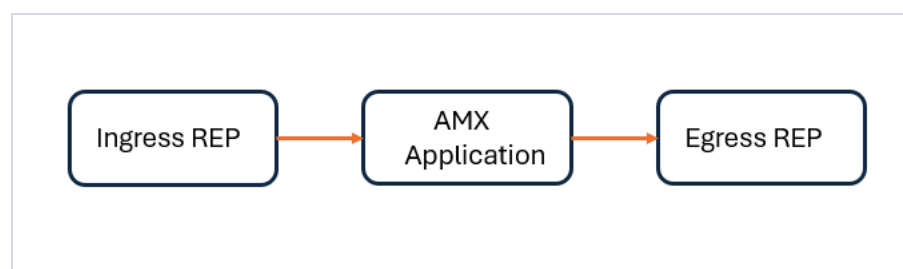
- With any AMI entitlement (AMI SKU, ZTA bundle, or SecureVUE PLUS bundle), you are also entitled to deploy AMX.
- The GigaVUE V Series Node deployed must be entirely dedicated to the AMX application, it cannot have other applications in it.
- The monitoring session can only have Raw End Point (REP), it cannot have other applications, maps, or tunnels when using the AMX application. Refer to *Create Raw Endpoint* section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) for more detailed information on how to add a REP to the monitoring session and how to configure it.
- When using this application for production usage, it is recommended to use large size Virtual Machines.
- If you reload the GigaVUE V Series Node after configuring the AMX application, then the Ingestor in the AMX application fails.
- When using GigaVUE Enriched Metadata for Cloud Workloads, if duplicate IP address is assigned to workloads, the metadata received from the most recently queried workload will be enriched. Hence, it is not recommended to use the feature in environments that are prone to have duplicate IP addresses.
- When using GigaVUE Enriched Metadata for Cloud Workloads, endpoints and the GigaVUE V Series Node running AMI and AMX should be co-located in the same cloud platform.

Configure Application Metadata Exporter

NOTE: Refer to [Prerequisites for Application Metadata Exporter](#) topic for all information related to the prerequisites.

In GigaVUE-FM, you must do the following to configure the Application Metadata Exporter application in the Monitoring Session.

S.No	Steps	Refer to
1	Create an ingress REP	Create Raw Endpoint (VMware vCenter) Create Raw Endpoint (VMware NSX-T) Create Raw Endpoint (AWS) Create Raw Endpoint (Azure) Create Raw Endpoint (Third Party Orchestration)
2	Create a link between the ingress REP and Application Metadata Exporter application	N/A
3	Create an egress REP	Create Raw Endpoint (VMware vCenter) Create Raw Endpoint (VMware NSX-T) Create Raw Endpoint (AWS) Create Raw Endpoint (Azure) Create Raw Endpoint (Third Party Orchestration)
4	Create a link between the Application Metadata Exporter application and egress REP	N/A



To add AMX application:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.

**Notes:**

- Ensure to create separate Monitoring Domains and Monitoring Sessions for Application Metadata Exporter (AMX) and Application Metadata Intelligence (AMI). Even when AMI is deployed virtually, it operates independently and requires its own Monitoring Session.
- You can use the Third-Party Orchestration method when deploying fabric components—such as the AMX V Series Node—on your own.
- When deploying AMX using the Third-Party Orchestration method, Monitoring Session must also be configured in the same work flow. To deploy through Third Party Orchestration, go to **Traffic > Virtual > Orchestrated Flows > Third Party Orchestration**.
- Before deploying AMX, ensure to change the **Traffic Acquisition Method** to **Customer Orchestrated Source** in the Monitoring Domain. Refer to [Create Monitoring Domain](#).

2. After creating a new Monitoring Session or on an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab. The GigaVUE-FM Monitoring Session canvas page appears.
3. In the canvas, click the  icon on the left side of the page to view the traffic processing elements. Drag and drop **AMX** from **APPLICATIONS** to the graphical workspace. The application quick view appears.
4. Enter the **Alias** for the application.

5. In the **Ingestor** section, enter or select the following details. Click  to add another ingestor to add multiple inputs to the AMX application and click  to remove an existing ingestor.

Fields	Description
Name	Enter name for the Ingestor.
Port	Enter the port number to which the Application Metadata or the NetFlow/IPFIX or the Control Plane metadata must be ingested.
Type	Select any one of the following: AMI - Select this option if the input is AMI. Mobility Control Plane - Select this option if the input is Control Plane Metadata. NetFlow/IPFIX - Select this option if the input type is NetFlow/IPFIX. Note: If your selected ingestor type is NetFlow/IPFIX, Metadata Enrichment will be disabled by default. NetFlow/IPFIX input type is not supported for Metadata Enrichment.

6. Enter or select the following details in the **Metadata Enrichment** section:



You can use the **Actions** button to add multiple Metadata Enrichment. Keep in mind the following when configuring multiple Metadata Enrichment:

- You can only configure either Mobility or Workload enrichment
- You can only configure one Metadata enrichment with either **Mobility** or **Workload** as the **Type**
- You can only configure a maximum of 5 Metadata enrichment with **Others** as the **Type**.

Fields	Description
Enrichment Name	Enter a unique name for each enrichment.
Enable	Use this option to enable the enrichment.
Type	Select the type from the drop-down menu. - o Mobility - o Workload - o Others
Mobility	
Attribute Fields	Select the attributes from the list. You can use the Select All option to select all the available attributes. Refer to Attributes for GigaVUE Enriched Metadata for Mobile Networks for more detailed information on the list of available attributes and their description.
Workload	
Platforms	Select the platform in which your Workload Virtual Machines are present. • VMware vCenter • AWS • Azure • Kubernetes
Attribute Fields	Select the attributes from the list. You can use the Select All option to select all the available attributes. Refer to Attributes for GigaVUE Enriched Metadata for Cloud Workloads for more detailed information on the list of available attributes and their description. Advanced Options The advanced options allow you to configure additional details like interval and delay. Click Add. Enter the following details: - o Enter the Key. - o Enter the Value.
Source Information	Enter the details of the source. Name: Enter a unique name for each Source Information. The name should be unique across the ingestor and the source information.

Fields	Description
	Key: The default keys for each platform are listed as follows. Click + to add more keys. AWS: Refer to Manage access keys for IAM users section in AWS documentation for more detailed information on how to create an access key ID and a secret access key. - aws_access_key_id - aws_secret_access_key - aws_region Azure: Refer to Register a Microsoft Entra app and create a service principal section in Azure documentation for more detailed information on how to configure client ID, client secret, tenant ID, and subscription ID in Azure. - azure_client_id - azure_client_secret - azure_tenant_id - azure_subscription_id VMware: - url - The URL of VMware vCenter. - username - Username of the VMware vCenter - password - vCenter password used to connect to the vCenter - self_signed_certificate Kubernetes: - Upload kubeconfig YAML file from your local. Refer to Kubernetes (AKS) for Prerequisites details. Value: Enter the value for the keys. This field is editable after saving the changes. Secure Keys: Use this option to mask the value. After saving the changes, Secure Keys and Key fields are disabled and the value is masked. Click  to add another Source Information and click  to remove a Source Information. You can add multiple Source Information if your workloads are across different vCenters, AWS Accounts, or Azure Subscriptions. You can create an individual Source Information for each of the vCenters, AWS Accounts, or Azure Subscriptions.
	Others: Use this setting to perform custom mapping for advanced use cases. For details contact Gigamon Support.
Attribute Fields	Click Add and enter the attribute.
Settings	Click Add and enter the details.

7. Enter or select the following details in **Cloud Tools Export** section:

Fields	Description
Alias	Enter the alias name for the cloud tool export.
Endpoint	Enter the endpoint URL where the cloud tool instance is installed and the ports are configured. Enable Secure Endpoint option to hide the API keys from the URL. Example: Normal Endpoint: <code>http://examples.com/mykey/key123</code> Masked Endpoint: <code>http://examples.com/mykey/****</code>
Headers	Enter the custom header value of the cloud tool instance. AMX supports exporting headers in the following formats: • JSON array • NDJSON If Content-Type is not configured, AMX defaults to NDJSON and automatically sets content type to application/x-ndjson. Setting the content type to application/json is mandatory to export data in JSON array format. Ensure that the Secure Keys option is enabled.
Type	Select any one of the following: AMI - Select this option to export AMI. Mobility Control - Select this option to export control plane metadata. AMI Enriched - Select this option to export enriched metadata for cloud workloads. NetFlow/IPFIX - Select this option to export NetFlow/IPFIX packets to tools such as HTTPS or Kafka.
Account ID	Enter the account ID number of the selected Cloud Tool.
API Key	Enter the API key of the Cloud Tool.
Source IP Address	Source IP Address is needed when the egress interface is configured with multiple IP addresses. Configure the source IP address which is connected to the Cloud Tool. Both IPv4 and IPv6 are supported. This field is optional.
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Format	The default output format is JSON.
Zip	Enable the box to compress the output file. Enable this field when using New Relic as the cloud tool.
Interval	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 90 seconds.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Export Retries	The number of times the application tries to export the entries to Cloud Tool. The recommended minimum value is 4 and the maximum is 10.
Maximum	The number of JSON entries in a file. The maximum number of allowed entries is

Fields	Description
Entries	20000 and the minimum is 10, however 1000 is the default value.
Backoff Reset Window	With a non-zero value, the exporter keeps trying to reach the tool as many times as the retry. The default setting is 0, and the Backoff Reset Window is disabled at this value.
Request Timeout	This is the time exporter waits for a response back from the tool. The default value is 10 seconds.
Labels	Click Add. Enter the following details: Enter the Key. Enter the Value. Refer to the deployment guides of the respective cloud tools for configuring the Key and Value.

8. Enter or select the following details in the **Kafka Exports** section:

Fields	Description
Alias	Enter the alias name for the Kafka Export.
Topic	The topic name to push JSON streams to, which is generally given to users part of the Kafka administration.
Type	Select any one of the following: AMI - Select this option to export AMI. Mobility Control - Select this option to export control plane metadata. AMI Enriched - Select this option to export enriched metadata. NetFlow/IPFIX - Select this option to export NetFlow/IPFIX ingestor types.
Brokers	The URL that contains the Kafka cluster endpoints. Click  to add another broker and click  to remove an existing broker.
Source IP Address	Source IP Address is needed when the egress interface is configured with multiple IP addresses. Configure the source IP address which is connected to the Kafka Broker. Both IPv4 and IPv6 are supported. This field is optional.
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Format	The default output format is JSON.
Zip	Enable the box to compress the output file.
Interval	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 90 seconds. The default time interval is 30 seconds.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Export Retries	The number of times the application tries to export the entries to Kafka. The recommended minimum value is 4 and the maximum is 10.
Maximum Entries	The number of JSON entries in a file. The maximum number of allowed entries is 20000 and the minimum is 10, however 1000 is the default value.

Fields	Description
Backoff Reset Window	With a non-zero value, the exporter keeps trying to reach the tool as many times as the retry. The default setting is 0, and the Backoff Reset Window is disabled at this value.
Labels	Click Add . Enter the following details: - o Enter the Key. - o Enter the Value.
Producer Configurations	Click Add to enter the authentication details if a Kafka broker needs authentication. For Example: • security.protocol=SASL_SSL • sasl.mechanism=PLAIN or sasl.mechanisms=PLAIN • sasl.username=username • sasl.password=password

- Click **Save** to deploy the Monitoring Session. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the GigaVUE V Series Node for which you wish to deploy the Monitoring Session.
- Click **Deploy** from the **Actions** menu to deploy the Monitoring Session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on all the V Series Nodes.

Switching to outer_ip for Mobility Enrichment

In 5G Control Plane (CP) records, only the lower 64 bits of the inner IP address are captured. To overcome this limitation, you can switch to outer_ip. Follow the steps below based on your configuration:

If AMX is already configured and the Monitoring Session is deployed:

- Undeploy the Monitoring Session in GigaVUE-FM.
- Create a new .yaml file in the GigaVUE V Series Node: vi /etc/amx_settings.yaml
- Modify the enrichment mode:

```
# Default mobility enrichment mode: inner_ip (default) or outer_ip
mobility_outer_ip_version: <Enter version as v6 or v4>
mobility_enrichment_mode: outer_ip
```
- Deploy the Monitoring Session.

During Initial AMX Configuration:

1. Create a new .yaml file in the GigaVUE V Series Node: `vi /etc/amx_settings.yaml`
2. Modify the enrichment mode:


```
# Default mobility enrichment mode: inner_ip (default) or outer_ip
mobility_outer_ip_version: <Enter version as v6 or v4>
mobility_enrichment_mode: outer_ip
```
3. Save the file and proceed with the deployment.

Application Monitoring Options

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab. Refer to [View Application Metadata Exporter Statistics](#) for more detailed information.

Configure Metadata Export Filter for AMX

NOTE: Metadata export filter is now available as an Early Access feature, giving you the opportunity to explore its capabilities before the general availability (GA).

An export filter can be configured to control which metadata records are exported from the Application Metadata Exporter (AMX) to downstream tools such as Kafka. By defining a filter condition, only records that satisfy the specified criteria are exported, reducing unnecessary data volume sent to the target tool. This is an optional functionality that can be used as per the requirement.

The Application Metadata Exporter generally stores all received metadata records in an internal ClickHouse database. The export filter applies a ClickHouse query condition at the exporter component. When the filter is active, only records matching the condition are exported; all other records are dropped before reaching the tool.

Rules and Notes

- The export filter can only be configured by directly editing the `/etc/amx_settings.yaml` file on the V Series Node. This option is not available through GigaVUE-FM.
- The backend does not validate the filter string. Ensure that the value of `set_export_filters` is a valid ClickHouse sub-query. An invalid query may result in no records being exported.

- If the filter is misconfigured or contains an invalid ClickHouse sub-query, AMX does not return an explicit error. Instead, no metadata records are exported. To diagnose such issues, review the AMX logs on the V Series Node for filter-related error messages. Log files are located at `/var/log/syslog/` on the V Series Node.

To configure the export filter:

1. Create or edit the `/etc/amx_settings.yaml` file on the V Series Node where AMX is deployed.
2. Define the `set_export_filters` key with a valid ClickHouse sub-query as its value. For example, `set_export_filters: "mdata['app_name'] LIKE 'http%'"`.
3. To apply the new filter settings, undeploy the monitoring session and then deploy it again.

Deploy Application Metadata Exporter in VMware ESXi using Third Party Orchestration

This section outlines the workflow for deploying Application Metadata Exporter (AMX) application using Third Party Orchestration on VMware ESXi.

Predeployment Checklist:

1. The minimum resource requirements for deploying V Series to configure AMX are as follows. You can deploy one or more V Series for deploying AMX subject to your traffic volume (flows per second). [Contact Gigamon Support](#) for sizing guidance, if needed.
 - **8 vCPUs, 16 GB memory, and 80 GB disk space** for exporting Application Metadata in JSON format.
 - **40 vCPUs, 64 GB RAM, 128 GB disk space** for exporting NetFlow/IPFIX records in JSON format.

Exporting JSON records involves file read/write operations; using SSD storage is recommended.

2. Ensure you have a valid SecureVUE Plus VBL license to deploy AMX and to export NetFlow/IPFIX records in JSON format. With any AMI entitlement (AMI SKU, ZTA bundle, or SecureVUE PLUS bundle), you are also entitled to deploy AMX.
3. Ensure you have access to the [VUE Gigamon Community portal](#) for downloading V Series OVA image.
4. V Series requires three interfaces for deploying AMX—management, data, and tool. It is recommended to allocate dedicated interface for each. Create three separate port groups (ESXi/vCenter) or subnets (other platforms): a Management Port Group for connectivity to GigaVUE-FM, a Data Port Group for receiving traffic such as application metadata in CEF or NetFlow/IPFIX formats, and a Tool Port Group for exporting JSON records.

Note: Preparing a network topology with the IP layout helps in configuration, monitoring, and troubleshooting.

5. Select the appropriate deployment mode for the GigaVUE V Series node based on your requirements:
 - Single physical uplink for Management, Data and Tool connectivity.
 - Single physical uplink for Management and Tool connectivity, and another uplink for Data connectivity.
 - (Recommended) Separate uplinks (three) for Management, Data, and Tool connectivity.
6. If static IP addressing is used, obtain the following details from your server team:
 - IP addresses for the management, data, and tool interfaces.
 - IP address of the DNS server and the gateway connected to the tool interface.
 - Subnet Mask and MTU.
7. Verify whether remote web console access to the V Series is available. Console access is required for troubleshooting. If remote access is not available, request the server team to enable SSH access.
8. Review the deployment guide for the tool specific configuration needed to export records from AMX. Refer to [AMX Tool Integration](#).
9. Review the connectivity requirements for GigaVUE-FM, AMI, AMX, and the associated tools in your environment. Ensure that the required ports are open and any external connectivity dependencies are addressed.
10. Ensure that the standalone GigaVUE-FM deployment meets the recommended requirements shown in the following table. For medium and large scale deployments, refer to [Recommended Requirements for GigaVUE-FM Deployments](#). This step is optional. A standalone GigaVUE-FM instance is required only when an existing GigaVUE-FM is not available for managing AMX.

Requirements	Small Scale Deployment
CPU	
CPU count(minimum)	2
CPU Min speed (per CPU)	2.30GHz
Memory	
Memory Size	16GB
Disk Space	
OS Disk Size (min)	40GB
Config Disk Size - 15 Days Data	80GB

Requirements	Small Scale Deployment
Config Disk Size - 35 Days Data	160GB
Config Disk Size - Rollup 35 Days + 120 Days Rollup	200GB
NIC	1
Number of NICs	1GB
Management/Data	
Appliance Scalability	Up to 50
Number of GigaVUE HC Series/GigaVUE TA Series Devices	Up to 50
Number of GigaVUE V Series Nodes	1 Cluster with 100 Nodes and 10000 pods with 2 rules
Number of Worker Pods monitored	

Refer to the following topics to deploy AMX using Third Party Orchestration:

- [\(Optional\) Install GigaVUE-FM using ISO Image File on VMware ESXi Host](#)
- [\(Optional\) Configure Metadata Export Filter for AMX](#)
- [\(Optional\) Configure Role-Based Access for Third Party Orchestration](#)
- [Create Monitoring Domain to Acquire Traffic from Customer Orchestrated Source](#)
- [Create Tokens to Secure REST API and Third Party Orchestration Access to GigaVUE-FM](#)
- [Deploy V Series Node and Register with GigaVUE-FM](#)
- [Create a Monitoring Session to Configure Application Metadata Exporter](#)
- [Configure Ingestor in AMX to Process Traffic](#)
- [Integrate AMX with Third Party Tool](#)
- [Configure Exporter to Export Attributes to Third Party tools](#)
- [Verify Your Deployment](#)

(Optional) Install GigaVUE-FM using ISO Image File on VMware ESXi Host

This step is optional and applies only when an existing GigaVUE-FM instance is not available.

To install:

1. Log in to the VMware ESXi host web interface.

2. In the ESXi Host Client, go to **Storage > Datastore browser** for a datastore that is accessible to the host.
 3. Click **Upload** and select the GigaVUE-FM ISO image from your local system to a suitable folder on the datastore.
 4. After uploading the ISO image file, go to the **Virtual Machines** and select **Create/Register VM**. The New Virtual Machine wizard appears.
 5. In the **Select creation type** page, select **Create a new virtual machine** and click **Next**.
 6. In the **Select a name and guest OS** page:
 - o Enter a name for the virtual machine.
 - o Select the **Guest OS family** as Linux.
 - o Select the **Guest OS version** as Other Linux (64-bit).
 - o Click **Next**.
 7. In the **Select storage** page, choose the datastore where the VM files will reside and click **Next**.
 8. In the **Customize settings** page:
 - a. On the **Virtual Hardware** tab, enter the following details:
 - CPU: 2
 - Memory: 16GB
 - Hard disk 1: 40GB
 - Click **Add hard disk** to add two more disks with 4GB and 40GB.
 - b. In the **CD/DVD Drive**, select **Datastore ISO file**. The Datastore browser appears.
 - c. Select the ISO image uploaded in Step 3. By default, the **Connect** checkbox for both **Network Adapter** and **CD/DVD Drive** is enabled.
 - d. On the **VM Option** tab, expand **Boot Options**, and under Firmware, select **EFI**.
 - e. Click **Next**.
- NOTE:** If you leave the firmware as BIOS, GigaVUE-FM attempts to boot in BIOS mode, and the boot process fails .
9. Review all settings on the **Ready to complete** page and click **Finish** to create the virtual machine.
 10. Select the newly created VM and click **Power on**.
 11. Open the VM console to monitor the boot process. It may take approximately 15–20 minutes for the VM to boot.

Access GigaVUE-FM

1. Log in to GigaVUE-FM using the IP address available on the ESXi web Interface.

2. Use the following default login Credentials:
 - Username: admin
 - Password: admin123A!!
3. On first login, you will be asked to change the password. Enter the current password, then set and confirm a new one.

(Optional) Configure Metadata Export Filter for AMX

Optionally, you can configure an export filter to control which metadata records are exported from AMX. For more information, see [Configure Metadata Export Filter](#).

(Optional) Configure Role-Based Access for Third Party Orchestration

If you do not want to use an **Admin Profile** to deploy GigaVUE V Series through a Third Party orchestrator, you can create the required users, roles, and user groups in GigaVUE-FM.

Create a Custom User

You can add users only if you are a user with **fm_super_admin role** or a user with either read or write access to the GigaVUE-FM security Management category.

To add users:

1. Go to **Settings** and select **Authentication > GigaVUE-FM User Management > Users**.
2. On the User page, select **New User**.
3. In the Add User page, enter the following details:
 - **Name:** Actual name of the user
 - **Username:** User name configured in GigaVUE-FM
 - **Email:** Email ID of the user
 - **Password/Confirm Password:** Password for the user.
 - **User Group:** Select the desired User Group to associate the user.
GigaVUE-FM prompts for your password.
4. Click **Ok**. The new user is added.

Create a Custom Role and Assign the User

A user role defines permission for users to perform any task or operation in GigaVUE-FM or on the managed device. You can associate a role with user.

NOTE: A user with read-only access cannot perform configurations on the screen. The menus and action buttons in the UI pages are disabled appropriately.

To create a role:

1. Go to **Settings** and select **Authentication > GigaVUE-FM User Management > Roles**.
2. Select **New Role**.
3. In the New Role page, select or enter the following details:
 - **Role Name:** Name of the role.
 - **Description:** Description of the role.
 - **Select Permission:** From the **Select Permissions** tab, select **Third Party Orchestration**, and provide write permissions.
4. Select **Apply** to save the configuration.

Create a Custom User Group and Assign the Custom Role and the User

A user group consists of a set of roles and set of tags associated with users in that group. You can associate the user to one or more groups.

To create a new user group:

1. Go to **Settings**, and then select **Authentication > GigaVUE-FM User Management > User Groups**.
2. Select **New Group**.
3. In the New User Group page, select **Next** to progress forward and **Back** to navigate backward.
4. In the **Group Info** tab, enter the Group Name and Description details:
5. In the **Assign Roles** tab, select the role that you want to assign to the user group.
6. In the **Assign Tags** tab, select the required tag key and tag value.
7. In the **Assign Users** tab, select the required users.
8. Select **Apply** to save the configuration. The new user group is added.

Create Monitoring Domain to Acquire Traffic from Customer Orchestrated Source

To create a Monitoring Domain in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > Third Party Orchestration**, and select **Monitoring Domain**. The **Monitoring Domain** page appears.
2. On the **Monitoring Domain** page, select **New**. The **Monitoring Domain Configuration page** appears.
3. Enter a name for the **Monitoring Domain**.
4. Enter a name for the **Connection**.
5. Select **Customer Orchestrated Source** as the **Traffic Acquisition Method**.

6. Click **Save**.

Create Tokens to Secure REST API and Third Party Orchestration Access to GigaVUE-FM

Use tokens when applications or users access GigaVUE-FM through REST APIs or when registering GigaVUE V Series using Third Party Orchestration. Tokens let GigaVUE-FM verify who is making the API calls and what they are allowed to do, without exposing passwords.

You can create tokens only if you are a user with **fm_super_admin role** or a user with write access to the GigaVUE-FM security Management category.

To create a token:

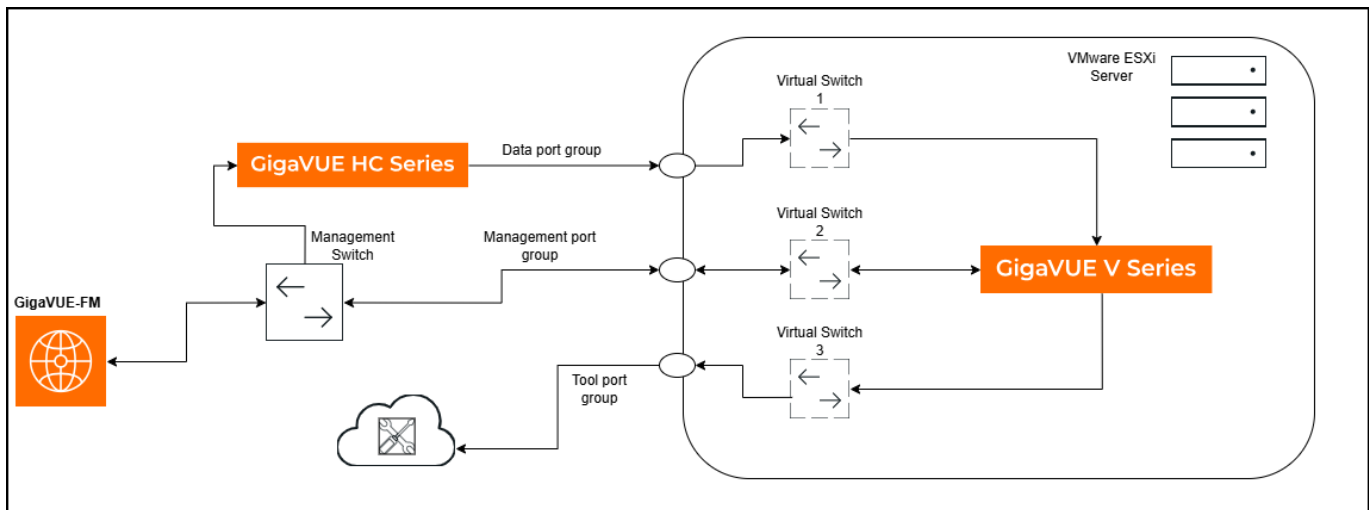
1. Go to **Settings > Authentication > GigaVUE-FM User Management**. The **User Management** page appears.
2. Select **Current User Tokens** from the **Tokens** drop-down list.
3. Click **New Token**. The **New Token** pop-up appears.
4. Enter a name for the new token in the **Name** field.
5. Enter the days until the token is valid in the **Expiry** field.
6. Select the user group for which you are privileged to access the GigaVUE-FM from the **User Group** drop-down list. The token inherits the read or write RBAC privileges of this group.
7. Select **OK** to generate a new token. You can copy and use the generated token to authenticate the GigaVUE-FM REST APIs.

Deploy V Series Node and Register with GigaVUE-FM

The following image illustrates a scenario for deploying and registering a GigaVUE V Series node. In this example, a GigaVUE HC Series device monitors north-south traffic and forwards Application Metadata to a SIEM/observability tool that accepts only JSON records. The entire solution is managed through GigaVUE-FM.

The GigaVUE HC Series uses Application Metadata Intelligence to generate application metadata in CEF format. Application Metadata Exporter, running on the GigaVUE V Series node, converts these CEF records to JSON before exporting them to the tool over HTTPS or Kafka.

NOTE: AMI is supported on both GigaVUE HC Series and GigaVUE V Series platforms. You can also deploy a separate GigaVUE V Series node to generate application metadata for monitoring east-west traffic.



To deploy and register:

1. Log into the vSphere or VMware ESXi web interface.
2. Right-click the ESXi Host, Cluster or data center (if using vSphere) on which you want to deploy the GigaVUE V Series Node and then select **Create/Register VM**. The **New Virtual Machine** wizard appears.
3. In the **Select Creation Type** page, select Deploy a virtual machine from an OVF and OVA file option. Downloaded the AMX supported OVA from the [VUE Gigamon Community portal](#). Extract the OVA to obtain the OVF and VMDK files, then select **vseries-node-file-ovf15.ovf** (AMX-supported OVF that brings up three interfaces) for the AMX deployment.
4. Click **Next**. The **Select OVF and VMDK files** page appears.
5. In the **Select and VMDK files** page, enter a unique name for the virtual machine and upload the .ovf and .vmdk files from your local machine.
6. Click **Next** and the **Select storage** page appears.
7. Select a datastore where the virtual machine's files will be stored.
8. Click **Next**. The **Deployment Options** page appears.
9. In the **Deployment Options** page, select the management port, data port, and tool port as referenced in the prerequisites.
 - a. Select the **Deployment Type** from the list:
 - Do Not Use DHCP – Select this option if you want to use static IP addresses for the management, data, and tool ports.
 - Management, Data and Tool Port DHCP – Select this option if you want to use dynamic IP addresses for the management, data, and tool ports.
 - Management Port DHCP – Select this option if you want to use dynamic IP address only for the management port.

- Tool Port DHCP - Select this option if you want to use dynamic IP address only for the tool port.
 - Data Port DHCP – Select this option if you want to use dynamic IP address only for the data port.
- b. Select Thin/Thick in the **Disk Provisioning** field.
 - c. Unselect the **Power on automatically** check box. This is selected by default. It is recommended to disable the Power on automatically option and review all configuration before switching on the virtual machine.
10. Click **Next**. The **Additional Settings** page appears.
 11. Do the following configuration in the **Additional Settings** page.
 - a. In the **System** section, enter the hostname of the V Series node instance in the **Hostname** field and create a new admin password for the V Series node instance in the **Administrative Login Password** field.

This credential will be used for V series SSH access. The default username is gigamon. If the deployment fails, you can login to V Series SSH/Console and check the logs for troubleshooting.
 - b. In the **Network Connectivity** section, enter the required fields based on the selected network configuration.

NOTE: Ensure to unselect the **Management Port DHCP** checkbox if you want to use static IP address for the management port. If you select the Management Port DHCP checkbox, dynamic IP address will be configured for the management port even if you have selected Do Not Use DHCP option in the Configuration page.

- c. Enter the required value in the **Management Port MTU size in bytes** field. The default value is 1500B.
- d. Enter the DNS server address in the **Nameserver** field to resolve the domain name of the tool destination URL.
- e. In the **Optional Parameters** section, enter the Monitoring Domain name in the **GroupName** field and connection name in the **SubGroupName** field. The Monitoring Domain and connection name corresponds to the domain name and connection that you created during the [Create Monitoring Domain to Acquire Traffic from Customer Orchestrated Source](#) configuration.
- f. Enter the token created in GigaVUE-FM in the **JWT Token used for registration** field. Refer to [Create Tokens to Secure REST API and Third Party Orchestration Access to GigaVUE-FM](#).

- g. Enter the GigaVUE-FM IP address and remote port in the **RemoteIP** and **RemotePort** fields respectively. In case of any error, you should re-deploy the V Series.
- h. In the **Custom node properties** field enter `app_mode=linux_apps` (mandatory).
12. Click **Next** and the **Ready to complete** page appears.
13. Review all the entered information and modify the configuration if required.
14. Click **Finish**. When the operation completes, you have successfully deployed a GigaVUE V Series Node.

Verify GigaVUE V Series Node Registration

During the initial bring up, the V Series reboots multiple times for initialization. After few minutes, you can check the status of the deployment in GigaVUE-FM. If the status is failed, you can check the logs to perform troubleshooting.

To check the logs:

1. Log in to V Series Node via console or SSH to management IP address.
2. Enter the below path in the terminal to check the registration details.

```
tail -f /var/log/vseries-node-reg.log
```

A single AMX instance processes traffic within the published performance KPIs. Deploy additional instances when traffic volume exceeds these thresholds or when packet drops occur, or CPU or memory utilization remains consistently high, to maintain stable and efficient performance. For details regarding performance KPIs, [Contact Technical Support](#).

Create a Monitoring Session to Configure Application Metadata Exporter

In GigaVUE-FM, you must do the following to configure the Application Metadata Exporter application in the Monitoring Session.

1. **Access the Monitoring Session Page:**
 - a. In GigaVUE-FM, go to **Traffic > Virtual > Orchestrated Flows > Third Party Orchestration**.
 - b. After creating a new Monitoring Session or on an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab. The GigaVUE-FM Monitoring Session canvas page appears.
2. **Create an ingress REP:**
 - a. In the canvas, from the New expand menu, drag and drop New Raw Endpoint to the graphical workspace.
 - b. On the new raw endpoint icon, select the  menu button and select **Details**. The **Raw** quick view page appears.

- c. Enter the Alias and Description details for the Ingress Raw End Point and click **Save**.

3. Add AMX Application:

- a. In the canvas, from the **Applications** expand menu, drag and drop AMX to the graphical workspace.
- b. Configure the ingestor settings to process traffic. Refer to [Configure Ingestor in AMX to Process Traffic](#) for details.
- c. Configure the required exporter settings to export attributes to Third Party tools. Refer to [Configure Exporter to Export Attributes to Third Party tools](#) for details.
- d. Create a link between the ingress REP and Application Metadata Exporter application.

4. Create an egress REP:

- a. From the **New** expand menu, drag and drop New Raw Endpoint to the graphical workspace.
- b. On the new raw endpoint icon, select the  menu button and select **Details**. The **Raw** quick view page appears.
- c. Enter the Alias and Description details for the Egress Raw End Point and click **Save**.
- d. Create a link between the Application Metadata Exporter application and egress REP



Notes:

- Ensure to create separate Monitoring Domains and Monitoring Sessions for Application Metadata Exporter (AMX) and Application Metadata Intelligence (AMI). Even when AMI is deployed virtually, it operates independently and requires its own Monitoring Session.
- When deploying AMX using the Third-Party Orchestration method, Monitoring Session must also be configured in the same work flow.

Configure Ingestor in AMX to Process Traffic

The following scenarios provide more information about the different ways to configure Ingestor AMX:

- [Scenario 1 - Export Application Metadata in JSON format over HTTPS/Kafka](#)
- [Scenario 2 - Export GigaVUE Enriched Metadata for Mobile Networks and Export over HTTPS/Kafka](#)
- [Scenario 3 - Export GigaVUE Enriched Metadata for Cloud Workloads and Export over HTTPS/Kafka](#)

- [Scenario 4 - Transform NetFlow/IPFIX records to JSON format and export over HTTPS/Kafka](#)
- [Scenario 5 - Configure Identity Enrichment Metadata using Zscaler Private Access \(ZPA\)](#)

Scenario 1 - Export Application Metadata in JSON format over HTTPS/Kafka

Refer to [Application Metadata Exporter - Export Scenarios](#) topic for more details and conceptual information.

To configure ingestor for AMI:

1. On the AMX quick view in the **Ingestor** section, enter an alias name for the ingestor.
2. In the **Type** field, select **AMI** as the input type.
3. Enter the port number on which Application Metadata must be ingested. The default port value is 514.
4. Click  to add another ingestor to add multiple inputs to the AMX application and click  to remove an existing ingestor.

Scenario 2 - Export GigaVUE Enriched Metadata for Mobile Networks and Export over HTTPS/Kafka

Refer to [Application Metadata Exporter - Export Scenarios](#) topic for more details and conceptual information.

To export GigaVUE Enriched Metadata for Mobile Workloads:

1. On the AMX quick view in the **Ingestor** section, enter an alias name for the ingestor.
2. In the **Type** field, select **AMI** as the input type.
3. Enter the port number on which Application Metadata must be ingested. The default port value is 514.
4. Click  to add another ingestor.
5. In the Type field, select **Mobility Control Plane** as the input type.
6. Enter the port number on which application metadata must be ingested.
7. Click  again to add another ingestor to add multiple inputs to the AMX application and click  to remove an existing ingestor.
8. In the **Metadata Enrichment** section, enter a unique name for the enrichment.
9. Select the Enable option to enable the enrichment.
10. Select **Mobility** from the **Type** drop-down menu.

11. Select the required attributes from the list. You can use **Select All** to choose all available attributes. Refer to the [Attributes for GigaVUE Enriched Metadata for Mobile Networks](#) for more details.

Scenario 3 - Export GigaVUE Enriched Metadata for Cloud Workloads and Export over HTTPS/Kafka

Refer to [Application Metadata Exporter - Export Scenarios](#) topic for more details and conceptual information.

To export GigaVUE Enriched Metadata for Cloud Workloads:

1. On the AMX quick view in the **Ingestor** section, enter an alias name for the ingestor.
2. In the Type field, select **AMI** as the input type.
3. Enter the port number on which Application Metadata must be ingested. The default port value is 514.
4. Click  to add another ingestor.
5. In the Type field, select **Mobility Control Plane** as the input type.
6. Enter the port number on which Application Metadata must be ingested.
7. Click  again to add another ingestor to add multiple inputs to the AMX application and click  to remove an existing ingestor.
8. In the **Metadata Enrichment** section, enter a unique name for the enrichment.
9. Select the Enable option to enable the enrichment.
10. Select **Workload** from the **Type** drop down menu.
11. Select the platform as **VMware VCenter** from the drop down list.
12. Select the required attributes from the list. You can use **Select All** to choose all available attributes. Refer to the [Attributes for GigaVUE Enriched Metadata for Cloud Workloads](#) for more details.

Scenario 4 - Transform NetFlow/IPFIX records to JSON format and export over HTTPS/Kafka

Refer to [Application Metadata Exporter - Export Scenarios](#) topic for more details and conceptual information.

To configure ingestor for NetFlow/IPFIX:

1. On the AMX quick view in the **Ingestor** section, enter an alias name for the ingestor.

2. In the Type field, select the input type as **NetFlow/IPFIX**. Only the elements specified in the mapping file will be included in the JSON output. Editing or customizing the mapping file is not supported. Refer to [Supported Element Types for NetFlow Integrator Element Mapping](#).
3. Enter the port number on which NetFlow/IPFIX must be ingested. The default port value is 2055.
4. Click  to add another ingestor to add multiple inputs to the AMX application and click  to remove an existing ingestor. A maximum of 12 NetFlow/IPFIX type ingestors can be configured per deployment.

NOTE: If you select NetFlow/IPFIX as the ingestor type, Metadata Enrichment is disabled by default. Metadata Enrichment is not supported for NetFlow/IPFIX inputs.

Scenario 5 - Configure Identity Enrichment Metadata using Zscaler Private Access (ZPA)

Refer to [Application Metadata Exporter - Export Scenarios](#) topic for more details and conceptual information.

Prerequisites

Before configuring identity enrichment using Zscaler Private Access (ZPA), ensure that the following prerequisites are met.

Zscaler Infrastructure

The following Zscaler components must already be set up in your environment. These are standard ZPA deployment requirements. For detailed instructions, refer to the Zscaler documentation.

- **Acquire Zscaler Tenant Access:** Ensure that you have admin access to the Zscaler Private Access admin portal (ZPA tenant). Refer to [Zscaler Tenant Access](#) for more information.
- **Integrate Identity Provider (IdP):** An IdP (such as Okta, Microsoft Azure AD, or any supported IdP) must be configured and integrated with ZPA. ZPA uses the IdP to authenticate users before granting access to private applications. Refer to [About External Identity Providers](#) for more information.
- **Configure App Connector Group :** At least one App Connector group must be created and have active App Connectors registered to it. You can use an existing App Connector group or create a new one before proceeding. For instructions, refer to the Zscaler documentation. Refer to [Configuring App Connector Groups](#) for more information.

- **Install App Connector:** The Zscaler App Connector package must be downloaded and installed on a Linux-based VM (Ubuntu, plain Linux, or similar) in the domain where your private applications reside. Refer to the scaler App Connector deployment guide for platform-specific instructions (Linux, Docker, GCP, Kubernetes, and so on). Refer to [App Connectors](#) for more information.
- **Define Private Applications:** Application segments must be created for all private applications you want to monitor (for example, internal web apps, Jira, databases). Each application segment must include the application IP address and port range, and must be linked to a server group and an App Connector group. Refer to [Configuring Defined Application Segments](#) for more information.

Gigamon Infrastructure

- **Deploy VSN Node with AMX on ESXi:** The Application Metadata Exporter (AMX) must be deployed on a V Series Node (VSN). In this release, only the ESXi platform is supported. The IP address of the VSN node on which AMX is running, as it is required when configuring the ZPA Log Receiver. Refer to [Deploy V Series Node and Register with GigaVUE-FM](#) for more information.
- **Configure AMI:** Application Metadata Intelligence (AMI) must be active and generating flow records. The AMI metadata (source IP, destination IP, source port, destination port) is used to match and enrich flows with ZPA log data. For more information on configuring AMI, refer to [Configure Application Metadata Intelligence for Virtual Environment](#).

Integrate ZPA with Gigamon AMX

After the Zscaler infrastructure and Gigamon infrastructure are set up, configure a Log Receiver in the ZPA admin portal to stream ZPA logs to AMX. This is the key step that establishes the integration between ZPA and Gigamon.

The following table lists the specific options you must select when configuring a log receiver to integrate with AMX. For navigation steps and detailed instructions, refer to [Configuring Log Receiver](#) topic in Zscaler documentation.

Parameters	Description
Log Receiver	
Name	Enter a name for the log receiver.
Domain or IP Address	Enter the domain or IP address to the IP address of the VSN node on which AMX is deployed (not the ESXi host IP address).
TCP Port	Enter the same port that is configured as the ZPA LSS ingestor port on AMX.
App Connector Groups	Select an app connector group that was created.
Log Stream	
Log Type	Select User Activity as the log type.
Log Template	Select the Custom template.
Log Stream Content	Add the new user activity log ("ConnectionSetupTime": %j {ConnectionSetupTime} }\n) in the content.

Configure Ingestor for AMX

You can configure metadata enrichment for ZPA only. Optionally, you can combine it with GEM for Cloud Workloads for VMware vCenter.

To export identity enrichment metadata using ZPA :

1. Configure an ingestor for AMX
 - a. On the AMX quick view in the **Ingestor** section, enter an alias name for the ingestor.
 - b. In the **Type** field, select **AMI** as the input type.
 - c. Enter the port number on which application metadata must be ingested. The default port value is 514.
 - d. Click  to add another ingestor to add multiple inputs to the AMX application and click  to remove an existing ingestor.
2. Configure identity metadata enrichment using ZPA
 - a. On the AMX quick view in the **Metadata Enrichment** section, enter an alias for the enrichment.
 - b. Select the **Enable** option to enable the enrichment.
 - c. In the **Type** field, select **Identity** as the input type.
 - d. Select **Zscaler Private Access** from the **Platform** dropdown list.
 - e. Select the attributes for identity enrichment from the **Attributes** tab.
 - f. In the **Source Information** tab, enter the port number on which AMX receives the ZPA LSS logs.
 - g. Click  to add another ZPA source information to add multiple inputs to the AMX application and click  to remove an existing source information.
3. (Optional) Configure GigaVUE Enriched Metadata workload for ESXi
 - a. On the AMX quick view in the **Metadata Enrichment** section, enter an alias for the enrichment.
 - b. Select the Enable option to enable the enrichment.
 - c. In the **Type** field, select **Workload** as the input type.
 - d. Select **VMware vCenter** from the **Platform** dropdown list.

NOTE: Only VMware vcenter platform is applicable as additional workload along with ZPA.

- e. Select the required workload attributes for ESXi.
- f. In the Source Information tab, enter the Key-Value pair details as given:
 - Key - url and Value - Primary URL for the vCenter Server SDK. For example, `https://<vCenter-IP-or-FQDN>/sdk`.
 - Key - username and Value - VMware vCenter username.
 - Key - password and Value - vCenter password.
- g. Click  to add another ESXi source information to add multiple inputs to the AMX application and click  to remove an existing source information.

Integrate AMX with Third Party Tool

This section explains how to set up the third-party tool and configure the exporter settings required to route application metadata attributes for analysis and visualization.

Set up the Third Party Tool for AMX Integration

You must set up the third party tools to ingest and visualize application metadata.

Refer to [AMX Tool Integration](#) for configuration guidance and the verification steps required to confirm that data export and visualization are functioning correctly.

Configure Exporter to Export Attributes to Third Party tools

AMX supports the following types of exporters:

- [Configure Cloud Tool Exporter](#)
- [Configure Kafka Exporter](#)

Configure Cloud Tool Exporter

To configure Cloud Tool Export settings in AMX:

1. On the AMX quick view in the **Cloud Tool Exports** section, enter or select the required details as described in [Cloud Tool Exporter - Field References](#).
2. Click **Save**.

Deploy the Monitoring Session

1. Click **Deploy** from the **Actions** menu.

2. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the GigaVUE V Series Node for which you wish to map the interfaces and deploy the Monitoring Session.
3. Select the interfaces for the ingress and egress REPs configured in the Monitoring Session. The interface naming includes the type and IP address of the interface, for example, DATA (ens192) IPv4: 10.114.42.135 IPv6: fcab:0:1:2040:a0a1:874e:7a66:40a2.
4. Select **Deploy**. Once deployed, the status is displayed as **Success** in the Monitoring Sessions **Sources** tab. The session is successfully deployed on the selected V Series Node.

Cloud Tool Exporter - Field References

Fields	Description
Alias	Enter the alias name for the cloud tool export.
Endpoint	Enter the endpoint URL where the cloud tool instance is installed and the ports are configured. Enable Secure Endpoint option to hide the API keys from the URL. Example: • Normal Endpoint: http://examples.com/mykey/key123 • Masked Endpoint: http://examples.com/mykey/****
Headers	Enter the custom header value of the cloud tool instance. Example: Add Content-Type: application/json in a separate header field. Ensure that the Secure Keys option is enabled.
Type	Select any one of the following: AMI - Select this option to export AMI or identity enrichment metadata Mobility Control - Select this option to export control plane metadata. AMI Enriched - Select this option to export enriched metadata for cloud workloads and identity enrichment using ZPA. NetFlow/IPFIX - Select this option to transform NetFlow/IPFIX records to JSON format.
Labels	Click Add. Enter the following details: - o Enter the Key. - o Enter the Value. Note: Refer to the deployment guides of the respective cloud tools for configuring the Key and Value.
Advanced Settings	
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Zip	Enable the box to compress the output file. Note: Enable this field when using New Relic as the cloud tool.
Interval (sec)	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 90 seconds.
Parallel Writer	Specifies the number of simultaneous JSON exports done.

Fields	Description
Max Entries	The number of JSON entries in a file. The valid range is 5000–20000 and the default value is 5000.
Request Timeout	This is the time exporter waits for a response back from the tool. The default value is 10 seconds.
Source IP Address	Source IP Address is needed when the egress interface is configured with multiple IP addresses. Configure the source IP address which is connected to the Cloud Tool. Both IPv4 and IPv6 are supported. This field is optional.

Configure Kafka Exporter

To configure Kafka Export settings in AMX:

1. On the AMX quick view in the **Kafka Exports** section, enter or select the required details as described in [Kafka Exporter - Field References](#).
2. Click **Save**.

Deploy the Monitoring Session

1. Click **Deploy** from the **Actions** menu.
2. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the GigaVUE V Series Node for which you wish to map the interfaces and deploy the Monitoring Session.
3. Select the interfaces for the ingress and egress REPs configured in the Monitoring Session. The interface naming includes the type and IP address of the interface for example, DATA (ens192) IPv4: 10.114.42.135 IPv6: fcab:0:1:2040:a0a1:874e:7a66:40a2.
4. Select **Deploy**. Once deployed, the status is displayed as **Success** in the Monitoring Sessions **Sources** tab. The session is successfully deployed on the selected V Series Node.

Kafka Exporter - Field References

Fields	Description
Alias	Enter the alias name for the Kafka Export.
Topic	The topic name to push JSON streams to, which is generally given to users part of the Kafka administration.
Type	Select any one of the following: AMI - Select this option to export AMI or identity enrichment metadata Mobility Control - Select this option to export control plane metadata. AMI Enriched - Select this option to export enriched metadata for cloud workloads and identity enrichment using ZPA. NetFlow/IPFIX - Select this option to export NetFlow/IPFIX ingestor types.
Brokers	The URL that contains the Kafka cluster endpoints. Click  to add another broker and

Fields	Description
	click  to remove an existing broker.
Labels	Click Add . Enter the following details: - o Enter the Key. - o Enter the Value.
Advanced Settings	
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Interval	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 90 seconds. The default time interval is 30 seconds.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Max Entries	The number of JSON entries in a file. The valid range is 5000–20000 and the default value is 5000.
Source IP Address	Source IP Address is needed when the egress interface is configured with multiple IP addresses. Configure the source IP address which is connected to the Kafka Broker. Both IPv4 and IPv6 are supported. This field is optional.
Producer Configurations	Click Add to enter the authentication details if a Kafka broker needs authentication. For Example: • security.protocol=SASL_SSL • sasl.mechanism=PLAIN or sasl.mechanisms=PLAIN • sasl.username=username • sasl.password=password

Verify Your Deployment

You can view the Ingestor, Exporter and Enrichment statistics for the deployed Monitoring Session in the **TRAFFIC PROCESSING** tab. For more details, refer to [View Application Metadata Exporter Statistics](#).

To troubleshoot any issues in Application Metadata Exporter deployment, refer to [Troubleshoot Application Metadata Exporter Deployment](#).

Deploy Application Metadata Exporter in VMware ESXi using FM Orchestration

This section outlines the work flow for deploying Application Metadata Exporter application on VMware ESXi platform using GigaVUE-FM Orchestration.

Predeployment Checklist:

1. Ensure the virtual or cloud environment meets the required resources: 8 vCPUs, 16 GB memory, and 80 GB disk space. Right size the V Series based on the expected flow volume and coordinate with the server team for resource allocation. [Contact Gigamon Support](#) for sizing guidance, if needed.

Exporting JSON records involves file read/write operations; using SSD storage is recommended.

2. AMX requires three interfaces—management, data, and tool which the server team must allocate, preferably as dedicated physical interfaces. GigaVUE-FM, configure a Management Port Group for connectivity with GigaVUE-FM, a Data Port Group to receive traffic from the H Series node, and a Tool Port Group to forward traffic to the tools.

Note: Preparing a network topology with the IP layout helps in configuration, monitoring, and troubleshooting.

3. If static IP addressing is used, obtain the following details from the server team:
 - IP addresses for the management, data, and tool interfaces.
 - IP address of the DNS server and the gateway connected to the tool interface.
4. Create the required Port Groups (ESXi) or Subnets (Nutanix, AWS, Azure) for assigning the data and tool ports for AMX. Coordinate with the server team to complete this configuration.
5. Verify whether remote web console access to the V Series is available. If not, request the server team to enable SSH access. Console access is required for configuring netplan when static IP addressing is used and for troubleshooting issues, if necessary.
6. Review the connectivity requirements for GigaVUE-FM, AMI, AMX, and the associated tools in your environment. Ensure that the required ports are open and any external connectivity dependencies are addressed.
7. Review the deployment guide for the tool specific configuration needed to export records from AMX.
8. Ensure you have selected the appropriate deployment mode for the GigaVUE V Series node based on your requirements:
 - Single uplink for Management, Data and Tool connectivity.
 - Single uplink for Management and Tool connectivity, and another uplink for Data connectivity.
 - (Recommended) Separate uplinks (three) for Management, Data, and Tool connectivity.
9. Create unique virtual switches for each port group.
10. Ensure you have a valid SecureVUE Plus VBL license.

11. Ensure that the VMware ESXi host for GigaVUE-FM meets the hardware requirements: one or more 64-bit x86 CPUs with virtualization assist enabled, at least 16 GB RAM, and at least 84 GB disk space (40 GB system, 4 GB swap, and 40 GB data).
12. Ensure that the standalone GigaVUE-FM deployment meets the recommended requirements shown in the following table. For medium and large scale deployments, refer to [Recommended Requirements for GigaVUE-FM Deployments](#).

Requirements	Small Scale Deployment
CPU	
CPU count(minimum)	2
CPU Min speed (per CPU)	2.30GHz
Memory	
Memory Size	16GB
Disk Space	
OS Disk Size (min)	40GB
Config Disk Size - 15 Days Data	80GB
Config Disk Size - 35 Days Data	160GB
Config Disk Size - Rollup 35 Days + 120 Days Rollup	200GB
NIC	1
Number of NICs	1GB
Management/Data	
Appliance Scalability	Up to 50
Number of GigaVUE HC Series/GigaVUE TA Series Devices	Up to 50
Number of GigaVUE V Series Nodes	1 Cluster with 100 Nodes and 10000 pods with 2 rules
Number of Worker Pods monitored	

Refer to the following topics to deploy AMX using GigaVUE-FM Orchestration:

- [Install GigaVUE-FM using ISO Image File on VMware ESXi](#)
- [Upload GigaVUE V Series Node Image into GigaVUE-FM](#)
- [\(Optional\) Configure Metadata Export Filter for AMX](#)
- [\(Optional\) Integrate Private CA](#)
- [Create Monitoring Domain to Acquire Traffic from Customer Orchestrated Source](#)
- [Deploy Application Metadata Exporter in VMware ESXi using FM Orchestration](#)
- [Create a Monitoring Session to Configure Application Metadata Exporter](#)
- [Configure Ingestor in AMX to Process Traffic](#)
- [Integrate AMX with Third Party Tool](#)

- [Configure Exporter to Export Attributes to Third Party tools](#)
- [Verify Your Deployment](#)

Install GigaVUE-FM using ISO Image File on VMware ESXi

You can install GigaVUE-FM on VMware ESXi host using the ISO image file.

Prerequisites

- Download the GigaVUE-FM ISO image file from the Software and Release Notes page on the [VUE Gigamon Community portal](#) to your local.
- Ensure you have an ESXi host environment that meets CPU, memory, and storage requirements.

Installation Steps

Follow the steps given below to install GigaVUE-FM using ISO image on ESXi host:

1. Log in to the VMware ESXi host web interface.
2. In the ESXi Host Client, go to **Storage > Datastore browser** for a datastore that is accessible to the host.
3. Click **Upload** and select the GigaVUE-FM ISO image from your local system to a suitable folder on the datastore.
4. After uploading the ISO image file, go to the **Virtual Machines** and select **Create/Register VM**. The New Virtual Machine wizard appears.
5. In the **Select creation type** page, select **Create a new virtual machine** and click **Next**.
6. In the **Select a name and guest OS** page,
 - a. Enter a name for the virtual machine.
 - b. Select the **Guest OS family** as Linux.
 - c. Select the **Guest OS version** as Other Linux (64-bit).
 - d. Click **Next**.
7. In the **Select storage** page, choose the datastore where the VM files will reside and click **Next**.

8. In the **Customize settings** page,
 - a. On the **Virtual Hardware** tab, enter the following details:
 - CPU: 2
 - Memory: 16GB
 - Hard disk 1: 40GB
 - Click **Add hard disk** to add two more disks with 4GB and 40GB.

NOTE: Increase the disk space depending upon the configuration load requirements for the given GigaVUE-FM instance.

- b. In the **CD/DVD Drive**, select **Datastore ISO file**. The Datastore browser appears.
 - c. Select the ISO image uploaded in Step 3.

NOTE: By default, the **Connect** checkbox for both **Network Adapter** and **CD/DVD Drive** is enabled.

- d. On the **VM Option** tab, expand **Boot Options**, and under Firmware, select **EFI**.
 - e. Click **Next**.

NOTE: If you leave the firmware as BIOS, GigaVUE-FM attempts to boot in BIOS mode, and the boot process fails .

9. Review all settings on the **Ready to complete** page and click **Finish** to create the virtual machine.
10. Select the newly created VM and click **Power on**.
11. Open the VM console to monitor the boot process. It may take approximately 15–20 minutes for the VM to boot.

Access GigaVUE-FM

1. Log into GigaVUE-FM using the IP address available on the ESXi web interface.
2. Use the default credentials: In the VM console, enter the default credentials:
 - Username: admin
 - Password: admin123A!!
3. On first login, you will be asked to change the password. Enter the current password (admin123A!!), then set and confirm a new one.
4. Accessing the Shell Bash in GigaVUE-FM: After the password is successfully changed, no reboot is required. You are logged in to the fmctl command prompt instead of a standard bash shell. If you need to run other Linux commands, you can switch to the (admin) bash shell by running the **shell** command in the fmctl command prompt. For the list of fmctl commands, refer to [GigaVUE-FM CLI Commands](#).

Upload GigaVUE V Series Node Image into GigaVUE-FM

This step is optional. You can upload the GigaVUE V Series Node image to GigaVUE-FM even while deploying the GigaVUE V Series Node.

To upload the V Series image into GigaVUE-FM,

1. Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, and select **Settings > OVA Files**.
2. In the **OVA Files** page, select **Browse**, and then select the image file. For example, *gigamon-gigavue-vseries-node-x.x.x-0-xxxxxx.ova*. You can upload three OVA files to GigaVUE-FM for VMware vCenter.
3. Select **Upload to Server**. You have uploaded the OVA image file to the GigaVUE-FM server.

(Optional) Configure Metadata Export Filter for AMX

Optionally, you can configure an export filter to control which metadata records are exported from AMX. For more information, see [Configure Metadata Export Filter](#).

(Optional) Integrate Private CA

You can integrate your own PKI infrastructure with GigaVUE-FM.

Rules and Notes

- Always place the root CA in a separate file.
- When using multiple intermediate CAs, consider the following:
 - Include all intermediate CAs in a single file in the correct order.
 - Place the last intermediate CA in the chain at the top.
 - Place the preceding CAs in descending order.

To integrate private CA

- Generate a Certificate Signing Request (CSR).
- Get a signature of the Certificate Authority (CA) on the CSR.
- Upload CA Certificate to GigaVUE-FM.

Generate CSR

To create an intermediate CA certificate:

1. Go to  > **System > Certificates**.
2. In the top navigation bar, from the **PKI** drop-down list, select **CSR**. The **Generate Intermediate CA Certificate** page appears.
3. Enter details in the following fields:
 - **Country:** Enter the name of your country.
 - **Organization:** Enter the name of your organization.
 - **Organization Unit:** Enter the name of the department or unit.
 - **Common Name:** Enter the common name associated with the certificate.
4. From the **Algorithm** drop-down list, select the desired encryption algorithm used to encrypt your private key.
5. Select **Generate CSR**.

The CSR is downloaded successfully.

Upload CA Certificate

Get the CSR signed from your Enterprise PKI or any public PKI and upload the signed intermediate CA certificate to GigaVUE-FM.

To upload the signed CA certificate to GigaVUE-FM:

1. Go to  > **System > Certificates**.
2. In the top navigation bar, from the **PKI** drop-down list, select **CA**. The **CA Certificate** page appears.
3. From the **Actions** drop-down list, select **Upload CA**. The **Upload CA** pop-up appears.
4. Next to **Intermediate CA**, select **Choose File** to upload the signed intermediate CA certificate.
5. Next to **Root CA**, select **Choose File** to upload the corresponding root or intermediate CA.

The **CA Certificate** page displays the uploaded CA certificate.

Create Monitoring Domain to Acquire Traffic from Customer Orchestrated Source

To create a Monitoring Domain in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, and select **Monitoring Domain**. The **Create Monitoring Domain Configuration** page appears.
2. On the **Monitoring Domain** page, select **New**. The **VMware Configuration page** appears.
3. Enter the following fields:

- a. **Monitoring Domain** - Enter a name for the monitoring domain.
 - b. **Connection** - Enter a name for the connection.
 - c. **Virtual Center** - Enter the IP address or FQDN of the vCenter
 - d. **Username** - Enter the username of the vCenter user.
 - e. **Password** - Enter the password to connect to the vCenter.
4. Select the Traffic Acquisition Method as Customer Orchestrated Source.
 5. Click **Save**. Once you save the changes, the **Virtual Fabric Launch Configuration** page appears. The configuration details are explained in the following section.

Deploy V Series Node

This section provides step-by-step instructions on how to deploy GigaVUE V Series Nodes in VMware vCenter Monitoring Domain.

To deploy GigaVUE V SeriesNodes using GigaVUE-FM, follow these steps:

1. Go to the **VMware Fabric Launch Configuration** page using one of the following options:
 - **Automatic Option:** Create a monitoring domain, and the page opens automatically.
 - **Manual Option:** Open **VMware Fabric Launch Configuration** page from the **Monitoring Domain** page.
 - a. To launch the **VMware Fabric Launch Configuration** from the Monitoring Domain, go to **Inventory > VIRTUAL > VMware vCenter (V Series)**.
 - b. Select **Actions > Deploy Fabric**.

The **VMware Fabric Launch Configuration** page appears.

VMware vCenterESXi Fabric LaunchMonitoring DomainSettings

VMware Fabric Launch ConfigurationDeployCancel

Datacenter*DataCenter

Cluster*Cluster-2_Scaled

V Series Node Image*gigamon-gigavue-vseries-node-6.13.0...Add

Form Factor*Large, 8vCPU, 16GB RAM, 80GB Disk

Enable Custom Certificates

Select AllSelect None

10.115.81.126

Common Configuration

10.115.81.126

VSeries.10.115.81.126-1

☒ Datastores☐ Datastore Clusters

Datastore*datastore1 (2)

Name Server ⓘUse Comma to Separate

V Series Node Name*VSeries.10.115.81.126-1

Management

Interface NameNetwork adapter 1

Network*VM Network

IP TypeStatic

IP Address*10.115.85.38

Gateway IP*10.115.80.1

CIDR Prefix* ⓘ21

MTUEnter MTU Value

Data interfaces

Interface NameNetwork adapter 2

Network*DPortGroup_tunnel

IP TypeStatic

IP Address*172.21.1.220

Application Metadata Exporter

99

2. On the **VMware Fabric Launch Configuration** page, enter or select the following details:

Field	Description	
Datacenter	Select the vCenter datacenter with the ESXi hosts to be provisioned with GigaVUE V Series Nodes.	
Cluster	Select the cluster where you want to deploy the GigaVUE V Series Nodes.	
V Series Node Image	Select the OVA file uploaded in the Upload GigaVUE V Series Node Image into GigaVUE-FM , from the dropdown list.	
Form Factor	Select Large, 8vCPU, 16GB RAM, 80GB Disk option.	
Enable Custom Certificates	Enable this option to validate the custom certificate during SSL Communication. GigaVUE-FM validates the Custom certificate with the trust store. If the certificate is unavailable in Trust Store, communication does not happen, and a handshake error occurs. Note: If the certificate expires after the successful deployment of the fabric components, then the fabric components move to failed state.	
Certificate Note: This field appears only when Enable Custom Certificates option is enabled.	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes. For more information, refer to Secure Communication between GigaVUE Fabric Components .	
Hosts	Select the ESXi hosts for GigaVUE V Series Node deployment. The Common Configuration dropdown wizard and the specific host dropdown wizard appears. Expand the individual host and configure the GigaVUE V Series Node.	
	ESXi Host	
	Datastore	Network datastore shared among all ESXi hosts.
	Name Server	The server that stores the mapping between the domain names and the IP addresses. The maximum number of name servers that can be entered is three. Enter valid IPv4 addresses, separated by a comma.
	V Series Node Name	Enter a name for the GigaVUE V SeriesNode.
	Management	
	Network	Management network for GigaVUE V Series Nodes.
	IP Type	Select the management network IP type as Static or DHCP.
	IP Address	Enter the IP address of the management port.
	Gateway IP Note: This field	Gateway IP address of the management network.

Field	Description	
	appears only when the Management IP type is Static.	
	CIDR Prefix Note: This field appears only when you select the IP Type as Static.	Enter the CIDR prefix of the IP address.
	MTU (Optional)	The Maximum Transmission Unit (MTU) is the maximum size of each packet that can be transferred as a single entity in a network connection. Enter value between 1280 to 9000.
	Data Interfaces - When using Customer Orchestrated Source as the Traffic Acquisition Method, you must configure two data interfaces, one for data port and other for tool port.	
	Interface 1	
	Network	Tunnel Network for the GigaVUE V Series Nodes.
	IP Type	Select the tunnel network IP address type as Static or DHCP.
	IP Address	Enter the IP address of the data port.
	Gateway IP	Gateway IP address of the tunnel network.
	CIDR Prefix Note: This field appears only when you select the IP Type as Static.	Enter the CIDR prefix of the IP address.
	MTU (Optional)	The Maximum Transmission Unit (MTU) is the maximum size of each packet that can be transferred as a single entity in a network connection. Enter value between 1280 to 9000.
	Use IPv6 Note: This field appears only when Customer Orchestrated Source as the Traffic Acquisition Method.	Enable this option to use IPv6 address.

Field	Description	
	Interface 2	
	Network	Tunnel Network for the GigaVUE V Series Nodes.
	IP Type	Select the tunnel network IP address type as Static or DHCP.
	IP Address	Enter the IP address of the tool port.
	Gateway IP	Gateway IP address of the tool network.
	CIDR Prefix	Enter the CIDR prefix of the IP address.
	Note: This field appears only when you select the IP Type as Static.	
	MTU (Optional)	The Maximum Transmission Unit (MTU) is the maximum size of each packet that can be transferred as a single entity in a network connection. Enter value between 1280 to 9000.
	Use IPv6	Enable this option to use IPv6 address.
	Note: This field appears only when Customer Orchestrated Source as the Traffic Acquisition Method.	
	Virtual Disk Format	Select the Virtual Disk Format from the dropdown list.
	Deployment Folder	Enter the folder name in vCenter, under which the GigaVUE V SeriesNodes must be deployed.
	Password	Enter the password you wish to use for the GigaVUE V Series Node.

3. Select **Deploy**. After deployment in vCenter, it appears on the **Monitoring Domain** page under the Monitoring Domain, where the GigaVUE V Series Node is deployed.

NOTE: GigaVUE-FM can process a maximum of ten GigaVUE V Series Nodes deployment requests in parallel on VMware vCenter. Each deployment request can have multiple GigaVUE V Series Nodes for deployment.

Create a Monitoring Session to Configure Application Metadata Exporter

In GigaVUE-FM, you must do the following to configure the Application Metadata Exporter application in the Monitoring Session.

1. **Access the Monitoring Session Page:**

- a. In GigaVUE-FM, go to **Traffic > Virtual > Orchestrated Flows > VMware ESXi**.
- b. After creating a new Monitoring Session or on an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab. The GigaVUE-FM Monitoring Session canvas page appears.

2. **Create an ingress REP:**

- a. In the canvas, from the New expand menu, drag and drop New Raw Endpoint to the graphical workspace.
- b. On the new raw endpoint icon, select the  menu button and select **Details**. The **Raw** quick view page appears.
- c. Enter the Alias and Description details for the Ingress Raw End Point and click **Save**.

3. **Add AMX Application:**

- a. In the canvas, from the **Applications** expand menu, drag and drop AMX to the graphical workspace.
- b. Configure the ingestor settings to process traffic. Refer to [Configure Ingestor in AMX to Process Traffic](#) for details.
- c. Configure the required exporter settings to export attributes to Third Party tools. Refer to [Configure Exporter to Export Attributes to Third Party tools](#) for details.
- d. Create a link between the ingress REP and Application Metadata Exporter application.

4. **Create an egress REP:**

- a. From the **New** expand menu, drag and drop New Raw Endpoint to the graphical workspace.
- b. On the new raw endpoint icon, select the  menu button and select **Details**. The **Raw** quick view page appears.
- c. Enter the Alias and Description details for the Egress Raw End Point and click **Save**.
- d. Create a link between the Application Metadata Exporter application and egress REP

**Notes:**

- Ensure to create separate Monitoring Domains and Monitoring Sessions for Application Metadata Exporter (AMX) and Application Metadata Intelligence (AMI). Even when AMI is deployed virtually, it operates independently and requires its own Monitoring Session.
- When deploying AMX using the Third-Party Orchestration method, Monitoring Session must also be configured in the same work flow.

Configure Ingestor in AMX to Process Traffic

The following scenarios provide more information about the different ways to configure Ingestor AMX:

- [Scenario 1 - Export Application Metadata in JSON format over HTTPS/Kafka](#)
- [Scenario 2 - Export GigaVUE Enriched Metadata for Cloud Workloads and Export over HTTPS/Kafka](#)
- [Scenario 3 - Transform NetFlow/IPFIX records to JSON format and export over HTTPS/Kafka](#)
- [Scenario 4 - Transform NetFlow/IPFIX records to JSON format and export over HTTPS/Kafka](#)
- [Scenario 2 - Export GigaVUE Enriched Metadata for Cloud Workloads and Export over HTTPS/Kafka](#)

Scenario 1 - Export Application Metadata in JSON format over HTTPS/Kafka

To configure ingestor for AMI:

1. On the AMX quick view in the **Ingestor** section, enter an alias name for the ingestor.
2. In the **Type** field, select **AMI** as the input type.
3. Enter the port number on which Application Metadata must be ingested. The default port value is 514.
4. Click  to add another ingestor to add multiple inputs to the AMX application and click  to remove an existing ingestor.

Scenario 2 - Export GigaVUE Enriched Metadata for Cloud Workloads and Export over HTTPS/Kafka

To export GigaVUE Enriched Metadata for Cloud Workloads:

1. On the AMX quick view in the **Ingestor** section, enter an alias name for the ingestor.
2. In the Type field, select **AMI** as the input type.

3. Enter the port number on which Application Metadata must be ingested. The default port value is 514.
4. Click  to add another ingestor.
5. In the Type field, select **Mobility Control Plane** as the input type.
6. Enter the port number on which Application Metadata must be ingested.
7. Click  again to add another ingestor to add multiple inputs to the AMX application and click  to remove an existing ingestor.
8. In the **Metadata Enrichment** section, enter a unique name for the enrichment.
9. Select the Enable option to enable the enrichment.
10. Select **Workload** from the **Type** drop down menu.
11. Select the platform as **VMware VCenter** from the drop down list.
12. Select the required attributes from the list. You can use **Select All** to choose all available attributes. Refer to the [Attributes for GigaVUE Enriched Metadata for Cloud Workloads](#) for more details.

Scenario 3 - Transform NetFlow/IPFIX records to JSON format and export over HTTPS/Kafka

To configure ingestor for NetFlow/IPFIX:

1. On the AMX quick view in the **Ingestor** section, enter an alias name for the ingestor.
2. In the Type field, select the input type as **NetFlow/IPFIX**. Only the elements specified in the mapping file will be included in the JSON output. Editing or customizing the mapping file is not supported. Refer to [Supported Element Types for NetFlow Integrator Element Mapping](#).
3. Enter the port number on which NetFlow/IPFIX must be ingested. The default port value is 2055.
4. Click  to add another ingestor to add multiple inputs to the AMX application and click  to remove an existing ingestor. A maximum of 12 NetFlow/IPFIX type ingestors can be configured per deployment.

NOTE: If you select NetFlow/IPFIX as the ingestor type, Metadata Enrichment is disabled by default. Metadata Enrichment is not supported for NetFlow/IPFIX inputs.

Scenario 4 - Transform NetFlow/IPFIX records to JSON format and export over HTTPS/Kafka

Refer to [Application Metadata Exporter - Export Scenarios](#) topic for more details and conceptual information.

To configure ingestor for NetFlow/IPFIX:

1. On the AMX quick view in the **Ingestor** section, enter an alias name for the ingestor.
2. In the Type field, select the input type as **NetFlow/IPFIX**. Only the elements specified in the mapping file will be included in the JSON output. Editing or customizing the mapping file is not supported. Refer to [Supported Element Types for NetFlow Integrator Element Mapping](#).
3. Enter the port number on which NetFlow/IPFIX must be ingested. The default port value is 2055.
4. Click  to add another ingestor to add multiple inputs to the AMX application and click  to remove an existing ingestor. A maximum of 12 NetFlow/IPFIX type ingestors can be configured per deployment.

NOTE: If you select NetFlow/IPFIX as the ingestor type, Metadata Enrichment is disabled by default. Metadata Enrichment is not supported for NetFlow/IPFIX inputs.

Scenario 5 - Configure Identity Enrichment Metadata using Zscaler Private Access (ZPA)

Refer to [Application Metadata Exporter - Export Scenarios](#) topic for more details and conceptual information.

Prerequisites

Before configuring identity enrichment using Zscaler Private Access (ZPA), ensure that the following prerequisites are met.

Zscaler Infrastructure

The following Zscaler components must already be set up in your environment. These are standard ZPA deployment requirements. For detailed instructions, refer to the Zscaler documentation.

- **Acquire Zscaler Tenant Access:** Ensure that you have admin access to the Zscaler Private Access admin portal (ZPA tenant). Refer to [Zscaler Tenant Access](#) for more information.

- **Integrate Identity Provider (IdP):** An IdP (such as Okta, Microsoft Azure AD, or any supported IdP) must be configured and integrated with ZPA. ZPA uses the IdP to authenticate users before granting access to private applications. Refer to [About External Identity Providers](#) for more information.
- **Configure App Connector Group :** At least one App Connector group must be created and have active App Connectors registered to it. You can use an existing App Connector group or create a new one before proceeding. For instructions, refer to the Zscaler documentation. Refer to [Configuring App Connector Groups](#) for more information.
- **Install App Connector:** The Zscaler App Connector package must be downloaded and installed on a Linux-based VM (Ubuntu, plain Linux, or similar) in the domain where your private applications reside. Refer to the scaler App Connector deployment guide for platform-specific instructions (Linux, Docker, GCP, Kubernetes, and so on). Refer to [App Connectors](#) for more information.
- **Define Private Applications:** Application segments must be created for all private applications you want to monitor (for example, internal web apps, Jira, databases). Each application segment must include the application IP address and port range, and must be linked to a server group and an App Connector group. Refer to [Configuring Defined Application Segments](#) for more information.

Gigamon Infrastructure

- **Deploy VSN Node with AMX on ESXi:** The Application Metadata Exporter (AMX) must be deployed on a V Series Node (VSN). In this release, only the ESXi platform is supported. The IP address of the VSN node on which AMX is running, as it is required when configuring the ZPA Log Receiver. Refer to [Deploy Application Metadata Exporter in VMware ESXi using FM Orchestration](#) for more information.
- **Configure AMI:** Application Metadata Intelligence (AMI) must be active and generating flow records. The AMI metadata (source IP, destination IP, source port, destination port) is used to match and enrich flows with ZPA log data. For more information on configuring AMI, refer to [Configure Application Metadata Intelligence for Virtual Environment](#).

Integrate ZPA with Gigamon AMX

After the Zscaler infrastructure and Gigamon infrastructure are set up, configure a Log Receiver in the ZPA admin portal to stream ZPA logs to AMX. This is the key step that establishes the integration between ZPA and Gigamon.

The following table lists the specific options you must select when configuring a log receiver to integrate with AMX. For navigation steps and detailed instructions, refer to [Configuring Log Receiver](#) topic in Zscaler documentation.

Parameters	Description
Log Receiver	
Name	Enter a name for the log receiver.
Domain or IP Address	Enter the domain or IP address to the IP address of the VSN node on which AMX is deployed (not the ESXi host IP address).
TCP Port	Enter the port configured as the ZPA LSS ingestor port on AMX.
App Connector Groups	Select an app connector group that was created.
Log Stream	
Log Type	Select User Activity as the log type.
Log Template	Select JSON template.
Log Stream Content	Add the following new user activity log in the content: "ConnectionSetupTime": %{ConnectionSetupTime} }\n

Configure Ingestor for AMX

You can configure metadata enrichment for ZPA only. Optionally, you can combine it with GEM for Cloud Workloads for VMware vCenter.

To export identity enrichment metadata using ZPA :

1. Configure an ingestor for AMI
 - a. On the AMX quick view in the **Ingestor** section, enter an alias name for the ingestor.
 - b. In the **Type** field, select **AMI** as the input type.
 - c. Enter the port number on which application metadata must be ingested. The default port value is 514.
 - d. Click  to add another ingestor to add multiple inputs to the AMX application and click  to remove an existing ingestor.
2. Configure identity metadata enrichment using ZPA
 - a. On the AMX quick view in the **Metadata Enrichment** section, enter an alias for the enrichment.
 - b. Select the Enable option to enable the enrichment.
 - c. In the **Type** field, select **Identity** as the input type.
 - d. Select **Zscaler Private Access** from the **Platform** dropdown list.
 - e. Select the attributes for identity enrichment from the **Attributes** tab.
 - f. In the **Source Information** tab, enter the port number on which AMX receives the ZPA LSS logs.

- g. (Click  to add another ZPA source information to add multiple inputs to the AMX application and click  to remove an existing source information.
3. (Optional) Configure GigaVUE Enriched Metadata workload for ESXi
- On the AMX quick view in the **Metadata Enrichment** section, enter an alias for the enrichment.
 - Select the Enable option to enable the enrichment.
 - In the **Type** field, select **Workload** as the input type.
 - Select **VMware vCenter** from the **Platform** dropdown list.
- NOTE:** Only VMware vcenter platform is applicable as additional workload along with ZPA.
- Select the required workload attributes for ESXi.
 - In the Source Information tab, enter the Key-Value pair details as given:
 - Key - url and Value - Primary URL for the vCenter Server SDK. For example, https://<vCenter-IP-or-FQDN>/sdk.
 - Key - username and Value - VMware vCenter username.
 - Key - password and Value - vCenter password.
- g. Click  to add another ESXi source information to add multiple inputs to the AMX application and click  to remove an existing source information.

Integrate AMX with Third Party Tool

This section explains how to set up the third-party tool and configure the exporter settings required to route application metadata attributes for analysis and visualization.

Set up the Third Party Tool for AMX Integration

You must set up the third party tools to ingest and visualize application metadata.

Refer to [AMX Tool Integration](#) for configuration guidance and the verification steps required to confirm that data export and visualization are functioning correctly.

Configure Exporter to Export Attributes to Third Party tools

AMX supports the following types of exporters:

- [Configure Cloud Tool Exporter](#)

- [Configure Kafka Exporter](#)

Configure Cloud Tool Exporter

To configure Cloud Tool Export settings in AMX:

1. On the AMX quick view in the **Cloud Tool Exports** section, enter or select the required details as described in [Cloud Tool Exporter - Field References](#).
2. Click **Save**.

Deploy the Monitoring Session

1. Click **Deploy** from the **Actions** menu.
2. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the GigaVUE V Series Node for which you wish to map the interfaces and deploy the Monitoring Session.
3. Select the interfaces for the ingress and egress REPs configured in the Monitoring Session.
4. Select **Deploy**. Once deployed, the status is displayed as **Success** in the Monitoring Sessions **Sources** tab. The session is successfully deployed on the selected V Series Node.

Cloud Tool Exporter - Field References

Fields	Description
Alias	Enter the alias name for the cloud tool export.
Endpoint	Enter the endpoint URL where the cloud tool instance is installed and the ports are configured. Enable Secure Endpoint option to hide the API keys from the URL. Example: • Normal Endpoint: http://examples.com/mykey/key123 • Masked Endpoint: http://examples.com/mykey/****
Headers	Enter the custom header value of the cloud tool instance. Example: Add Content-Type: application/json in a separate header field. Ensure that the Secure Keys option is enabled.
Type	Select any one of the following: AMI - Select this option to export AMI. Mobility Control- Select this option to export control plane metadata. AMI Enriched - Select this option to export enriched metadata for cloud workloads and identity enrichment using ZPA. NetFlow/IPFIX - Select this option to transform NetFlow/IPFIX records to JSON format.
Labels	Click Add. Enter the following details: - o Enter the Key. - o Enter the Value.

Fields	Description
	Note: Refer to the deployment guides of the respective cloud tools for configuring the Key and Value.
Advanced Settings	
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Zip	Enable the box to compress the output file. Note: Enable this field when using New Relic as the cloud tool.
Interval (sec)	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 90 seconds.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Max Entries	The number of JSON entries in a file. The valid range is 5000–20000 and the default value is 5000.
Request Timeout	This is the time exporter waits for a response back from the tool. The default value is 10 seconds.
Source IP Address	Source IP Address is needed when the egress interface is configured with multiple IP addresses. Configure the source IP address which is connected to the Cloud Tool. Both IPv4 and IPv6 are supported. This field is optional.

Configure Kafka Exporter

To configure Kafka Export settings in AMX:

1. On the AMX quick view in the **Kafka Exports** section, enter or select the required details as described in [Kafka Exporter - Field References](#).
2. Click **Save**.

Deploy the Monitoring Session

1. Click **Deploy** from the **Actions** menu.
2. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the GigaVUE V Series Node for which you wish to map the interfaces and deploy the Monitoring Session.
3. Select the interfaces for the ingress and egress REPs configured in the Monitoring Session.
4. Select **Deploy**. Once deployed, the status is displayed as **Success** in the Monitoring Sessions **Sources** tab. The session is successfully deployed on the selected V Series Node.

Kafka Exporter - Field References

Fields	Description
Alias	Enter the alias name for the Kafka Export.
Topic	The topic name to push JSON streams to, which is generally given to users part of the Kafka administration.
Type	Select any one of the following: AMI - Select this option to export AMI. Mobility Control - Select this option to export control plane metadata. AMI Enriched - Select this option to export enriched metadata. NetFlow/IPFIX - Select this option to export NetFlow/IPFIX ingestor types.
Brokers	The URL that contains the Kafka cluster endpoints. Click  to add another broker and click  to remove an existing broker.
Labels	Click Add . Enter the following details: - o Enter the Key. - o Enter the Value.
Advanced Settings	
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Interval	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 90 seconds. The default time interval is 30 seconds.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Max Entries	The number of JSON entries in a file. The valid range is 5000–20000 and the default value is 5000.
Source IP Address	Source IP Address is needed when the egress interface is configured with multiple IP addresses. Configure the source IP address which is connected to the Kafka Broker. Both IPv4 and IPv6 are supported. This field is optional.
Producer Configurations	Click Add to enter the authentication details if a Kafka broker needs authentication. For Example: • security.protocol=SASL_SSL • sasl.mechanism=PLAIN or sasl.mechanisms=PLAIN • sasl.username=username • sasl.password=password

Verify Your Deployment

You can view the Ingestor, Exporter and Enrichment statistics for the deployed Monitoring Session in the **TRAFFIC PROCESSING** tab. For more details, refer to [View Application Metadata Exporter Statistics](#).

To troubleshoot any issues in Application Metadata Exporter deployment, refer to [Troubleshoot Application Metadata Exporter Deployment](#).

Deploy Application Metadata Exporter (AMX) on KVM Hypervisor

For using the KVM hypervisor on GigaVUE-FM, the following sections provide information on deploying a fresh installation of GigaVUE-FM in the KVM environment. This setup enables the deployment of the Application Metadata Exporter (AMX) on a GigaVUE-FM Hardware Appliance.

Install GigaVUE-FM on KVM hypervisor

Prerequisite:

1. Download the recent GigaVUE-FM image from [Gigamon Customer Portal](#) and move qcow2 file to a desired location.
2. Install and enable Cockpit services on the KVM hypervisor. To enable Cockpit View on the KVM hypervisor, follow these steps:
 - a. Update the system package list.

```
sudo apt update
```

- b. Install Cockpit and Cockpit-Machines.

```
sudo apt install -y cockpit cockpit-machines
```

- c. Enable and start the Cockpit service.

```
sudo systemctl enable --now cockpit.socket
```

Once these commands are executed, access KVM using port 9090 in your browser:
<http://<your-server-IP>:9090>

To create a VM in KVM hypervisor for deploying the GigaVUE-FM, follow the instructions.

Parameters	Instructions	Mandatory field
Connection	Select System .	Yes
Installation Type	Select Cloud base image from the drop-down list.	Yes

Parameters	Instructions	Mandatory field
Installation Source	Select the location of the qcow2 image.	Yes
Operating System	Select the latest Rocky Linux version.	Yes
Storage	Select Create new qcow2 volume .	Yes
Storage Limit	Enter the required storage limit (ex: 40 GiB).	Yes
Memory	Enter the required memory allocation (ex: 16 GiB).	Yes

Click **Create and edit** to edit the Virtual Machine. Modify the **Firmware** to **UEFI** and click **Install**.

Edit the VM as mentioned in the following table.

Parameters	Instructions	Mandatory field
Firmware	Select UEFI from the drop-down list	Yes
Disks		
Add new disk		
Size	Enter the disc size as required (ex: 40 GiB).	Yes
Format	Select the format (ex: qcow2).	Yes
CPU		
vCPU Maximum	Enter the maximum number of vCPU's required (ex: 10).	Yes
vCPU Count	Enter the number of CPUs to allocate (ex: 8).	Yes

NOTE: The values mentioned for CPU, size, format, storage, and memory are sample entries and can be customized as required. Refer to [Before You Install](#) to know more about the hardware and virtual computing requirements for GigaVUE-FM.

Click **Run** to deploy **GigaVUE-FM**. Copy the IP address of the newly launched GigaVUE-FM and paste it on the browser to login to the GigaVUE-FM. You can login to GigaVUE-FM using the default user name **admin** and the default password admin123A!!.

View Application Metadata Exporter Statistics

To view the application Statistics for the Application Metadata Exporter application, follow the steps given below:

1. Go to **Traffic > Virtual > Orchestrated Flows > Third Party Orchestration**. The **Monitoring Sessions** Overview page appears.
2. Select the monitoring session you want to view the statistics.

3. Go to the **TRAFFIC PROCESSING** tab. In the canvas page, click the  menu button on the **AMX** application and select **Details**. The Application quick view appears.
4. Click on **STATISTICS** tab.
5. To view the statistics of a particular GigaVUE V Series Nodes, select the required GigaVUE V Series Node from the **V Series Node IP** dropdown menu to view the **Ingestor**, **Exporter**, and **Attributes Enrichment** statistics.

You can download the Ingestor and Exporter statistics using the following options:

- **Download TCP Dump** (Ingestor)- Select this option to download the PCAP file (for example, cap_ens192_20260407_073719655-run-001.pcap.gz). The TCP dump capture is limited to 100 packets and runs for up to 30 seconds, or until 100 packets are captured (whichever occurs first). You can capture a TCP dump for only one AMX ingestor at a time. The TCP dump download option is available only for the following ingestor types: AMI, NetFlow/IPFIX, Mobility, and Zscaler LSS.
- **Download Records** (Exporter) - Select this option to download the JSON file (for example, Elastic-exporter-records.json.gz) of the exporter records. You can download records for a single AMX exporter or for multiple exporters. The exporter record download waits up to 30 seconds for records to be exported. If no records are produced, the operation times out.

For instructions on how to download the ingestor and exporter records, and troubleshoot AMI/AMX issues, refer to [Troubleshoot AMI/AMX Deployment](#).

For more information on health status of exporters, refer to [View Health Status](#).

You can view the following parameters in the Application Metadata Exporter application statistics page.

Exporter - Statistics to monitor exports from AMX

Parameters	Description
Name	Displays the name of exporters created for this application.
Exported Entries	Displays the number of entries available in the files that will be uploaded from AMX to the cloud tool or the Kafka consumers.
Average File Size	Displays the average size of the file.
File Upload Errors	Displays the number of file uploaded from the AMX to the cloud tool or the Kafka consumers.
File Upload Errors	Displays the number of times the file was not uploaded to the cloud tools or Kafka consumers due to errors.
Re Exported Entries (Only for Kafka Tool Exporter)	Displays the number of records re-exported from the errors directory after the Kafka tool is restored. Errored files are re-exported automatically at a

Parameters	Description
	rate of 10 files per 5 seconds.
Exported Entries Rolling 15 Sec	Displays the rolling average of entries exported per second over the past 15 seconds.
Exported Entries Rolling 30 Sec	Displays the rolling average of entries exported per second over the past 30 seconds.
Exported Entries Rolling 60 Sec	Displays the rolling average of entries exported per second over the past 60 seconds.
Exported MBytes	Total number of megabytes exported.
Exported MBytes Rolling 15 Sec	Rolling average of megabytes exported over the past 15 seconds.
Exported MBytes Rolling 30 Sec	Rolling average of megabytes exported over the past 30 seconds.
Exported MBytes Rolling 60 Sec	Rolling average of megabytes exported over the past 60 seconds.

Ingestor - Statistics to monitor ingestion

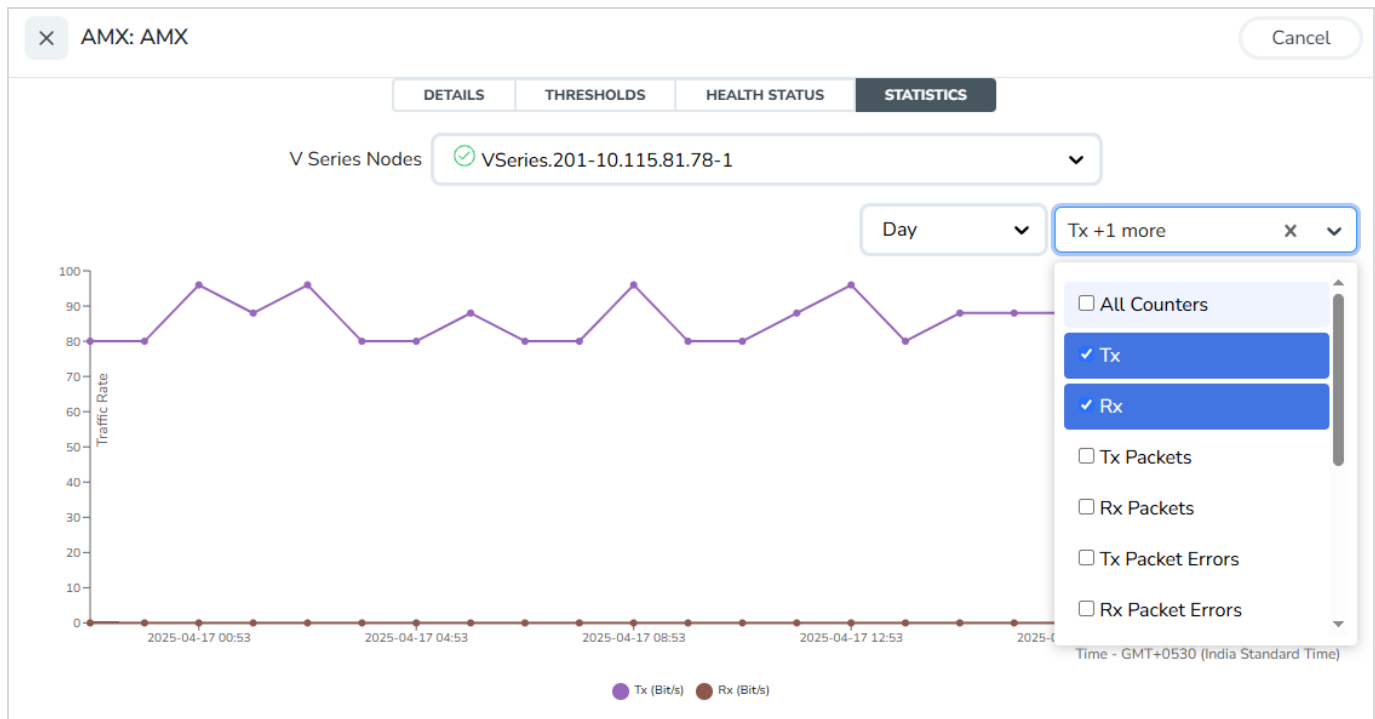
Parameters	Description
Name	Displays the name of the ingestor created for this application.
Packets Received	Displays the packets received from the AMI to AMX ingestor.
Packets Dropped	Displays the packets dropped when the traffic passes from AMI to AMX ingestor.
Octets Received	Displays the octets received from the AMI to AMX ingestor.
Octets Dropped	Displays the octets dropped when the traffic passes from AMI to AMX ingestor.
Records Added	Displays the number of workload information pulled from the workload environment.
Records Dropped	Displays the number of the workload details that were dropped from the workload environment.
Request Success	Displays if the workload information was fetched from the cloud environment. The default interval at which the AMX fetches the workload information is 60 seconds.
Request Authentication Errors	Displays if the workload information was not fetched from the cloud environment due to any authentication errors like wrong password.

Parameters	Description
Request Timedout Errors	Displays if the workload information was not fetched from the cloud environment even after the default interval of 60 seconds.
Request Errors	Displays when the workload information could not be fetched from the cloud environment due to issues other than authentication failures or timeout conditions.
Decode Success	Displays number of successful decoding operations performed by a system when processing NETFLOW/IPFIX packets.
Decode Fail	Displays the number of failed attempts to decode NETFLOW/IPFIX packets.
Elements Skipped	Displays number of data elements that were not processed or were omitted during the NETFLOW/IPFIX ingestion process.
Pkts Rx Rolling 15 Sec	Rolling average of packets received per second over the past 15 seconds.
Pkts Rx Rolling 30 Sec	Rolling average of packets received per second over the past 30 seconds.
Pkts Rx Rolling 60 Sec	Rolling average of packets received per second over the past 60 seconds.
Mbytes Rx	Total number of megabytes ingested.
Mbytes Rx Rolling 15 Sec	Rolling average of total megabytes received over the past 15 seconds.
Mbytes Rx Rolling 30 Sec	Rolling average of total megabytes received over the past 30 seconds.
Mbytes Rx Rolling 60 Sec	Rolling average of total megabytes received over the past 60 seconds.

Attributes Enrichment - Statistics to monitor enrichment

Parameters	Description
Name	Displays the name of the Metadata enrichment.
One Min Percent	Displays the percentage of the traffic that is enriched from the last 1 minute.
Five Min Percent	Displays the percentage of the traffic that is being enriched from the last 5 minutes.
Ten Min Percent	Displays the percentage of the traffic that is being enriched from the last 10 minutes.

The following image shows the statistical details for general AMX application.



Attributes for GigaVUE Enriched Metadata for Mobile Networks

This section describes the various attributes available within GigaVUE Enriched Metadata for Mobile Networks.

Each flow will generate only one record per export interval; however, in this section, the attributes are separated into the following categories:

- [Control Plane Attributes](#)
- [User Plane Attributes](#)

For device centric use cases			For cell tower centric use cases			For app centric use cases			
imsi/supi	imei/pei	msisdn/gpsi	apn/dnn	mcc & mnc	ecgi_cellid	app_name	up_bytes	down_bytes	...
3102271700732	3565447644601	14155552345	cal.mobile.net	291, 292	2344_343	youtube	3455	4566778	...
For subscriber centric use cases			For network(roamers) centric use cases			For data volume use cases			

Control Plane Attributes

The control plane attributes are generated based on network signaling message transactions with successful responses. These include signaling transactions for session establishment, modification, deletion, and others. These attributes are used for enriching the user plane metadata with the corresponding control plane subscriber, device, and location information.

Attribute	Description
imsi	International Mobile Subscriber Identity. A 3GPP-defined unique private identifier for a mobile user on a 4G network.
imei	International Mobile Equipment Identity. A 3GPP-defined unique identifier for a mobile device on a 4G network.
msisdh	Mobile Station Integrated Services Digital Network. A 3GPP-defined identifier for a mobile device on a 4G network.
supi	Subscription Permanent Identifier. A 3GPP-defined unique identifier for a mobile user on a 5G network.
gpsi	Generic Public Subscription Identifier. A 3GPP-defined public identifier for a mobile user on a 5G network.
pei	Permanent Equipment identifier. A 3GPP-defined unique identifier for a mobile device on a 5G network.
ctrl_tun_access_ipv4_addr	Control Plane Access Tunnel IPv4 Address. MME identifier for S11, SGW identifier for S5/S8-C, AMF identifier for N11 and SGSN for Gn, GP
ctrl_tun_access_ipv6_addr	Control Plane Access Tunnel IPv6 Address. MME identifier for S11, SGW identifier for S5/S8-C, AMF identifier for N11 and SGSN for Gn, GP
ctrl_tun_access_teid	Control Plane Access Tunnel Endpoint Identifier
ctrl_tun_core_ipv4_addr	Control Plane Core Tunnel IPv4 Address. SGW identifier for S11, PGW identifier for S5/S8-C, SMF identifier for N11 and GGSN for Gn, GP
ctrl_tun_core_ipv6_addr	Control Plane Core Tunnel IPv6 Address. SGW identifier for S11, PGW identifier for S5/S8-C, SMF identifier for N11 and GGSN for Gn, GP
ctrl_tun_core_teid	Control Plane Core Tunnel Endpoint Identifier
user_tun_up_link_ipv4_addr	User Plane Uplink Tunnel IPv4 Address. Identifier of the SGW/UPF that receives the uplink user plane data from the eNodeB/gNodeB
user_tun_up_link_ipv6_addr	User Plane Uplink Tunnel IPv6 Address. Identifier of the SGW/UPF that receives the uplink user plane data from the eNodeB/gNodeB
user_tun_up_link_teid	User Plane Uplink Tunnel Endpoint Identifier

teid	
user_tun_down_link_ipv4_addr	User Plane Downlink Tunnel IPv4 Address. Identifier of the eNodeB/gNodeB that receives the uplink user plane data from the SGW/UPF
user_tun_down_link_ipv6_addr	User Plane Downlink Tunnel IPv6 Address. Identifier of the eNodeB/gNodeB that receives the uplink user plane data from the SGW/UPF
user_tun_down_link_teid	User Plane Downlink Tunnel Endpoint Identifier
if_name	3GPP Control Plane Interface Name
name	Name of the event on the 3GPP control plane interface
cause_code	Outcome of the event on the 3GPP control plane interface. Mostly set to 16 to indicate a successful event
sm_context_ref	Session Management Context
ebi	EPS(Evolved Packet System) Bearer ID
lbi	Linked Bearer Identity
pdu_session_id	PDU(Packet Data Unit) Session ID
apn	Access Point Name
dnn	Data Network Name
ue_ipv4_addr	User Equipment IPv4 Address
ue_ipv6_addr	User Equipment IPv6 Address
ue_ipv4v6_addr	User Equipment IPv4v6 Address
ue_non_ip_addr	User Equipment non-IP Address
ue_addr_type	User Equipment IP address type (IPv4 or IPv6)
qci	QoS Class Identifier
qfi	QoS Flow Identifier
five_qi	5G QoS Identifier
cgi_mcc	Mobile Country Code from Cell Global Identity
cgi_mnc	Mobile Network Code from Cell Global Identity
cgi_lac	Local Area Code from Cell Global Identity
cgi_cell_id	Cell Identification from Cell Global Identity
sai_mcc	Mobile Country Code from Service Area Identifier
sai_mnc	Mobile Network Code from Service Area Identifier
sai_lac	Local Area Code from Service Area Identifier

sai_sac	Service Area Code from Service Area Identifier
tai_mcc	Mobile Country Code from Tracking Area Identity
tai_mnc	Mobile Network Code from Tracking Area Identity
tai_tac	Tracking Area Code from Tracking Area Identity
ecgi_mcc	Mobile Country Code from E-UTRAN Cell Global Identifier
ecgi_mnc	Mobile Network Code from E-UTRAN Cell Global Identifier
ecgi_cell_id	Cell Identification from E-UTRAN Cell Global Identifier
lai_mcc	Mobile Country Code from Location Area Identity
lai_mnc	Mobile Network Code from Location Area Identity
lai_lac	Local Area Code from Location Area Identity
enode_id_mcc	Mobile Country Code from Evolved Node
enode_id_mnc	Mobile Network Code from Evolved Node
macro_enode_id	Evolved Node ID
ncgi_mcc	Mobile Country Code from NR Cell Global Identity
ncgi_mnc	Mobile Network Code from NR Cell Global Identity
ncgi_nr_cell_id	Cell Identification from NR Cell Global Identity
rat_type	Type of Radio Access Technology
snssai_sst	Slice/Service Type from Single Network Slice Selection Assistance Information
snssai_sd	Slice Differentiator id from Single Network Slice Selection Assistance Information

User Plane Attributes

The user plane attributes are generated by Application Metadata Intelligence (AMI), and include information such as IP addresses, protocols, timestamps, and byte/packet counters. These attributes are generated from the network flows and do not require DPI capabilities. The attributes for the mobile network traffic are generated for the inner IP flow by bypassing the outer headers

Attribute	Description
ts	Timestamp of the metadata generated in UTC
vendor	Identifying Gigamon as the vendor providing the metadata
version	Version number of the GigaSMART software release from the AMI application
generator	Identifies the Gigamon device that generates the user plane metadata. For example - HC3
src_ip	Source IPv4 address of the inner flow
dst_ip	Destination IPv4 address of the inner flow

src_mac	Source MAC address of the inner flow
dst_mac	Destination MAC address of the inner flow
mpls	MPLS Label if the flow has the MPLS header
protocol	Layer 4 protocol of the inner flow
src_port	Layer 4 protocol source port of the inner flow
dst_port	Layer 4 protocol destination port of the inner flow
device_inbound_interface	Traffic receiving port on the Gigamon device example HC3
tcp_sport	Source TCP port
tcp_dport	Destination TCP port
udp_sport	Source UDP port
udp_dport	Destination UDP port
src_bytes	Source bytes from client to server in the flow including the outer and the inner IP header
dst_bytes	Destination bytes from client to server in the flow including the outer and the inner IP header
src_inner_bytes	Source bytes from the client to the server in the flow with the inner IP header (without the outer header)
dst_inner_bytes	Destination bytes from the server to the client in the flow with the inner IP header (without the outer header)
src_packets	Source packets from client to server in the flow including the header
dst_packets	Destination packets from client to server in the flow including header
total_bytes	Total bytes is sum of source and destination bytes
total_packets	Total packets is sum of source and destination packets
id	Unique flow id assigned to a flow
ingress_vlan_id	Vlan id in the packet received for the flow
src_ipv6	Source IPv6 address of the inner flow
dst_ipv6	Destination IPv6 address of the inner flow
ip_version	IP version v4, v6
ip_cos_id	QOS value in the IPv4 header
ip_dscp	DSCP value in the IPv4 header
ip_ttl	Time to live in the IPv4 header
ip6hop_limit	Hop limit in the IPv6 header
flow_labelv6	flow label in the IPv6 header
ip6_ds	DSCP value in the IPv6 header
tcp_flags	TCP flag in the TCP header
gre_key	Generic routing encapsulation header key in the GRE header
ip_hdr_len	IPv4 header length
ip_frag_flags	IPv4 fragmentation flags
ipv6frag_flags	IPv6 fragmentation flags

ip_frag_id	IPv4 fragment id
ipv6frag_id	IPv6 fragment id
ip_frag_offset	IPv4 fragment offset
ipv6frag_offset	IPv6 fragment offset
ipv4opt	IPv4 options
ip_precedence_id	IPv4 precedence id
ip6precedence_id	IPv6 precedence id
ip_tot_len	IPv4 total length
ip6tot_len	IPv6 total length
ipv6hdr_len	IPv6 header length
payload_len_id	Payload length for the flow excluding the L3 IPv4 header
next_hdr_v6	Layer 4 protocol
icmp_type_v4	ICMP message type IPv4
icmp_code_v4	ICMP response code IPv4
icmp_code_v6	ICMP response code IPv6
icmp_type_v6	ICMP message type IPv6
tcp_ack_id	TCP ack id
tcp_hdr_len	TCP header length
tcp_seq_no	TCP sequence number
tcp_urgent_ptr	TCP urgent pointer
tcp_win_size	TCP window size
udp_msg_len	UDP message length
ip6traffic_class	IPv6 traffic class same as QoS in IPv4
flow_start_usec	Inner flow start time in microseconds in UTC
flow_end_usec	Inner flow end time in microseconds in UTC
flow_start_sec	Inner flow start time in seconds in UTC
flow_end_sec	Inner flow end time in seconds in UTC
start_time	Inner flow start time in milliseconds in UTC
end_time	Inner flow end time in milliseconds in UTC
egress_intf_id	egress IP interface-id for the Gigamon device sending the metadata
sys_up_time_first	Difference between the flow start time and the gigaSMART uptime in milliseconds
sys_up_time_last	Difference between the flow end time and the gigaSMART uptime in milliseconds
end_reason	Inner flow end reason – TCP ack, reset, inactive, etc
tcpflagsyn	TCP flag SYN from TCP header
tcpflagsynack	TCP flag SYNACK from TCP header
tcpflagfin	TCP flag FIN (finish)from TCP header
tcpflagrst	TCP flag RST (reset) from TCP header
Labels	Labels are added to the metadata by configuration in AMX. There can be multiple labels configured and added. Each label is configured as a key and a string value.

Labels configured in the JSON example in the section below	
label_event_type	Label identifying the vendor generating the event in the AMX exporter
label_deployment	Label identifying the deployment address of the AMX exporter
label_traffic	Label identifying the traffic region where the AMX is deployed
MSS	Maximum payload size a TCP segment can carry without the headers. The MSS value is exported at the beginning of a flow. Its exported only when bidirectional flows are configured.
aggr-window-size	The actual TCP window size minimum, mean, and maximum values, calculated separately for both sender and receiver packets.
zero-window	This captures TCP zero window event statistics for both sender and receiver, indicating when the TCP receive buffer is full and data transmission is temporarily paused due to flow control.

Attributes for GigaVUE Enriched Metadata for Cloud Workloads

This section describes the various attributes available within GigaVUE Enriched Metadata for Cloud Workloads for the following platforms:

- [AWS](#)
- [Azure](#)
- [VMware vCenter](#)
- [Azure Kubernetes Service](#)
- [Zscaler Private Access \(ZPA\) Attributes](#)

For VPC/Organization Unit centric use cases			For aws service centric use cases			For data volumes use cases			
account_id	vpc/subnet_id	region/az_id	inst_type/id	dns	aws_service	app_name	up_bytes	down_bytes	...
244919184467	vpc-079c6ec	r-d7b3a	t3a.xl/i-dfd23	ec2.us-q	eks	icloud	3455	4566778	...
For account centric use cases			For service centric use cases			For app centric use cases			

- [Azure Kubernetes Service](#)

For various label centric use cases (usage, security monitoring, network issues)							For data volumes use cases		
iam_arn	node_orglabel	pod_applabel	node_type/id	pod/dns	service_name	app_name	up_bytes	down_bytes	...
arn:xx:12a:grp	eng_dep1	postgres_db	t3a.xl/i-dfd23	ng_1/ec2.us-q	db_lb	icloud	3455	4566778	...
For IAM centric use cases (AKS)		For service centric use cases			For app centric use cases				

The following table defines the purpose and scope of each referenced dataset, detailing configuration, resource, and operational parameters across AWS, Azure, and Kubernetes environments to support multi-cloud infrastructure documentation.

AWS

Attribute	Description	Source	Destination
aws_instance_id	ID of the EC2 instance	✓	✓
aws_instance_type	Type of EC2 instance	✓	✓
aws_availability_zone	Availability Zone of the EC2 instance	✓	✓
aws_image_id	ID of the base image use for EC2 instance	✓	✓
aws_private_dns_name	Private DNS hostname name assigned to the EC2 instance	✓	✓
aws_private_ip	Private IPv4 address assigned to the EC2 instance	✓	✓
aws_public_dns_name	Public DNS name assigned to the EC2 instance	✓	✓
aws_public_ip	Public IPv4 address assigned to the EC2 instance	✓	✓
aws_instance_state	Current state of the EC2 instance	✓	✓
aws_subnet_id	ID of the subnet in which the EC2 instance is running	✓	✓
aws_vpc_id	ID of the VPC in which the EC2 instance is running	✓	✓
aws_iam_	Amazon Resource Name (ARN) of the IAM instance profile	✓	✓

instance_profile_arn			
aws_iam_instance_profile_id	ID of the IAM instance profile	✓	✓
aws_security_group_name	Security group name assigned for the EC2 instance	✓	✓
aws_security_group_id	Security group ID assigned for the EC2 instance	✓	✓
aws_network_if_id	ID of the network interface	✓	✓
aws_network_if_attach_id	ID of the network interface attachment	✓	✓
aws_tags	Tags assigned to the EC2 instance in kv format with kv delimiter ':' and pair delimiter ','	✓	✓
aws_flat_tags	Tags assigned to the EC2 instance extracted to top level keys and values	✓	✓
aws_owner_id	ID of the AWS account that created the network interface	✓	✓
workload_platform	Platform Name - AWS	✓	✓

Azure

Attribute	Description	Source	Destination
azure_subscription_id	Subscription ID of the Azure account that created the VM	✓	✓
azure_resource_group	Resource Group of the VM	✓	✓
azure_vm_id	Complete path of the Azure VM. This includes subscription	✓	✓
azure_instance_id	Instance ID of the Azure VM	✓	✓
azure_instance_type	Instance type of the Azure VM	✓	✓
azure_availability_zone	Availability zone of the Azure VM	✓	✓
azure_image_id	Image ID of the Azure VM	✓	✓
azure_private_ip	Private DNS name assigned to the VM instance	✓	✓

dns_name			
azure_private_ip	Private IP address assigned to the VM instance	✓	✓
azure_public_dns_name	Public DNS name assigned to the VM instance	✓	✓
azure_public_ip	Public IP address assigned to the VM instance	✓	✓
azure_instance_state	Current state of the VM instance	✓	✓
azure_subnet_id	Subnet ID of the VM instance	✓	✓
azure_vnet_id	ID of the VNET in which the VM instance is running	✓	✓
azure_network_if_id	ID of the network interface	✓	✓
azure_network_if_attach_id	ID of the network interface attachment	✓	✓
azure_tags	Tags assigned to the VM instance in kv format with kv delimiter ':' and pair delimiter ','	✓	✓
azure_flat_tags	Tags assigned to the VM instance extracted to top level keys and values	✓	✓
azure_owner_id	Owner of the VM instance	✓	✓
azure_location	Resource Location	✓	✓
azure_scaleset_name	Scale set name	✓	✓
azure_scaleset_mode	Scale set orchestration mode	✓	✓
workload_platform	Platform Name - Azure	✓	✓

VMware vCenter

Attribute	Description	Source	Destination
vmware_vm_name	Name of the guest VM	✓	✓
vmware_vm_network	Network name of the guest VM	✓	✓
vmware_vm_status	Current status of the guest VM	✓	✓
vmware_vm_tags	Tags assigned to the guest VM in kv format with kv delimiter ':' and pair delimiter ','	✓	✓
vmware_vm_flat_tags	Tags assigned to the guest VM extracted to top level keys and values	✓	✓

vmware_vm_os_family_name	OS type of the guest VM (eg: Linux)	✓	✓
vmware_vm_os_distro_name	OS distribution name of the guest VM	✓	✓
vmware_vm_os_distro_version	OS distribution version of the guest VM	✓	✓
vmware_vm_os_distro_pretty_name	OS distribution pretty name of the guest VM	✓	✓
vmware_vm_dns_host_name	Host DNS name of the guest VM	✓	✓
vmware_vm_dns_host_domain_name	Host DNS domain name of the guest VM	✓	✓
vmware_host_name	Host name of the guest VM	✓	✓
vmware_host_ip	Host IP address of the guest VM	✓	✓
vmware_datacenter_name	Datacenter name of the guest VM	✓	✓
vmware_cluster_name	Cluster name of the guest VM	✓	✓
vmware_vcenter_name	vCenter name of the guest VM	✓	✓
workload_platform	Platform Name - VMware	✓	✓

Azure Kubernetes Service

Attribute	Description	Source	Destination
k8s_cluster_name	Name identifying the Kubernetes cluster	✓	✓
k8s_cluster_version	Version of Kubernetes running on the cluster	✓	✓
k8s_cluster_status	Operational state of the Kubernetes cluster	✓	✓
k8s_node_name	Identifier for the node within the cluster	✓	✓
k8s_node_internal_ip	Internal IP address assigned to the node	✓	✓
k8s_node_external_ip	External IP address of the node	✓	✓
k8s_node_os_version	Operating system version installed on the node	✓	✓
k8s_node_os_image	Name of the OS image used by the node	✓	✓
k8s_node_kernel_version	Kernel version of the node	✓	✓
k8s_node_cri_version	Version of the container runtime interface used on the node	✓	✓
k8s_node_status	Health and availability status of the node	✓	✓

k8s_node_labels	Node labels parsed into key-value pairs for metadata enrichment	✓	✓
k8s_pod_name	Name assigned to the Kubernetes pod	✓	✓
k8s_pod_labels	Pod labels parsed into key-value pairs for metadata enrichment	✓	✓
k8s_pod_namespace	Namespace in which the pod is deployed	✓	✓
k8s_pod_status	Operational state of the pod	✓	✓
k8s_pod_ip	IP address assigned to the pod	✓	✓
k8s_service_name	Name of the Kubernetes service	✓	✓
k8s_service_type	Type of service	✓	✓
k8s_container_name	Name of the container running inside the pod	✓	✓
k8s_container_image	Image used to create the container	✓	✓
k8s_container_port	Container port details	✓	✓

Zscaler Private Access (ZPA) Attributes

Attribute	Description
z_iss_username	Username of Zscaler Private Access user.
z_iss_client_private_ip	Private IP address of the Zscaler Private Access client
z_iss_client_public_ip	Public IP address of the Zscaler Private Access. client.
z_iss_customer	Name of Zscaler Private Access customer.
z_iss_connection_id	ID of the Zscaler Private Access connection.
z_iss_connection_status	Status of the Zscaler Private Access connection.
z_iss_connection_status_code	Status code of the Zscaler Private Access connection.
z_iss_connector	Name of the Zscaler Private Access application connector.
z_iss_hostname	Name of the host device as given by the Zscaler client connector.
z_iss_client_country_code	Country code of the Zscaler Private Access client location.
z_iss_policy	Name of the Zscaler Private Access policy.
z_iss_app_group	Group name of the Zscaler Private Access application.
z_iss_policy_processing_time	Processing time of the Zscaler Private Access policy.
z_iss_idp	Identity provider used by Zscaler Private Access.
z_iss_client_city	City of the Zscaler Private Access client location.
z_iss_platform	Client platform of Zscaler Private Access.
z_iss_connection_setup_time	Connection setup time for Zscaler Private Access.

Supported Element Types for NetFlow Integrator Element Mapping

This section outlines the element types (v5, v9, and v10) supported by the AMX application for element mapping from the ingest NetFlow/IPFIX flow records to JSON on the following platforms. These elements are predefined and cannot be configured:

- VMware ESXi
- VMware NSX-T

Elements	Description	Supported for NetFlow v5	Supported for NetFlow v9	Supported for NetFlow v10/IPFIX
type	Type of flow message	✓	✓	✓
sampler_address	Address of the device that generated the packet	✓	✓	✓
sampling_rate	Sampling rate of the flow	✓	✓	✓
export_time_ns	Export time in Nano seconds	✓	✓	✓
time_received_ns	Timestamp in nanoseconds of when the message was received	✓	✓	✓
sequence_num	Sequence number of the flow packet	✓	✓	✓
source_id	An identifier that uniquely identifies the flow source. For IPFIX it refers to the observation domain ID.	✗	✓	✓
etype	Ethernet type (0x86dd for IPv6...)	✓	✓	✓
src_addr	Source address (IP) • NetFlow v5 - IPv4 only • NetFlow v9 - IPV4_SRC_ADDR(8), IPV6_SRC_ADDR(27) • NetFlow v10/IPFIX - sourceIPv4Address(8), sourceIPv6Address(27)	✓	✓	✓
dst_addr	Destination address (IP) • NetFlow v5 - IPv4 only • NetFlow v9 - IPV4_DST_ADDR (12), IPV6_DST_ADDR (28) • NetFlow v10/IPFIX - destinationIPv4Address(12), destinationIPv6Address(28)	✓	✓	✓
ip_tos	IP Type of Service • NetFlow v5 – tos • NetFlow v9 - SRC_TOS (5) • NetFlow v10/IPFIX - ipClassOfService (5)	✓	✓	✓

¹The numbers within the enclosed brackets represent the element ID in IPFIX/NetFlow v10 and the field type ID in NetFlow v9.

ip_dscp	Differentiated Services Code Point • ipDiffServCodePoint (195)	x	✓	✓
ip_precedence	The value of the IP Precedence • ipPrecedence (196)	x	✓	✓
proto	Protocol (UDP, TCP, ICMP...) • NetFlow v5 – proto • NetFlow v9 - PROTOCOL (4) • NetFlow v10/IPFIX - protocolIdentifier (4)	✓	✓	✓
ip_ttl_max	Maximum TTL value observed for packets of the flow • NetFlow v9 - MAX_TTL (53) • NetFlow v10/IPFIX - maximumTTL (53)	x	✓	✓
src_port	Source port (when UDP/TCP/SCTP) • NetFlow v5 – srcport • NetFlow v9 - L4_SRC_PORT (7) • NetFlow v10/IPFIX - sourceTransportPort (7)	✓	✓	✓
dst_port	Destination port (when UDP/TCP/SCTP) • NetFlow v5 – dstport • NetFlow v9 - L4_DST_PORT (11) • NetFlow v10/IPFIX - destinationTransportPort (11)	✓	✓	✓
bytes	Number of bytes in a flow • NetFlow v5 – dOctets • NetFlow v9 - IN_BYTES (1), OUT_BYTES (23) • NetFlow v10/IPFIX - octetDeltaCount (1), postOctetDeltaCount (23)	✓	✓	✓
packets	Number of packets in a flow • NetFlow v5 – dPkts • NetFlow v9 - IN_PKTS (2), OUT_PKTS (24) • NetFlow v10/IPFIX - packetDeltaCount (2), postPacketDeltaCount (24)	✓	✓	✓
bytes_total	Running byte counter for a permanent flow • NetFlow v9 - IN_PERMANENT_BYTES (85) • NetFlow v10/IPFIX - octetTotalCount(85)	x	✓	✓
packets_total	Running packet counter for a permanent flow • NetFlow v9 - IN_PERMANENT_PKTS (86) • NetFlow v10/IPFIX - packetTotalCount(86)	x	✓	✓
flow_direction	Flow direction • NetFlow v9 - DIRECTION (61) • NetFlow v10/IPFIX - flowDirection(61)	x	✓	✓
in_if	Input interface	✓	✓	✓

	- NetFlow v5 – input - NetFlow v9 - INPUT_SNMP (10) - NetFlow v10/IPFIX - ingressInterface (10)			
out_if	Output interface - NetFlow v5 – output - NetFlow v9 - OUTPUT_SNMP (14) - NetFlow v10/IPFIX - egressInterface (14)	✓	✓	✓
time_flow_start_ns	Time the flow started in nanoseconds. Refer to Important Notes . - NetFlow v5 – System uptime and first - NetFlow v9 - System uptime and FIRST_SWITCHED (22) - NetFlow v10 - flowStartXXX (150, 152, 154, 156)	✓	✓	✓
time_flow_end_ns	Time the flow ended in nanoseconds. Refer to Important Notes . - NetFlow v5 – System uptime and last - NetFlow v9 - System uptime and LAST_SWITCHED (21) - NetFlow v10/IPFIX - flowEndXXX (151, 153, 155, 157)	✓	✓	✓
tcp_flags	TCP flags - NetFlow v5 – tcp_flags - NetFlow v9 - TCP_FLAGS (6) - NetFlow v10/IPFIX - tcpControlBits (6)	✓	✓	✓
ip_length_min	Minimum IP packet length - NetFlow v9 - MIN_PKT_LENGTH (25) - NetFlow v10/IPFIX - minimumIpTotalLength (25)	x	✓	✓
ip_length_max	Maximum IP packet length - NetFlow v9 - MAX_PKT_LENGTH (26) - NetFlow v10/IPFIX - maximumIpTotalLength (26)	x	✓	✓
next_hop	Nexthop IP address - NetFlow v5 – nexthop - NetFlow v9 - IPV4_NEXT_HOP (15), IPV6_NEXT_HOP (62) - NetFlow v10/IPFIX - ipNextHopIPv4Address (15), ipNextHopIPv6Address (62)	✓	✓	✓
ipv4_next_hop	Nexthop IPv4 address - NetFlow v9 - IPV4_NEXT_HOP (15) - NetFlow v10/IPFIX - ipNextHopIPv4Address (15)	x	✓	✓
ipv6_next_	Nexthop IPv6 address	x	✓	✓

hop	- NetFlow v9 - IPV6_NEXT_HOP (62) - NetFlow v10/IPFIX - ipNextHopIPv6Address (62)			
flow_id	An identifier of a flow that is unique within an Observation Domain - NetFlow v9 - flowId (148) - NetFlow v10/IPFIX - flowId (148)	x	✓	✓
firewall_event	Indicates a firewall event. Allowed values are listed in the firewall Event registry. firewallEvent(233)	x	✓	✓
icmp_type	Type of the ICMP message - NetFlow v9 - ICMP_TYPE (32) - NetFlow v10/IPFIX - icmpTypeXXX (176, 178), icmpTypeCodeXXX (32, 139)	x	✓	✓
icmp_code	Code of the ICMP message - NetFlow v9 - ICMP_TYPE (32) - NetFlow v10/IPFIX - icmpCodeXXX (177, 179) icmpTypeCodeXXX (32, 139)	x	✓	✓
flow_end_reason	The reason for flow termination. Values are listed in the flowEndReason registry.	x	✓	✓
application_id	Specifies an Application ID - NetFlow v9 - APPLICATION TAG (95) - NetFlow v10/IPFIX - applicationId (95)	x	✓	✓
application_description	Specifies the description of an application - NetFlow v9 - APPLICATION DESCRIPTION (94) - NetFlow v10/IPFIX - applicationDescription (94)	x	✓	✓
application_name	Specifies the name of an application - NetFlow v9 - APPLICATION NAME (96) - NetFlow v10/IPFIX - applicationName (96)	x	✓	✓
tcp_window_size	The window field in the TCP header tcpWindowsSize (186)	x	✓	✓
viptela_vpn_id	Private enterprise number for vIPtela Inc. (41916)	x	x	✓

Troubleshoot AMI/AMX Deployment

This topic helps troubleshoot AMI/AMX deployments on GigaVUE V Series Nodes and focuses specifically on scenarios where AMI is not exporting IPFIX/CEF records and AMX is not receiving traffic or is not exporting JSON records to downstream tools.

Scenario 1: AMI not exporting IPFIX/CEF records (exporter side)

Download exporter records

To download the exporter records:

1. In GigaVUE-FM, go to **Traffic > Virtual > Orchestrated Flows > VMware** (You can select the cloud platform which you have configured. This scenario explains the VMware platform). The Monitoring Session page appears.
2. Select the monitoring session that you want to troubleshoot.
3. Go to the **Traffic Processing** tab. The canvas appears with the monitoring session components
4. Select the AMI application and click Three-dots menu to view the application details.
5. Select the **Statistics** tab and the Exporter section appears.
6. Select the required records and click **Download Records**. The Exporter Mapping dialog appears.
7. Select the V Series Node and the tunnels for exporters from the dropdown list.
8. Click **Download Exporter**. The PCAP file (for example, Pcap__e1_link3_2026-03-12_174220.pcapng) is downloaded to your local machine. The progress of the PCAP file download appears in the browser.

NOTE: If there are no packets or records during the capture window, the system displays the message **No file captured**.

9. Verify whether the PCAP file contains valid IPFIX/CEF records for the specified exporter instance.

Scenario 2: AMX not receiving AMI/NetFlow records (ingestor side)

Verify topology and mapping

To verify topology and mapping:

1. Confirm whether the AMI exporter is configured to send records to the data interface of the correct AMX instance.
2. Use the AMX interface mapping in FM (management/data/tool) to ensure the correct interface is used for receiving records.

Download PCAP file using Download TCP Dump

To download the PCAP file:

1. In GigaVUE-FM, go to **Traffic > Virtual > Orchestrated Flows > VMware**. The Monitoring Session page appears. You can select the cloud platform which you have configured. This scenario explains the VMware platform.
2. Select the monitoring session that you want to troubleshoot.
3. Go to the **Traffic Processing** tab. The canvas appears with the monitoring session components
4. Select the AMX application and click Three-dots menu to view the application details.
5. Select the **Statistics** tab and select the V Series node for the AMX instance from the V Series Node IP dropdown list.
6. In the **Ingestor** section, select the required record and click **Download TCP Dump**. The **Ingestor Interface Mapping** dialog appears.
7. Select the interface mapping for the ingestor. The AMX interface naming includes the type and IP address of the interface:
 - For example, Zscaler ingestor - MGMT (ens160) IPv4: 10.114.26.181 IPv6: fcab:0:1:2040:a0a1:874e:7a66:40a2
 - Other ingestors (AMI, NetFlow/IPFIX, Mobility) - DATA (ens192) IPv4: 10.114.42.135 IPv6: fcab:0:1:2040:a0a1:874e:7a66:40a2
8. click **Download TCP Dump**. The PCAP file is downloaded to your local machine. The progress of the PCAP file download appears in the browser.

NOTE: The PCAP file is stored temporarily on the Application Metadata Exporter virtual machine and is automatically deleted after download.

9. Verify whether (IPFIX/CEF/NetFlow/JSON-over-UDP/GTPC) records are visible on the ingestor port. If the PCAP is empty or only shows partial traffic, this suggests a datapath issue upstream of AMX (AMI export or fabric).

Scenario 3: AMX not exporting JSON records (exporter side)

Check exporter status and counters

To check exporter status:

1. In the Exporter section, verify the number of files processed versus files skipped.
2. Check the error counters (if exposed via UI).

Download exporter records

To download the exporter records:

1. In GigaVUE-FM, go to **Traffic > Virtual > Orchestrated Flows > VMware**. The Monitoring Session page appears. You can select the cloud platform which you have configured. This scenario explains the VMware platform.
2. Select the monitoring session that you want to troubleshoot.
3. Go to the **Traffic Processing** tab. The canvas appears with the monitoring session components
4. Select the AMX application and click Three-dots menu to view the application details.
5. Select the **Statistics** tab and select the V Series node from the V Series Node IP dropdown list.
6. In the Exporter section, verify the number of Files processed vs files skipped.
7. Select the required records and click **Download Records**. The exporter JSON file is downloaded to your local machine. The progress of the PCAP file download appears in the browser.

NOTE: If there are no packets or records during the capture window, the system displays the message **No file captured**.

8. Validate the JSON structure and key fields required by the tool (e.g., Splunk, Elastic).
9. Check for malformed or truncated records.

GigaSMART NetFlow Generation

NetFlow Generation is a simple and effective way to increase visibility into traffic flows and usage patterns across systems. The flow-generated data can be used to build relationships and usage patterns between nodes on the network.

Refer to the following topic for step-by-step instructions on how to configure NetFlow for Virtual Environment:

- [Configure Application Metadata Intelligence for Virtual Environment](#)- For SecureVUE Plus Base Bundle
- [Create NetFlow Session for Virtual Environment](#) - ForNetVUE Base Bundle

Create NetFlow Session for Virtual Environment

NOTE: This configuration is applicable only when using NetVUE Base Bundle.

To create an NetFlow session, follow these steps:

1. Drag and drop **Application Metadata** from **APPLICATIONS** to the graphical workspace.
2. Click the Application Metadata application and select **Details**. The Application quick view appears.

3. In the Application quick view, enter or select the following details in the **General** tab:

Parameter	Description																							
Name	Enter a name for the application.																							
Description	Enter the description.																							
Application Metadata Settings																								
Flow Direction	Enable or Disable Bi-Directional Flow behavior. Bi-Directional is enabled by default. Disable this option for Uni-Directional Flow behavior.																							
Timeout	Specify the traffic flow inactivity timeout, in seconds. The session will be removed due to inactivity when no packets match.																							
Data Link	If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the Data Link and enable the VLAN option.																							
Observation ID	Enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is 00 01 02 05 , and in Decimal is 66053 .																							
Advanced Settings																								
Number of Flows	The number of flows supported by the application. Refer to the following table for the maximum number of flows supported for VMware, AWS, and Azure platforms. <table border="1"> <thead> <tr> <th>Cloud Platform</th><th>Instance Size</th><th>Maximum Number of Flows</th></tr> </thead> <tbody> <tr> <td>VMware</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr> <tr> <td rowspan="4">AWS</td><td>AMD - Large (c5n.2xlarge)</td><td>300k</td></tr> <tr> <td>AMD - Medium (t3a.xlarge)</td><td>100k</td></tr> <tr> <td>ARM - Large (c7gn.2xlarge)</td><td>100k</td></tr> <tr> <td>ARM - Medium (m7g.xlarge)</td><td>200k</td></tr> <tr> <td rowspan="2">Azure</td><td>Large (Standard_D8s_v4)</td><td>500k</td></tr> <tr> <td>Medium (Standard_D4s_v4)</td><td>100k</td></tr> <tr> <td>Nutanix</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr> </tbody> </table> - Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k.. - If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.	Cloud Platform	Instance Size	Maximum Number of Flows	VMware	Large (8 vCPU and 16GB RAM)	200k	AWS	AMD - Large (c5n.2xlarge)	300k	AMD - Medium (t3a.xlarge)	100k	ARM - Large (c7gn.2xlarge)	100k	ARM - Medium (m7g.xlarge)	200k	Azure	Large (Standard_D8s_v4)	500k	Medium (Standard_D4s_v4)	100k	Nutanix	Large (8 vCPU and 16GB RAM)	200k
Cloud Platform	Instance Size	Maximum Number of Flows																						
VMware	Large (8 vCPU and 16GB RAM)	200k																						
AWS	AMD - Large (c5n.2xlarge)	300k																						
	AMD - Medium (t3a.xlarge)	100k																						
	ARM - Large (c7gn.2xlarge)	100k																						
	ARM - Medium (m7g.xlarge)	200k																						
Azure	Large (Standard_D8s_v4)	500k																						
	Medium (Standard_D4s_v4)	100k																						
Nutanix	Large (8 vCPU and 16GB RAM)	200k																						

NOTE: When using NetVUE Base Bundle, Multi-Collect, Fast Mode, and Aggregate round-trip time fields are disabled.

4. In the Application quick view, enter or select the following details in the **Exporters** tab:

Parameter	Description
Exporter Name	Enter a name for the Exporter.
Actions	Using this option, you can perform the following functions: • Add Exporter - Use to add a new Exporter to this Application Metadata Intelligence Application • Apply Template - Use to select the tool template. Refer to Create Custom Tool Templates for more details on what are tool templates and to create custom tool templates. • Save as New Template - Use to save the current configuration as a new custom tool template. • Delete this Exporter - Use to delete the Exporter.
APPLICATION ID	Enable to export the data with Application Id.
Format	Select NetFlow
NetFlow: Select this option to use NetFlow	
Record / Template type	• Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. • Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active flow timeout value in seconds.
Inactive Timeout	Enter the inactive flow timeout in seconds.
Version	Select the NetFlow version.
Template Refresh Interval	Enter the time interval at which the template must be refreshed in seconds
APPLICATION & ATTRIBUTES: Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each application. (Not applicable when using Netflow V5, V9, Netflow IPFIX(V10), or CEF when the flow direction is Uni-Directional in the above Template drop-down menu.)	
Add Application	Click on the Add Application button. The Add Application dialog box opens. Select a Type. The available options are: • Application Family: Each application is mapped only mapped to one Application Family ▪ Select an Application Family and the Applications that needs to be filtered from the traffic. ▪ Attributes for the selected application is displayed in the Attribute column. You can select the required attributes. • Application Tag: Each application can be mapped to one or more Application Tags. ▪ Select an Application Tag and the Applications that needs to be filtered from the traffic. ▪ Attributes for the selected application is displayed in the

Parameter	Description
	Attribute column. You can select the required attributes.
NETWORK & TRANSPORT PARAMETERS:	
Select the Network and the transport packet attributes with the respective parameters	
Data Link	Select any one of the parameters such as Source MAC Address, Destination MAC Address and VLAN.
Interface	Select any one of the parameter such as Input Physical, Output Physical and Input Name.
IP	Select the parameter as Version if required.
IPv4	Select the required attributes. By default, Source Address, Destination Address, and Protocol are enabled.
IPv6	Select the required attributes. By default, Source Address, Destination Address, and Next Header are enabled.
Transport	Select the required attributes. By default, Source Port, Destination Port are enabled.
Counter	Select the Bytes, and Packets.
Timestamp	Select the required timestamp such as System Uptime First, Flow Start, System Uptime Last, and Flow End.
Flow	Select the parameter as End Reason if required.
GTP-U	Select the required parameters such as QFI and TEID.
Outer IPv4	Select any one of the parameter such as Source or Destination.
Outer IPv6	Select any one of the parameter such as Source or Destination.

5. Click **Save**.

Examples- Configuring Application Intelligence Solution with Other Applications

This sections provides information on how applications like Application Filtering Intelligence, Application Metadata Intelligence and Application Metadata Exporter can be used with other applications in the monitoring session.

Refer to the following topics for more detailed information:

- [Slicing and Masking with Application Filtering Intelligence](#)
- [De-duplication with Application Metadata Intelligence](#)

Slicing and Masking with Application Filtering Intelligence

When the traffic passes through the Application Filtering Intelligence, application metadata is created. You can use the Slicing and Masking application along with Application Filtering application slice, mask, or slice and mask the filtered packets before sending them to the

destination tunnel endpoint.

NOTE: When combining Slicing and Masking operations, the offset range of the Masking must be lesser than the offset value entered for the Slicing operation, as the Slicing operation is performed first.

Follow the steps below to configure Application Filtering Intelligence with Masking and Slicing:

1. Drag and drop **New Map / Application Filtering** from **New** to the graphical workspace.
2. Click the map and select **Details**. The Application quick view appears.
3. Configure Application Filtering Intelligence using the steps given in [Configure Application Filtering Intelligence for Virtual Environment](#).
4. Drag and drop **Slicing** from **Applications** to the graphical workspace.
5. Click the application and select **Details**. The Application quick view appears.
6. Configure Slicing application using the steps given in [Slicing](#)
7. Drag and drop **Masking** from **Applications** to the graphical workspace.
8. Click the application and select **Details**. The Application quick view appears.
9. Configure Masking application using the steps given in [Masking](#).
10. Drag and drop **New Tunnel** from **New** to the graphical workspace.
11. Click the tunnel and select **Details**. The Application quick view appears.
12. Select the **Type** as L2GRE/VXLAN. Select the Traffic Direction as **Out**. Refer to Create Ingress and Egress Tunnel section in the respective Cloud Deployment guides for step-by-step instructions on how to configure Tunnels.
13. Enter Source L4 Port and Destination L4 Port.
14. After placing the required items in the canvas, hover your mouse on the applications, click the red dot, and drag the arrow over to another item (map, application, or tunnel).

The filtered traffic will be sent to the Slicing application, the sliced traffic will be sent to Masking application and then to the destination tunnel Endpoint.

De-duplication with Application Metadata Intelligence

Duplicate packets are common in network analysis environments where both the ingress and egress data paths are sent to a single output. Using de-duplication with Application Metadata Intelligence lets you eliminate the duplicate packets in the Application Metadata output, only forwarding a packet once and thus reducing the processing load on your tools.

Follow the steps below to configure Application Metadata Intelligence with De-duplication:

1. Drag and drop **Application Metadata** from **Applications** to the graphical workspace.
2. Click the application and select **Details**. The Application quick view appears.
3. Configure Application Metadata Intelligence using the steps given in [Configure Application Metadata Intelligence for Virtual Environment](#).
4. Drag and drop **dedup** from **Applications** to the graphical workspace.
5. Click the application and select **Details**. The Application quick view appears.
6. Configure de-duplication application using the steps given in [De-duplication](#).
7. Drag and drop **New Tunnel** from **New** to the graphical workspace.
8. Click the tunnel and select **Details**. The Application quick view appears.
9. Select the **Type** as UDP.
10. Enter Source L4 Port, Destination L4 Port, and Destination IP. Refer to Create Ingress and Egress Tunnel section in the respective Cloud Deployment guides for step-by-step instructions on how to configure Tunnels.
11. After placing the required items in the canvas, hover your mouse on the map, click the red dot, and drag the arrow over to another item (map, application, or tunnel).

The duplicate packets are removed before sending the traffic to AMI. This will reduce the load on Application Metadata application which in turn can avoid exporting the duplicated Metadata to the tool.

De-duplication

De-duplication application targets, identifies, and eliminates duplicate packets, blocking unnecessary duplication and sending optimized flows to your security and network monitoring tools. De-duplication lets you detect and choose the duplicate packets to count or drop in a network analysis environment.

Duplicate packets are common in network analysis environments where both the ingress and egress data paths are sent to a single output. They can also appear when packets are gathered from multiple collection points along a path. The de-duplication application lets you eliminate these packets, only forwarding a packet once and thus reducing the processing load on your tools.

Refer to the following topics:

- [Feature Overview](#)
- [Configure De-duplication Application](#)
- [Distributed De-duplication](#)

Feature Overview

There are two actions that can be specified for handling the duplicate packets detected:

- drop, which drops the duplicate packets
- count, which counts the duplicate packets, but does not drop them

A time interval can be configured within which an identical packet will be considered a duplicate. The greater the interval over which traffic can be checked for duplicates, the higher the accuracy of the de-duplication detection and subsequent elimination.

For example, if two of the same packets are seen in the specified time interval, the packets will be detected as duplicates. If one packet is seen in the time interval and another packet is seen in a later time interval, the packets will not be detected as duplicates.

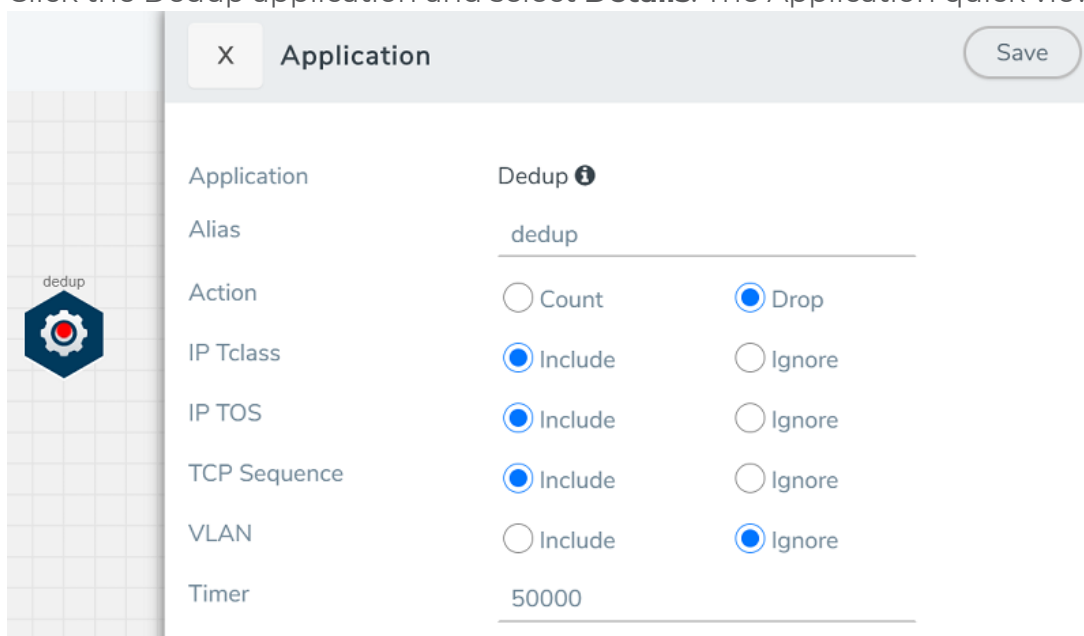
For IPv4 and IPv6 packets, to determine if a packet is considered to be a duplicate, parts of the IP headers (Layer 3 and Layer 4), as well as part of the payload are compared.

For non-IP packets, a packet is considered to be a duplicate if it is identical.

Configure De-duplication Application

To add a de-duplication application:

1. Drag and drop **Dedup** from **APPLICATIONS** to the graphical workspace.
2. Click the Dedup application and select **Details**. The Application quick view appears.



Application	
Application	Dedup ⓘ
Alias	dedup
Action	☐ Count ☒ Drop
IP Tclass	☒ Include ☐ Ignore
IP TOS	☒ Include ☐ Ignore
TCP Sequence	☒ Include ☐ Ignore
VLAN	☐ Include ☒ Ignore
Timer	50000

3. In the Application quick view, enter the information as follows:

Parameter	Description
Alias	Enter a name for the application.
Action	Specifies whether duplicate packets are to be counted or dropped as follows: - o Count– The de-duplication application counts the duplicate packets, but does not drop them. - o Drop– The de-duplication application drops the duplicate packets. The default is drop.
IP Tclass IP TOS TCP Sequence VLAN	These options are useful when applying de-duplication operations to packets in a NAT environment. Different NAT implementations can change certain packet header fields (for example, the TCP sequence number). If you want to be able to detect duplicates without requiring that these fields match (ToS field, TCP sequence number, VLAN ID), you can disable the corresponding option. - o IP Tclass – Ignore or include IPv6 traffic class. Use for IPv6. The default is include. - o IP TOS – Ignore or include the IP ToS bits when detecting duplicates. Use for IPv4. The default is include. - o TCP Sequence – Ignore or include the TCP Sequence number when detecting duplicates. The default is include. - o VLAN – Ignore or include the VLAN ID when detecting duplicates. The default is ignore. Include means the field will be included when the application compares packets. Ignore means the field will be ignored when the application compares packets.
Timer <Value: 10-500000 µs>	Configures the time interval within which an identical packet will be considered a duplicate. The greater the interval over which traffic can be checked for duplicates, the higher the accuracy of the de-duplication detection and subsequent elimination. The default is 50,000µs. For example, if two same packets are seen in the specified time interval, the packets will be detected as duplicates. If one packet is seen in the time interval and another packet is seen in a later time interval, the packets will not be detected as duplicates. NOTE: Retransmissions are not counted as duplicates.

4. Click **Save**.

Distributed De-duplication

In distributed de-duplication, when you set up a Monitoring Session with a de-duplication app, the traffic is first sent to a component which distributes the traffic based on a consistent mechanism to ensure that packets from a particular traffic go to the same de-duplication instance. The packets are shared across the GigaVUE V Series Nodes. The distributed de-duplication more efficient that the existing de-duplication.

NOTE: From version 6.9, Traffic Distribution option is renamed to Distributed De-duplication.

From version 6.5, distributed de-duplication is supported on Azure, AWS, GCP, Nutanix, VMware NSX-T, VMware ESXi, and OpenStack. An enhanced configuration profile for the load balancer will be set by default with no option for modification. The default profile will use source and destination IP addresses, source and destination ports as the configuration for calculating the hash value for traffic distribution.

Important:

1. False traffic health alarms could be raised due to distribution of traffic across GigaVUE V Series Nodes.
2. Statistics are displayed for all the applications. Distributed De-duplication requires additional entities which will be listed in statistics page.

Limitations

- When using distributed de-duplication application, if **Prefer IPv6** option is enabled when configuring GigaVUE V Series Node using GigaVUE-FM, IPv6 tunnel will be created only between GigaVUE V Series Node and UCT-V and the rest of the tunnels created are IPv4 tunnels. Refer to Configure GigaVUE Fabric Components section in the respective cloud deployment guide for more detailed information on how to deploy GigaVUE V Series Node with IPv6 tunnels.
- When using distributed de-duplication application, if **Enable IPv6 Preference** option is enabled when configuring GigaVUE V Series Node using Third Party Orchestration, IPv6 tunnel will be created only between GigaVUE V Series Node and UCT-V and the rest of the tunnels created are IPv4 tunnels. Refer to *Create Monitoring Domain* section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration Guide for more detailed information on how to create a monitoring domain to register GigaVUE fabric components with IPv6 tunnels.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

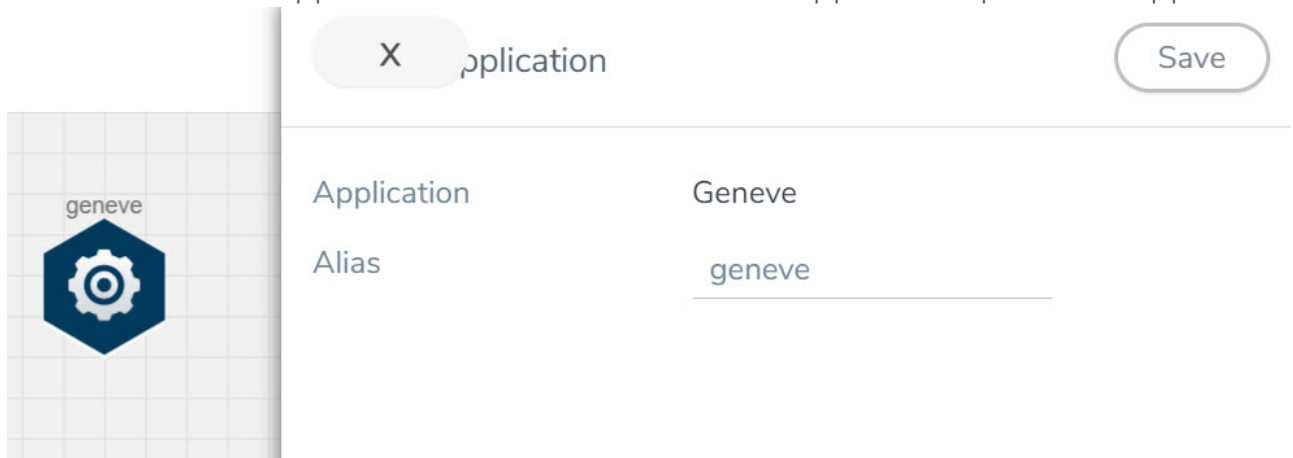
You can view the statistics of the application in the **STATISTICS** tab.

GENEVE Decapsulation

The GENEVE Decapsulation application is used to acquire and strip GENEVE headers. To route the traffic through the third-party network appliances seamlessly, the AWS gateway load balancer with a VPC adds GENEVE header to packets as they are forwarded to a third-party network appliance. Each appliance is expected to terminate the GENEVE tunnel and process the GENEVE encapsulated traffic. When the GigaVUE-FM directs the acquisition of the customer traffic, the packets are encapsulated and forwarded as GENEVE tunnels that are terminated in GigaVUE V Series nodes.

To add a GENEVE application:

1. Drag and drop **GENEVE** from **APPLICATIONS** to the graphical workspace.
2. Click the GENEVE application and select **Details**. The Application quick view appears.



Application	Geneve
Alias	<u>geneve</u>

3. Enter an alias for the GENEVE application.
4. Click **Save**.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to *Traffic Health Monitoring* section in the respective GigaVUE Cloud Suite deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to *Monitor Cloud Health* section in the respective GigaVUE Cloud Suite deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

Header Stripping

Header Stripping application efficiently examines the packets for specified headers like GTP, ISL, ERSPAN, MPLS, MPLS+VLAN, VLAN, VN-tag, VXLAN, FM6000Ts, GENEVE, and generic and remove them before sending the packet to the appropriate security and analysis tools. Each packet is examined for the packet forwarding addition, and it also ensures that the headers are removed before sending the packet to the tools. This application is useful when working with tools that either cannot recognize these headers or must engage in additional processing to adjust for them.

Furthermore, the presence of protocols like GTP, ISL, ERSPAN, MPLS, MPLS+VLAN, VLAN, VN-tag, VXLAN, GENEVE, and FM6000Ts in the packet can restrict or limit the ability to apply filtering and flow-based load balancing to the traffic as it is forwarded to specific tools. To address each of these challenges, Header Stripping of these protocols is required.

List of Protocols that are supported for stripping:

- GTP
- ISL
- ESPRAN
- MPLS
- MPLS+VLAN
- VLAN
- VN-tag
- VXLAN
- FM6000Ts
- GENEVE
- Generic

**Note:**

Header Stripping for the GENEVE protocol is currently supported for the following platforms:

- VMware vCenter
- VMware NSX-T
- Nutanix

Limitation

The GENEVE protocols currently supported for header stripping are the Transparent Ethernet Bridge (0x6558), IPv4 (0x0800), and IPv6 (0x86DD).

Configure Header Stripping Application

To configure the Header Stripping application in GigaVUE-FM, follow the steps given below:

1. Drag and drop **Header Stripping** from **APPLICATIONS** to the graphical workspace.
2. Click the Header Stripping application and select **Details**. The Application quick view appears.

3. In the application quick view, enter or select the required information as described in the following table:

Field	Description
Alias	Enter the alias name for the application.
Protocol	Select the type of protocol.
VLAN: Use this option to strip the VLAN header from the packets. You can either strip the outer VLAN header or the entire VLAN header. When choosing VLAN as your protocol for stripping, enter the following details:	
VLAN Header	The VLAN Header that should be stripped. The supported minimum value is 0, and the maximum value is 16777215. The default value is 0.
VXLAN: Use this option to strip VXLAN (Virtual eXtensible Local Area Network) headers. You can strip either matching VXLAN headers or all VXLAN headers. When choosing VXLAN as your protocol for stripping, enter the following details:	
VXLAN ID	The VXLAN ID that should be stripped. The default value is outer.
FM6000Ts: Use this option to strip FM6000Ts time stamp headers. Packets entering the application from other devices may contain FM6000 timestamps. FM6000 is an Intel chip used for time stamping. FM6000 has a hardware timestamp in the packet. When choosing FM6000Ts as your protocol for stripping, enter the following details:	
Time Stamp Format	The format of the time stamp you wish to strip. The only supported format for the time stamp is None .
ESPRAN: Use this option to strip ESPRAN Type II and Type III headers. When choosing ESPRAN as your protocol for stripping, enter the following details:	
ESPRAN FlowID	Specify an ESPRAN flow ID between 0 to 1023. A flow ID of zero is a wildcard value that matches all flow IDs.
GENEVE: Use this option to strip the GENEVE header from the packets. The default L4 Destination Port value is 6081. To change the default L4 destination port value, follow the steps given below:	
1. Expand the Custom Port section. 2. You can either select an existing template with the port details or provide them directly in the pop-up window. - o Using Template - If you wish to use an existing template, select the template from the Template drop-down menu. To create a new template, refer to Create Custom Port Template. Note: You cannot modify an existing template by editing the values directly in the Monitoring Session. However, you can modify the values in the Monitoring Session and save it as a new template. - o Without Template - You can directly enter your port details in the L4 Destination Port field. Click the Save as New Template button to save this existing configuration as a template. You can view the newly created template in the Custom Port Template page.	

Generic: Using this option to strip any header without worrying about the header level. When choosing generic as your protocol for stripping, enter the following details:	
Ah1	The anchor header (AH1), after which the header to be stripped occurs.
Offset	Based on the selected Offset, enter the following details: • Offset Range: If you wish to use offset range as your offset, then enter the following details: a. Offset Range Value: Specify the offset of the header occurrence from the above anchor header. The minimum supported value is one, and the maximum supported value is 1500. b. Header Count: Specify the number of headers the application should remove from the offset. The minimum supported value is one, and the maximum is 32. c. Custom Len: The length (in bytes) of the header that should be stripped. d. Ah2: The next possible standard header that occurs immediately after the header. • Start / End: If you wish to use start or end as your offset, then enter the following details: a. Header Count: Specify the number of headers that the application should remove from the offset.. The minimum supported value is one, and the maximum is 32. b. Custom Len: The length (in bytes) of the header that should be stripped. The minimum supported value is one, and the maximum supported value is 1500. c. Ah2: The next possible standard header that occurs immediately after the header.

4. Click **Save**.

Create Custom Port Template

GigaVUE-FM enables you to specify custom L4 destination port values when using the Header Stripping application. You can create a template and utilize it to define custom port values when configuring the Header Stripping application.

To create a custom port template for the Header Stripping application:

1. Go to **Inventory > Resources > Custom Port Template**. The **Custom Port Template** page appears.
2. Click **New** to create a new template. The **New Custom Port Template** dialog box appears.
3. Enter a name for the template.
4. Enter valid port numbers between the range 1025 to 65535 in the **L4 Destination Port** field. Enter only comma separated integer values. You can provide a maximum of 10 ports. For example: 1034,1098,1039
5. Click **Save**.

You can view the created template on the **Custom Port Template** page. If a template is associated with a Monitoring Session, you can view the name of the Monitoring Session to which the template is associated in the Affected Entity column.

You can use the **Actions** buttons to perform the following:

- **Edit:** You can use this option to edit a template. If a template is associated with a Monitoring Session, editing it will be reflected in all the Monitoring Sessions associated with that template.
- **Delete:** You can use this option to delete a template. You cannot delete a template associated to a Monitoring Session.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on traffic health monitoring and how to create a threshold template, refer to *Traffic Health Monitoring* section in the respective GigaVUE Cloud Suite deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to *Monitor Cloud Health* section in the respective GigaVUE Cloud Suite deployment guides.

You can view the application statistics in the **STATISTICS** tab.

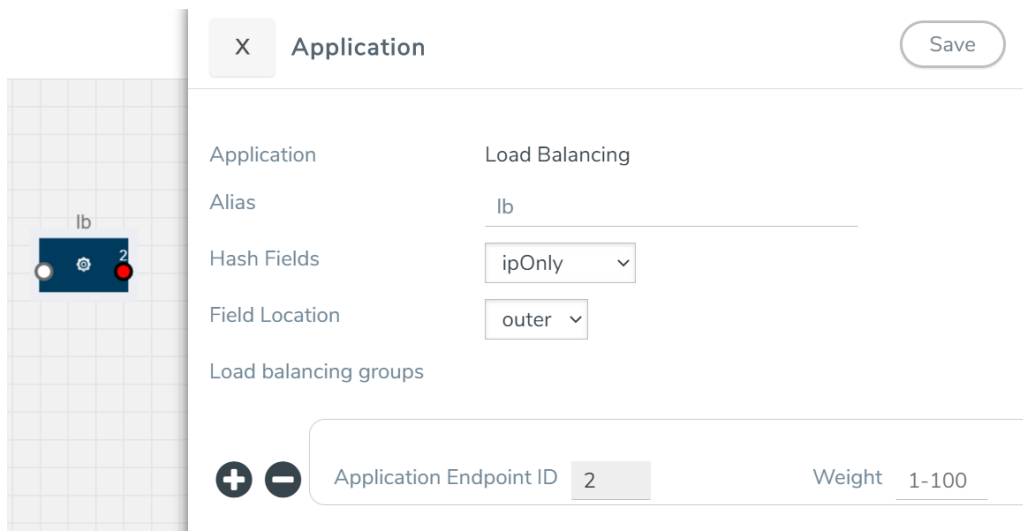
Load Balancing

Load balancing application performs stateless distribution or Enhanced Load Balancing of the packets between different endpoints. Stateless load balancing distributes the processed traffic to multiple tool ports or tunnel endpoints based on hash values generated from predefined protocol fields in the packet.

When Enhanced Load Balancing is enabled and an endpoint fails, the traffic is redistributed for the failed endpoint. When the failed endpoint recovers, the redistributed traffic is restored to the recovered endpoint. The traffic across other endpoints remain undisturbed during this process.

To add a load balancing application:

1. Drag and drop **Load Balancing** from **APPLICATIONS** to the graphical workspace.
2. Click the load balancing application and select **Details**. The Application quick view appears.



Application

Alias: lb

Hash Fields: ipOnly

Field Location: outer

Load balancing groups

	Application Endpoint ID	Weight
+	2	1-100
-		

3. In the Application quick view, enter the information as follows:

Metric	Description
Alias	Enter a name for the load balancing application
Stateless	Select this option to enable Stateless Load Balancing
Enhanced Load Balancing	Select this option to enable Enhanced Load Balancing and select the ELB profile.
Hash Field	ipOnly: The source IP and destination IP addresses. ipAndPort: The source IP and destination IP addresses, and Layer 4 source port and destination port numbers. fiveTuple: The source IP and destination IP addresses, source port and destination port numbers, and protocol field in the IP header. gtpuTeid: The GTP-u tunnel identifier (ID). Note: There is no inner or outer field location for GTPU-TEID. greFlowid: The flow identifier location. Note: - The default field location value is outer. - When configuring 5G-Cloud Ericsson SCP Transparent, greFlowid hash field should be selected. Refer to 5G-Cloud Ericsson SCP Support.
Field Location	Outer: The first occurrence of header or field. For example, IP Only outer is the first IP header in the packet, which could be IPv4 or IPv6. Inner: The second occurrence of header or field. The supported IP encapsulation types are: IP-in-IP, VXLAN, GTP, GRE, and ERSPAN.
Load balancing groups	Add or remove an application with the Endpoint ID and Weight value (1-100). A load balancing group can have minimum of two endpoints. Endpoint with higher weight receives more traffic.

- 4. Click **Save**.

NOTE: When you configure the Load Balancing Application in enhanced mode, you can associate it with only a single enhanced load balancing profile. However, you have the flexibility of changing the association to different profile as needed.

Enhanced Load Balancing

Enhanced Load Balancing redistributes the traffic from a failed endpoint to another endpoint which is a part of the ELB group. When the failed endpoint recovers, the redistributed traffic is restored to the recovered endpoint. The traffic across other endpoints remain undisturbed during this process. Hashing is performed on the packets based on outer and/or inner headers.

To enable to enhanced load balancing application:

- 1. Create an Enhanced Load Balancing Profile.
 - a. In the Monitoring domain page, click Settings, then click **Enhanced Load Balancing**
 - b. Click **New** and then create a profile.

Fields	Values
Hash fields	The various hash options are - ip - ip-src - ip-dst - l4-port - l4-portsrc - l4-portdst - gtpuportid
Position	Select either inner/outer location of the hash field to be matched with the incoming packet..
Hash-mask	When the hash-fields ip-src/ip-dst are defined along with the IP, then ip-src/ip-dst hash-mask will overwrite the IP hash mask. For load balancing, you must apply this mask before hashing the IP. The default options and their default values are: IPv4 : 255.255.255.255 IPv6 : FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

2. Go to monitoring session page and
 - a. Drag and drop **Load Balancing** from **APPLICATIONS** to the graphical workspace.
 - b. Click the load balancing application and select **Details**. The Application quick view appears.

× Load Balancing: lb
 Save

DETAILS

THRESHOLDS

HEALTH STATUS

STATISTICS

Application Load Balancing

Alias* lb

☐ Stateless
 ☒ Enhanced Load balancing

ELB profiles* Select... ▼

Load balancing groups

Application Endpoint ID	2	Weight	1	⊕ ⊖
Application Endpoint ID	3	Weight	1	⊕ ⊖

⏪

c. In the Application quick view, enter the information as follows:

Metric	Description
Alias	Enter a name for the load balancing application
Enhanced Load Balancing	Select this option to enable Enhanced Load Balancing and select the ELB profile.
Load balancing groups	Add or remove an application with the Endpoint ID and Weight value (1-100). A load balancing group can have minimum of two endpoints.

3. Click **Save**.

NOTE: When you configure the Load Balancing Application in enhanced mode, you can associate it with only a single enhanced load balancing profile. However, you have the flexibility of changing the association to different profile as needed.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to *Traffic Health Monitoring* section in the respective GigaVUE Cloud Suite deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to *Monitor Cloud Health* section in the respective GigaVUE Cloud Suite deployment guides.

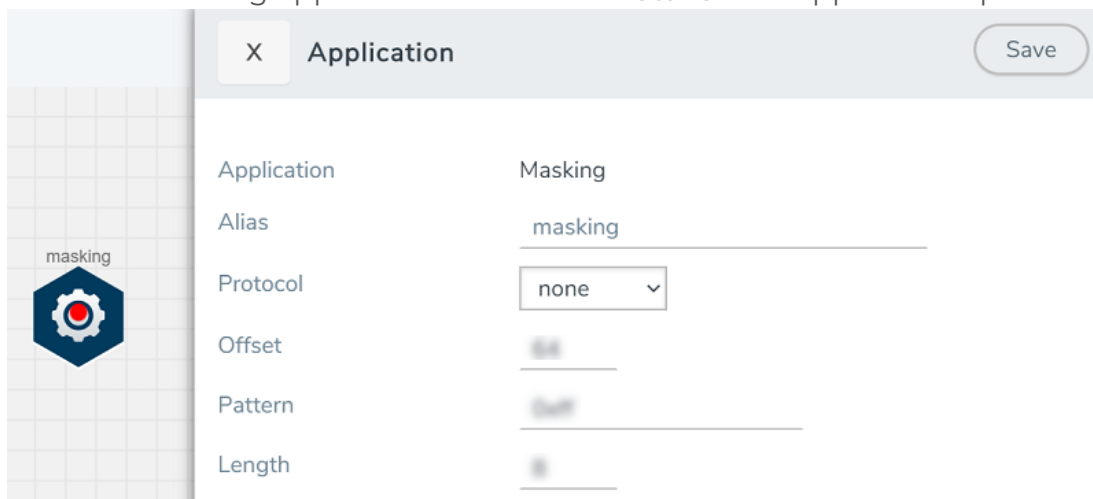
You can view the statistics of the application in the **STATISTICS** tab.

Masking

Masking lets you overwrite specific packet fields with a specified pattern so that sensitive information is protected during network analysis. Masking operations consist of an **offset**, **length**, and **pattern**.

To add a Masking application:

1. Drag and drop **Masking** from **APPLICATIONS** to the graphical workspace.
2. Click the Masking application and select **Details**. The Application quick view appears.



Application	Masking
Alias	masking
Protocol	none
Offset	0
Pattern	0x00
Length	8

3. In the Application quick view, enter the information as follows:

Component	Description
Alias	Enter a name for the application.
Protocol	The following are the protocols that you can select from the protocol drop-down list: - o None – Mask starting a specified number of bytes from the start of the packet. - o IPv4 – Mask starting a specified number of bytes after the IPv4 header. - o IPv6 – Mask starting a specified number of bytes after the IPv6 header. - o UDP – Mask starting a specified number of bytes after the UDP header. - o TCP – Mask starting a specified number of bytes after the TCP header. - o ftp-data – Identify using TCP port 20. Mask payloads using offset from the TCP header. - o HTTPS – Identify using TCP port 443. Mask payloads using offset from the TCP header. - o SSH – Identify using TCP port 22. Mask payloads using offset from the TCP header. - o GTP – Mask starting a specified number of bytes after the outer GTP header. - o GTP-IPv4 – Mask starting a specified number of bytes after the IPv4 header inside the encapsulating GTP packet. - o GTP-UDP – Mask starting a specified number of bytes after the UDP header inside the encapsulating GTP packet. - o GTP-TCP – Mask starting a specified number of bytes after the TCP header inside the encapsulating GTP packet.
Offset	Specifies where the application should start masking data with the supplied pattern. You can specify this in terms of either a static offset from the start of the packet or a relative offset from a particular protocol layer. This lets you automatically compensate for variable length headers, specifying a mask target in terms of a particular packet header.
Length	Specifies how much of the packet should be masked. The specified one-byte pattern can be repeated to mask from 1-9600 bytes.
Pattern	Specifies what pattern the application should use to mask the specified portion of the packet. You can specify a one-byte hex pattern (for example, 0xFF).

4. Click **Save**.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

SSL Decrypt

License: For information on licensing, refer to the *Volume Based License (VBL)* section of respective GigaVUE Cloud Suite Deployment Guide.

SSL Decrypt application delivers decrypted traffic to out-of-band tools that can then detect threats entering the network. Secure Socket Layer (SSL) is a cryptographic protocol that adds security to TCP/IP communications such as Web browsing and email. The protocol allows the transmission of secure data between a server and client who both have the keys to decode the transmission and the certificates to verify trust between them.

SSL encryption secures traffic between a client and a server, such as a Web server. SSL decryption uses keys to decode the traffic between the client and server.

SSL and Transport Layer Security (TLS) protocols consist of a set of messages exchanged between a client and server to set up and tear down the SSL connection between them. To set up the connection, the client and server use the Public Key Infrastructure (PKI) to exchange the bulk encryption keys needed for data transfer.

IMPORTANT: To use SSL Decrypt application in GigaVUE-FM 6.3.00, install new GigaVUE-FM 6.3.00 image. Refer to *GigaVUE-FM Installation and Upgrade Guide* for step-by-step instructions on how to install GigaVUE-FM. SSL Decrypt application does not work if you upgrade from any previous GigaVUE-FM version to GigaVUE-FM 6.3.00.

Keep in mind the following when using SSL Decrypt application:

1. On updating the keys, service, or key maps which are already used in a monitoring session, the monitoring session is dynamically updated, and you need not re-deploy the monitoring session. You can also see if the updated keys, services, or key maps were successfully updated to the monitoring session and the respective GigaVUE V Series Nodes on the **All Events** page. Refer to [Overview of Events](#) section in the *GigaVUE Administration Guide* for detailed information on Events.
2. When deleting a key that is part of a Key Map and that Key Map is used in a monitoring session which is already deployed, then the key will be removed from the Key Map. If that key is the only available entry in the Key Map, then it will not be removed.
3. When deleting a key that is part of a Key Map and that Key Map is used in a monitoring session that is not deployed, then the key will be removed from the Key Map and if that key is the only available entry in the Key Map, the whole key map will be removed from the monitoring session.

4. When deleting a service that is part of a Key Map and that Key Map is used in a monitoring session which is already deployed, then the service will be removed from the Key Map. If that service is the only available entry in the Key Map, then it will not be removed.
5. When deleting a service that is part of a Key Map and that Key Map is used in a monitoring session which is not deployed, then the service will be removed from the Key Map and if that service is the only available entry in the Key Map, the whole key map will be removed from the monitoring session.
6. In VMware NSX-T platform, the throughput of SSL Decrypt application is improved to 480 Mbps.

Refer to the following topics for more detailed information:

- [Supported Protocols, Algorithms, and Ciphers for SSL Decrypt](#)
- [Configure SSL Decrypt](#)

Supported Protocols, Algorithms, and Ciphers for SSL Decrypt

The supported protocols are as follows:

- SSL 3.0
- TLS 1.0
- TLS 1.1
- TLS 1.2

The supported authentication (Au) is as follows:

- RSA

The supported key exchange (Kx) is as follows:

- RSA

The supported encryption algorithms (Enc) are as follows:

- NULL
- RC4
- DES
- 3DES
- AES (including GCM mode)
- CAMELLIA
- SEED
- IDEA

The supported compression algorithm is as follows:

- NULL

The supported digest algorithms are as follows:

- MD5
- SHA1
- SHA2

The supported key sizes are 128, 256, 512, 1024, 2048, and 4096.

The supported TLS extensions are as follows:

- Extended Master Secret, RFC 7627
- Encrypt-then-MAC, RFC 7366

The following table lists the supported ciphers:

Table 1: Supported Ciphers for SSL Decrypt

Cipher Name	Kx	Au	Enc	Bits	Mac
TLS_RSA_WITH_NULL_MD5	RSA	RSA	NULL	0	MD5
TLS_RSA_WITH_NULL_SHA	RSA	RSA	NULL	0	SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5	RSA_EXPORT	RSA_EXPORT	RC4_40	40	MD5
TLS_RSA_WITH_RC4_128_MD5	RSA	RSA	RC4_128	128	MD5
TLS_RSA_WITH_RC4_128_SHA	RSA	RSA	RC4_128	128	SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	RSA_EXPORT	RSA_EXPORT	RC2_CBC_40	40	MD5
TLS_RSA_WITH_IDEA_CBC_SHA	RSA	RSA	IDEA_CBC	128	SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA_EXPORT	RSA_EXPORT	DES40_CBC	40	SHA
TLS_RSA_WITH_DES_CBC_SHA	RSA	RSA	DES_CBC	56	SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	RSA	3DES_EDE_CBC	168	SHA
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES_128_CBC	128	SHA
TLS_RSA_WITH_AES_256_CBC_SHA	RSA	RSA	AES_256_CBC	256	SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	RSA	RSA	CAMELLIA_128_CBC	128	SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	RSA	RSA	CAMELLIA_256_CBC	256	SHA
TLS_RSA_WITH_SEED_CBC_SHA	RSA	RSA	SEED_CBC	128	SHA

Cipher Name	Kx	Au	Enc	Bits	Mac
TLS_RSA_WITH_NULL_SHA256	RSA	RSA	NULL	0	SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA	RSA	AES_128_CBC	128	SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA	RSA	AES_256_CBC	256	SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256	RSA	RSA	AES_128_GCM	128	SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	RSA	RSA	AES_256_GCM	256	SHA384

All algorithms used for SSL Decrypt application are FIPS 140-3 compliant.

All key URLs must point to an RSA private key stored in the PEM or PKCS12 format, as follows:

- <http://keyserver.domain.com/path/keyfile.pem>
- <https://keyserver.domain.com/path/keyfile.pem>
- <ftp://keyserver.domain.com/path/keyfile.pem>
- <tftp://keyserver.domain.com/path/keyfile.pem>
- [scp://username\[:password\]@keyserver.domain.com/path/keyfile.pem](scp://username[:password]@keyserver.domain.com/path/keyfile.pem)

The supported applications are as follows:

- HTTPS
- FTPS
- SMTP, IMAP, and POP3 with StartTLS

Configure SSL Decrypt

To configure SSL Decrypt Application using GigaVUE-FM follow the steps given below:

- [Upload SSL Key Pairs](#)
- [Create SSL Service](#)
- [Key Mapping](#)
- [SSL Key Pair Store](#)
- [Add SSL Decrypt to Monitoring Session](#)

Upload SSL Key Pairs

To upload an SSL private key, do the following:

1. Go to **Inventory > Resources > Security > SSL Keys**.
2. Click **Add**. The **Create SSL Key Pair** page appears.
3. Enter the following details:

Field	Description
Key Alias	Enter a name for the key.
Comment	Enter a description
Key Type	Select the either of the key type:
PEM	
PassPhrase (optional)	SSH passphrases allows you to protect your private key from being used with out the passphrase. Enter the passphrase created with the private key.
SSL Key Store	Enter the SSL Key Pair Store in which the Key is stored.
Private key	Enter the Private Key using any of the following options: • Copy and Paste • Install from URL • Install from Local Directory
Certificate	Enter the Certificate using any of the following options: • Copy and Paste • Install from URL • Install from Local Directory
PKCS12	
PassPhrase	SSH passphrases allows you to protect your private key from being used with out the passphrase. Enter the passphrase created with the private key.
SSL Key Store	Enter the SSL Key Pair Store in which the Key is stored.

4. Click **Save**.

NOTE: SSL Decrypt application does not support HSM.

The following actions can also be performed from the SSL Key Pairs Page:

Field	Description
Edit	To edit a SSL Key pair, select the key from the list in the SSL Key Pairs page and click the Edit button.
Delete	To delete a SSL Key pair, select the key from the list in the SSL Key pairs page and click the Delete button.
Delete all	Use this button to delete all the SSL Key pairs in the SSL Key pairs page.
View certificate	To view the certificate associated with the particular SSL Key Pair, select the key from the list in the SSL Key Pairs page and click the View Certificate button.

Create SSL Service

After uploading a private key, you can add a service. A service maps to a physical server, such as an HTTP server. One server can run multiple services. A service is a combination of an IP address and a server port number.

Prerequisite

Before creating a service, upload a private key as described in [Upload SSL Key Pairs](#)

To create a SSL service, do the following:

1. Go to **Inventory > Resources > Security > SSL Service**. The SSL Services page appears.
2. Click **Add**. The **Create SSL Service** page appears.
3. On the Create SSL Service page, enter the following details:

Field	Description
Alias	Enter a name for the SSL Service.
Default Service	Enable this to use default service.
Server IP Address	Enter the IP address of the server in which the service runs.
Server Port	Enter the port number of the server.

4. Click **Save**.

The following actions can also be performed from the SSL Service Page:

Field	Description
Edit	To edit a SSL Service, select the service from the list in the SSL Service page and click the Edit button.
Delete	To delete a SSL Service, select the service from the list in the SSL Service page and click the Delete button.
Delete all	Use this button to delete all the SSL Service in the SSL Service page.

Key Mapping

After adding the SSL Service, now you map the private key with the service using Key Mapping.

To map a key with the service, follow the steps given below,

1. Go to **Inventory > Resources > Security > SSL Key Mapping**. The SSL Key Pair Mapping page appears.
2. Click **Add**.

3. Enter the Key Mapping Alias.
4. Select the SSL Service and Key Alias from the drop-down.
5. Click **Save**.

The following actions can also be performed from the SSL Key Pairs Page:

Field	Description
Edit	To edit a SSL Service, select the service from the list in the SSL Service page and click the Edit button.
Delete	To delete a SSL Service, select the service from the list in the SSL Service page and click the Delete button.
Delete all	Use this button to delete all the SSL Service in the SSL Service page.

SSL Key Pair Store

SSL Key Pair Store is a repository, that allows you to save all the key under a single location. You can create multiple key stores and in each key store you can store multiple keys.

1. Go to **Inventory > Resources > Security > SSL Key Store**. The SSL Key Pair Store page appears.
2. Click **Add**.
3. Enter the **Key Store Alias** and **Comment**.
4. Click **Save**.

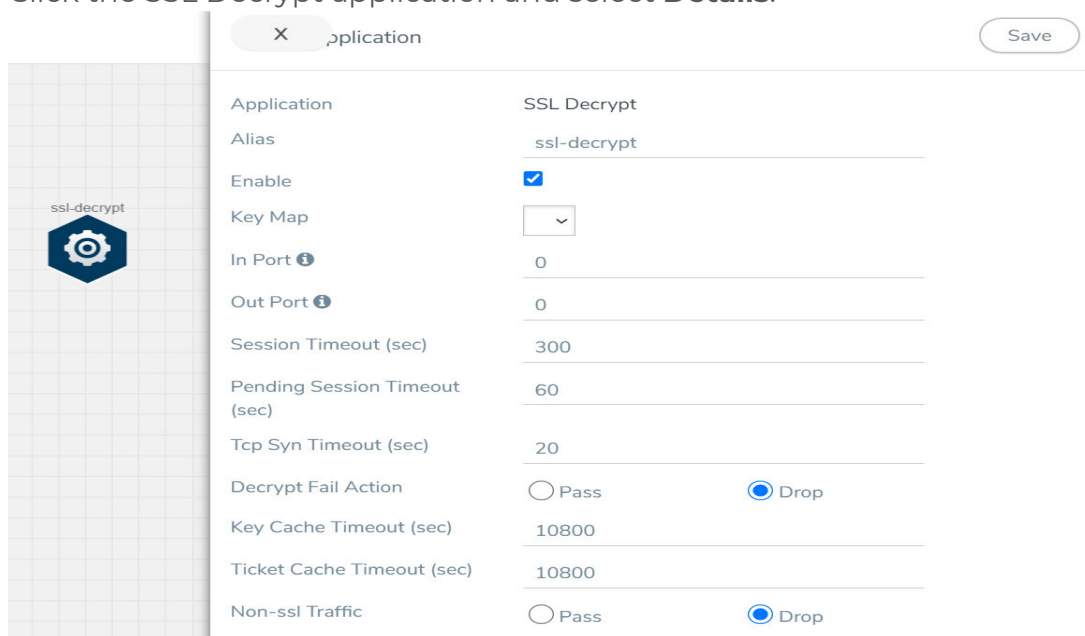
The following actions can also be performed from the SSL Key Pair Store Page:

Field	Description
Edit	To edit a SSL Key pair Store, select the Key Store from the list in the SSL Key Pair Store page and click the Edit button.
Delete	To delete a SSL Key Pair Store, select the SSL Key Pair Store from the list in the SSL Key Pair Store page and click the Delete button.
Delete all	Use this button to delete all the SSL Key Pair Store in the SSL Key Pair Store page.

Add SSL Decrypt to Monitoring Session

After mapping your keys with service, to add GigaSMART applications to GigaVUE V Series Node, follow the steps given below,

1. Drag and drop **SSL Decrypt** from APPLICATIONS to the graphical workspace.
2. Click the SSL Decrypt application and select **Details**.



Application configuration window for SSL Decrypt. The window includes a 'Save' button and a list of configuration parameters.

Application	SSL Decrypt
Alias	ssl-decrypt
Enable	☒
Key Map	v
In Port ⓘ	0
Out Port ⓘ	0
Session Timeout (sec)	300
Pending Session Timeout (sec)	60
Tcp Syn Timeout (sec)	20
Decrypt Fail Action	☐ Pass ☒ Drop
Key Cache Timeout (sec)	10800
Ticket Cache Timeout (sec)	10800
Non-ssl Traffic	☐ Pass ☒ Drop

3. Enter the following details in the Application quick view:

Fields	Description
Alias	Enter the alias name for the application.
Enable	Enable the box to enable SSL Decryption.
Key Map	Select the Key Map from the list of available Key Maps. Refer to Key Mapping for more details on how to map the key to SSL Service.
In Port	Enter the source port number from which the traffic should be fetched.
Out Port	Enter the destination port number to which the decrypted traffic should be delivered.
Session Timeout	Enter the value in seconds after which the session should be timeout. The default value is 300 seconds.
Pending Session Timeout	Enter the value in seconds after which the session must timeout if the session is in pending state
Tcp Syn Timeout	Enter the value in seconds after which the session must timeout when the session does not synchronize TCP.
Decrypt Fail Action	Select Pass to allow the traffic to pass through the application when the decryption fails and select Drop to drop the traffic before passing through the application when the decryption fails.
Key Cache Timeout (sec)	Enter the value in seconds until which the key cache information can be reused for resumption.
Ticket Cache Timeout (sec)	Enter the value in seconds until which the ticket cache information can be reused for resumption.
Non-ssl Traffic	Select Pass to allow the non-SSL traffic to pass through the application and select Drop to drop the non- SSL traffic before passing through the application.

4. Click **Save**.
5. Click **Deploy**. The Select nodes to deploy the monitoring session page appears.
6. Select the GigaVUE V Series Nodes you want to deploy and select an interface for each GigaVUE V Series Node. Then, click **Deploy**.

PCAPng Application

The PCAPng application reads the various blocks in the received PCAPng files and validates the blocks to be sent to the destination application or to the tools. The PCAPng file contains the following blocks:

- Mandatory Blocks
 - Section Header Block (SHB)
- Optional Blocks
 - Interface Description Block (IDB)
 - Enhanced Packet Block (EPB)
 - Simple Packet Block
 - Name Resolution Block
 - Interface Statistics Block

The actual packets are present in the Enhanced Packet Block. The block data is parsed to find the start and end offset of the valid packets and the packet is sent out to the next application.

NOTE: Only one EPB in a PCAPng file is supported.

The PCAPng application processes the data depending on the packet type that contains a combination of the blocks mentioned above:

Block Combination	Process
SHB+IDB+EPB+data	Packets are parsed, validated, and the data packet is sent out.
SHB+IDB	Packets are dropped.
EPB+Data	Packets are parsed, validated, and the data packet is sent out.

The PCAPng application validates if the incoming data matches any of the above three formats in the same order, and processes the packets accordingly.

The following figure shows a sample PCAPng file format that contains one section header block:

Create Link Between UDP-in-GRE Tunnel and PCAPng Application

To create a link with source as UDP-in-GRE tunnel and destination as PCAPng application:

1. In the GigaVUE-FM canvas, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.
2. On the New Tunnel quick view, enter or select the required information as described in the following table.

Field	Description
Alias	The name of the tunnel endpoint Note: Do not enter spaces in the alias name.
Description	The description of the tunnel endpoint
Type	Select UDPGRE as the tunnel type
Traffic Direction	The direction of the traffic flowing through the V Series node • Choose In (Decapsulation) for creating an Ingress tunnel, traffic from the source to the V Series node
IP Version	The version of the Internet Protocol. Select IPv4 or IPv6
Remote Tunnel IP	The IP address of the tunnel source
Key	GRE key value
Source L4 Port	Layer 4 source port number
Destination L4 Port	Layer 4 destination port number. You can configure only 4754 or 4755 as the destination UDP ports

3. Click **Save**.
4. Click and drag the PCAPng application into the canvas. Configure the alias for the application.
5. Select the App mode from the available options Primary or Secondary. Refer to for details.
6. Establish a link between the UDP-GRE TEP configured above and the PCAPng application.

Create Link Between PCAPng Application and Other Destinations

Create a link with source as PCAPng application and destination as one of the following:

- Other GigaSMART applications such as Slicing, Masking, etc.
- Other encapsulation TEPs.
- REP/MAP

Ericsson vTAP Domain Tagging Support

The PCAPng application now supports Ericsson vTAP domain tagging. It reads PCAPNG payloads carried in vTAP GRE-in-UDP tunnels and identifies the Ericsson domain. Refer to [5G-Service Based Interface Application](#) for more details.

When you enable domain classification, the PCAPng application:

- Detects Ericsson vTAP PCAPNG payloads using the vTAP GRE key.
- Classifies packets into domains. (For Example: pc-mm, pc-sm, ccsn-5gc..etc)
- Applies VLAN tags on egress using the Domain VLAN Mapping table. Each domain maps to one VLAN ID, and you can also set a separate VLAN ID for failed SBI transactions. Supported VLAN IDs range from 1 to 4094.
- If the application cannot classify a packet (for example, because metadata is missing), it uses the VLAN ID you configure for unclassified or failed traffic.

Configure the PCAPng Application for Domain Tagging

1. In the canvas, drag and drop the PCAPng application and select **Details**. The PCAPng application quick view appears.
2. On the application quick view, enter or select the required information as described in the following table:

Field	Description
Application	The name Pcapng appears by default.
Alias	Enter an Alias as required.
App Mode	Set App Mode to Primary to view and configure domain related options. NOTE: Primary mode is required to configure domain classification. When you set App Mode to Secondary, Domain Classification, Domain VLAN Mapping, and Flow Timeout fields are not visible.
Domain Classification	Enable the Domain Classification option to classify Ericsson vTAP traffic by domain.
Domain VLAN Mapping	• From the Domain VLAN Mapping list, select the VLAN mapping profile that maps Ericsson domains to VLAN IDs for per-domain tagging on the egress tunnel. • Click Add New to create a new 5G-Apps configuration. Refer to Adding CSV file for IP Mapping section in 5G-Service Based Interface Application for details. When Domain Classification is enabled, the selected Domain VLAN Mapping is used to tag packets per Ericsson domain with the configured VLAN ID (and, if applicable, a separate VLAN ID for failed SBI transactions) before sending traffic to the probes. NOTE: If duplicate entries are detected during mapping table upload, a validation error is displayed.
Flow Timeout	Set the Flow Timeout value in seconds to define how long an inactive Ericsson vTAP flow is kept before it is closed and its resources are released. Valid range: 360-1860 Default value: 660

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

5G-Service Based Interface Application

The 5G-Service Based Interface (5G-SBI) application synthesizes HTTP2 transactions with proper L2, L3, and L4 headers from JSON-encoded data received from Ericsson vTAPs via UDP-GRE. The 5G-SBI application takes the raw encoded data that monitoring tools cannot understand and reconstructs complete, tool-facing packets with valid TCP flows.

The 5G-SBI application operates on a DPDK-based V Series Node and supports the following traffic types:

- **SBI traffic (L7-JSON)** - AMF, SMF signaling from Ericsson PCC vTAPs (key value 1). The 5G-SBI application synthesizes this traffic into HTTP2 packets.
- **Non-SBI traffic** - PSVP, GTPC, Diameter, and other protocols from Ericsson PCC vTAPs (key values 5, 7, 9, 11, 15, 21, 23). The PCAPng application reads the data from the Enhanced Packet Block and forwards it directly to the egress tunnel without synthesis.

Ericsson vTAP

Ericsson virtual TAPs (vTAPs) mirror traffic from 5G Core network functions. Each network function module has its own vTAP. Ericsson PCC (Packet Core Controller) contains vTAPs for AMF, SMF, and other protocols. Ericsson CCx (Cloud Core) contains vTAPs for SCP traffic.

Each vTAP assigns a key value to identify the protocol type. The vTAP wraps the mirrored packet in PCAPng format (Enhanced Packet Block) and sends it over a UDP-GRE tunnel to the GigaVUE V Series Node.

The following table lists the Ericsson vTAP key values and their corresponding traffic types:

Key Value	Traffic Type	Category
0,2	Metadata (domain classification)	Control
1	AMF, SMF	SBI (L7-JSON)
3, 17, 19	SCP protocols	SBI (L7-Native)
5, 7, 9, 11, 15, 21, 23	PSVP, GTPC, Diameter	Non-SBI

NOTE: Key values 0 and 2 carry domain metadata only. This traffic is processed by the PCAPng application in Primary mode to identify which flow belongs to which domain. This traffic does not go to monitoring probes.

Ericsson vTAP Domain Tagging

Ericsson vTAP components mirror control plane and selected user plane traffic, for example, from Ericsson PCC nodes, and send it to the GigaVUE V Series using UDP-GRE with PCAPng/JSON metadata. Previously, the 5G-SBI application treated all mirrored flows uniformly, requiring monitoring tools to independently infer the Ericsson domain (for example, pc-mm, pc-sm, sc-scp) and the associated 3GPP interface.

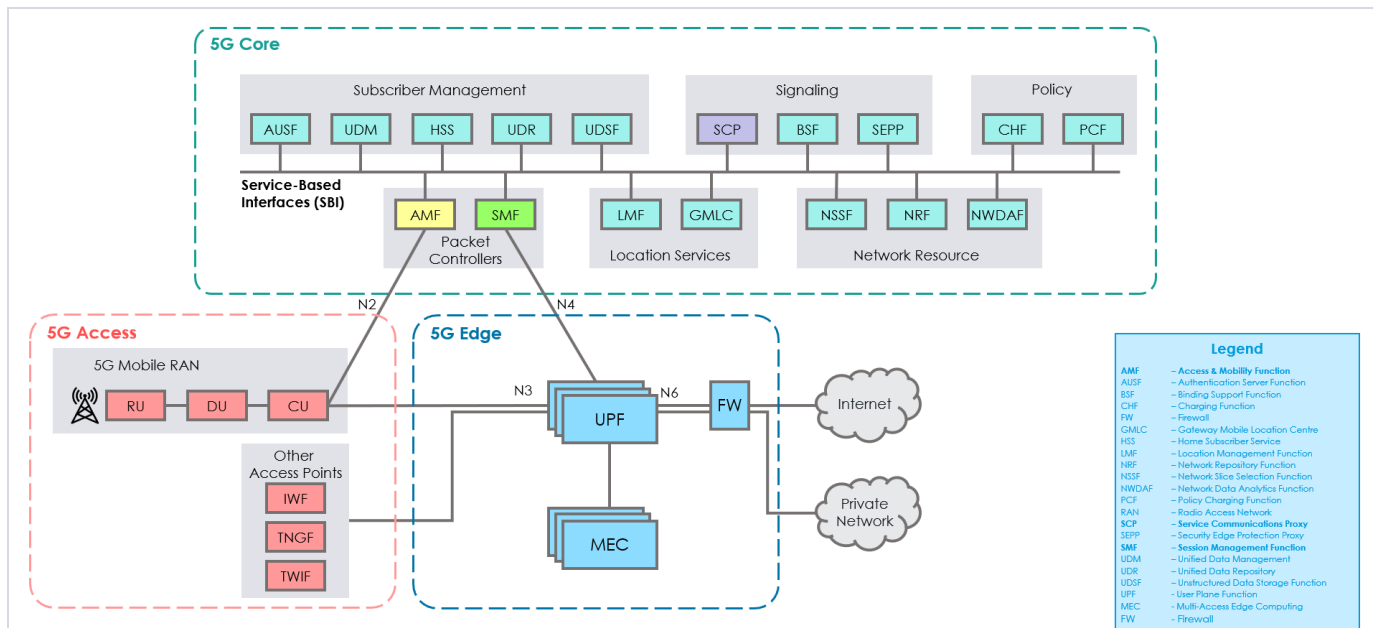
With Domain Tagging, the PCAPng application on V Series reads the Ericsson vTAP metadata, identifies the Ericsson domain for each flow, and assigns a VLAN ID based on a configurable domain to VLAN map. When you enable domain classification in the PCAPNG app and VLAN tagging on the VXLAN or L2GRE egress tunnel, V Series tags each packet with the appropriate VLAN so probes can separate domains simply by filtering on VLAN.

You can also reserve VLANs for:

- Traffic mapped to the **others** domain (for example, unsupported or unexpected Ericsson domains)
- Traffic mapped to the **unclassified** domain (for example, traffic for which domain information is not yet available)

Encoded messages from the Ericsson vTAP contain Kubernetes Pod ephemeral IP addresses for NF instances, which are internal to the Ericsson deployment and not accessible outside the Kubernetes cluster. Because these IPs cannot be used externally, the 5G SBI application always maps the NF identifiers (NF instance ID and FQDN) in the encoded message to the configured ingress IP address using the string-to-IP mapping table.

The NF instance ID and FQDN ID must be provided in the form of CSV file. You can upload the CSV file through GigaVUE-FM.



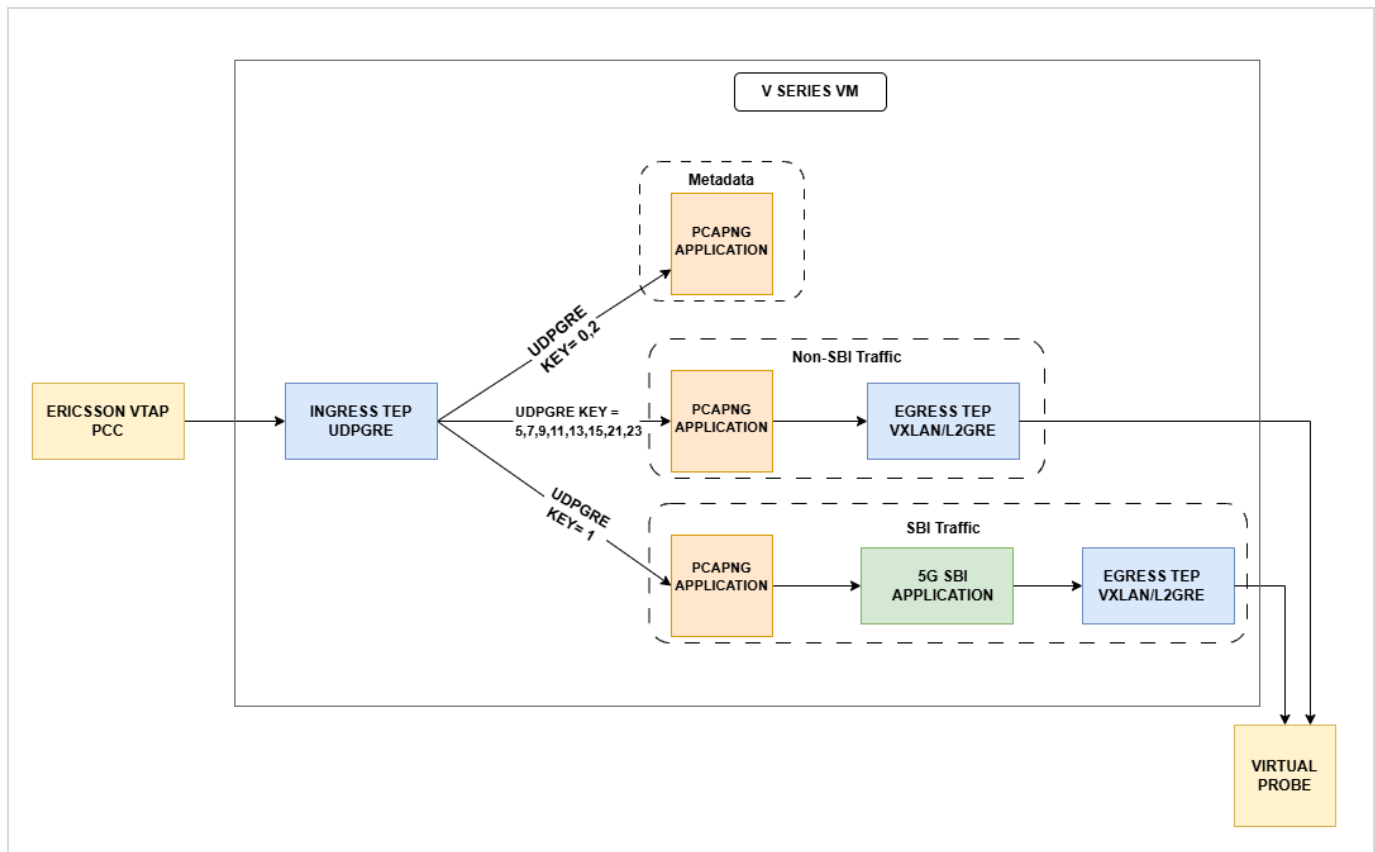
How SBI Application works

In the GigaVUE V Series Node, the SBI application receives the HTTP2 transaction messages as JSON encoded data from the PCAPng application, which in turn receives the data from the UDP-GRE TEP.

The SBI application:

1. Parses the JSON data to extract source and destination information, ports, and message type (request/response).
2. Synthesizes a complete HTTP/2 transaction with L2, L3, and L4 headers, along with the HTTP/2 headers and body from the original transactions.
3. Sends the synthesized packets to the egress TEP, which forwards them to the appropriate virtual probes.

The following image shows the block diagram of the data flow in the V Series Node containing the SBI application.



Supported Platforms:

The application is supported on the following platforms:

- VMware ESXi
- OpenStack
- Third Party Orchestration

Rules and Notes

- The maximum number of HTTP2 headers (in the synthesized HTTP2 transactions) that is supported is 64.
- The PCAPng application that is linked to 5G-SBI application (on the right side) should only be linked to UDP-GRE TEP with key value 1 on the left side. If it is linked to other UDP-GRE TEPs (key values other than 1), then the behavior cannot be defined and leads to unexpected results.
- The maximum number of NF and FQDN entries supported is 4K.
- In 5G-SBI application, the V Series node can log the following details to CSV files:
 - **Transaction details** - Represents the transaction or flow of request and response packets into the application. The details of the flow or transaction are recorded in the CSV file for 5 minutes or 60 minutes based on the configuration.

- **Flow statistics details** - Represents the packet and flow statistics in 60 seconds time interval.

These files help you to understand the records and traffic efficiently. The files are named as per the date and time in which the files were created. When the number and size of files grow, the application automatically detects the old files and deletes them.

- Ericsson vTAP domain tagging can be configured only in primary mode when configuring Pcapng application. Refer to [5G-Service Based Interface Application](#).

5G-Ericsson vTAP Packet Processing (5G-EVP)

The 5G-Ericsson vTAP Packet Processing (5G-EVP) application orders packets received from Ericsson vTAP sources and optionally decrypts DTLS(Datagram Transport Layer Security)-encrypted traffic before forwarding it to the downstream 5G-SBI and 5G-Cloud applications.

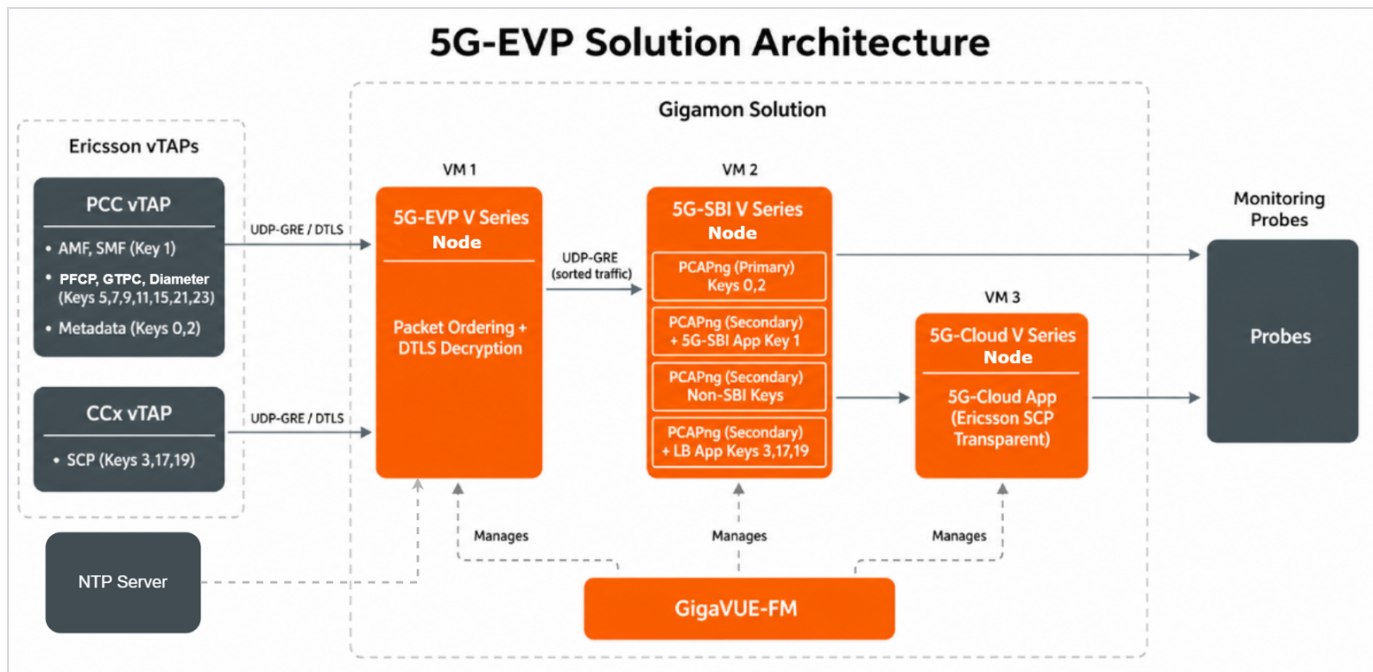
When multiple Ericsson vTAPs send traffic simultaneously, packets can arrive at the V Series Node out of order. Out-of-order packets can prevent monitoring probes from building session tables correctly, resulting in lost traffic visibility. The 5G-EVP application addresses this by ordering packets based on the timestamp at which each packet was originally observed on the network, ensuring that downstream applications and monitoring probes receive traffic in the correct sequence.

The 5G-EVP application runs on a dedicated V Series Node and sits in front of the existing 5G-SBI and 5G-Cloud nodes. It does not modify or replace those applications.

NOTE: The 5G-SBI and 5G-Cloud applications can operate without the 5G-EVP application. If packet ordering is not required, use the existing two-node deployment. However, the 5G-EVP application requires a downstream 5G-SBI or 5G-Cloud application to function.

Solution Architecture

The complete Ericsson vTAP solution with the 5G-EVP application uses three V Series Nodes managed by GigaVUE-FM. Each V Series Node requires a separate Monitoring Domain and a separate Monitoring Session.



V Series Apps	GigaVUE-FM
5G-EVP V Series Node	Orders packets from Ericsson vTAPs based on embedded timestamps and forwards ordered traffic to the downstream V Series Nodes over UDP-GRE. Optionally decrypts DTLS-encrypted traffic.
5G-SBI V Series Node	SBI and Non-SBI pipeline: Processes SBI (L7-JSON) traffic through the 5G-SBI application for synthesis. Forwards non-SBI traffic directly to egress tunnels. SCP pipeline: Distributes SCP (L7-Native) traffic through the LB application to multi-tap egress tunnels for downstream processing by the 5G-Cloud Node.
5G-Cloud V Series Node	Processes SBI (L7-Native) traffic from Ericsson SCP using the 5G-Cloud application.
GigaVUE-FM	Configures and monitors all three V Series Nodes. Manages NTP server configuration for the 5G-EVP Node.

Recommended VM Specifications

V Series Node	vCPUs	Memory	Disk Space
5G-EVP	20	32 GB	80 GB
5G-SBI	8	16 GB	80 GB
5G-Cloud	24	32 GB	80 GB

Recommended VM Specifications (DTLS)

V Series Node	vCPUs	Memory	Disk Space
5G-EVP	32	32 GB	80 GB
5G-SBI	8	16 GB	80 GB
5G-Cloud	24	32 GB	80 GB

Supported Deployment Combinations

The following table lists the supported deployment combinations. SBI and non-SBI traffic always coexist on the same 5G-SBI monitoring session. SCP traffic can be deployed independently or alongside SBI/non-SBI traffic.

Combination	Monitoring Sessions Required
SBI + Non-SBI traffic	EVP + 5G-SBI
SCP traffic	EVP + LB App + Multi-TEP VM + 5G-Cloud
SBI + Non-SBI + SCP	EVP + 5G-SBI + 5G-Cloud

Supported Platforms

- VMware ESXi (FM orchestration and third-party orchestration)
- OpenStack (FM orchestration and third-party orchestration)

Licensing

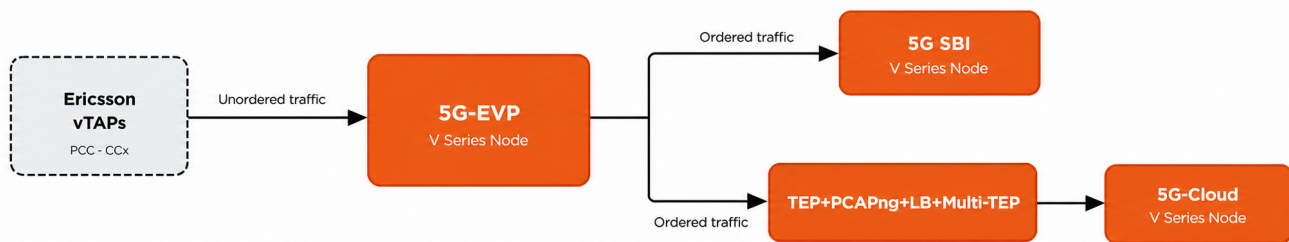
No new license is required. The 5G-EVP application is included in the existing V Series 5GC add-on license.

Overview of Packet Ordering

When multiple Ericsson vTAPs send traffic simultaneously, packets can arrive at the V Series Node out of order. Out-of-order packets can prevent monitoring probes from building session tables correctly, resulting in lost traffic visibility.

The 5G-EVP application orders packets based on the timestamp at which each packet was originally observed on the network. The application maintains a configurable time window and uses this window to hold incoming packets, order them by observed timestamp, and forward them in the correct sequence to the downstream 5G-SBI or 5G-Cloud Node.

Packets that arrive with timestamps outside the current ordering window are handled based on the configured policy.



NOTE: The maximum sorting window is 100 ms ($\text{numBuckets} \times \text{bucketInterval}$ must not exceed 100). The application validates this constraint and returns an error if the values exceed the limit.

DTLS Support

Ericsson can send vTAP traffic over DTLS (Datagram Transport Layer Security) for encrypted delivery. When you enable DTLS on the 5G-EVP application:

- Ericsson sends encrypted traffic on UDP port 4755 (instead of 4754 for non-secure traffic).
- The 5G-EVP application decrypts the traffic using the configured private key and certificate.
- The application forwards cleartext packets to the downstream 5G-SBI application over UDP-GRE on port 4754. The downstream applications see no difference.

Supported Modes

NOTE: You cannot disable both packet ordering and DTLS simultaneously. At least one must be enabled for the 5G-EVP application to function.

NTP Time Synchronization

The 5G-EVP application requires NTP time synchronization to maintain accurate clock alignment for packet ordering. When you enable packet ordering, the Primary NTP Server and Secondary NTP Server fields appear in the 5G-EVP application configuration.

GigaVUE-FM sends the NTP server configuration to the V Series Node during each deployment.

- If NTP synchronization fails after deployment, the 5G-EVP application health is impacted and GigaVUE-FM generates an event.
- If the chronyd configuration fails during deployment, GigaVUE-FM still proceeds with the deployment. However, packet ordering accuracy may be affected.

NOTE: The deployment may take additional time to complete due to NTP synchronization. Allow sufficient time for the NTP configuration to take effect before verifying application health.

Multiple Egress IP Addresses

When the 5G-EVP application forwards traffic to a downstream V Series Node using a single source IP, all traffic hashes to a single CPU core on the downstream node. To distribute traffic evenly across cores, configure up to 8 source IP addresses in the 5G-EVP egress tunnel. The application internally creates multiple tuples using these IPs and port combinations. Each flow always maps to a single tuple, which preserves per-flow ordering.

You must configure the additional IP addresses in NetPlan on the 5G-EVP VM before specifying them in the application configuration. Refer to [Configuring Multiple Egress IP Addresses](#).

Rules and Notes

- The 5G-EVP application operates on a dedicated V Series Node. Do not deploy it on the same node as the 5G-SBI or 5G-Cloud applications.
- A maximum of 8 source IP addresses can be configured for the 5G-EVP egress tunnel.
- The ordering window (Number of Buckets × Bucket Interval) must not exceed 100 ms.
- The Ingress REP and Egress REP on the 5G-EVP and 5G-Cloud monitoring session canvases are placeholder elements, they do not require configuration.
- Only one PCAPng application instance can be set to Primary mode per monitoring session. Any instance can be designated as Primary, it is not tied to specific key values.
- The 5G-SBI and 5G-Cloud applications can operate without the 5G-EVP application, but the 5G-EVP application cannot operate without a downstream 5G-SBI or 5G-Cloud application.
- Domain Tagging can coexist with packet ordering. There are no limitations on using both features together.

PCAPNG Processing and Flow Tracking

In this Ericsson vTAP design, PCAPng classifies flows by Ericsson domain and inserts the corresponding VLAN tag on the egress traffic.

The PCAPNG application on the V Series serves as the configuration point for Ericsson domain classification and VLAN mapping (app mode, domainClassification, flowTimeout, and domainTable). The 5G SBI application performs the actual parsing of Ericsson vTAP metadata, flow and domain determination, and SBI failure detection. The dataplane and egress tunnel configuration apply the VLAN tags and forward the traffic.

NOTE: In the PCAPng configuration, the Domain VLAN Mapping and Flow Timeout fields are displayed only when App Mode is set to Primary and the Domain Classification check box is enabled.

Egress Tunnels and VLAN Tag Insertion

When the V Series classifies Ericsson vTAP traffic by domain in the PCAPNG application, it forwards packets to the probes through egress tunnels (VXLAN or L2GRE).

When creating an Egress tunnel in the Monitoring Session Canvas, enable the **Domain Tagging** option to tag packets on the egress tunnel with the Ericsson domain-specific VLAN IDs derived from the PCAPng Domain VLAN Mapping.

NOTE: This setting is available only when **Domain Classification** is enabled in the associated PCAPng application. Refer to [5G-Service Based Interface Application](#) for details.

When **Domain Classification** is enabled in the PCAPNG app and **Domain Tagging** is enabled on the egress tunnel, the V Series does the following:

- Looks up the Ericsson domain for each packet.
- Maps it to a VLAN ID from the Domain Table (including any failed SBI or special case VLANs)
- Inserts that VLAN tag on the egress packet

This ensures each probe interface only receives the Ericsson domains it is configured to monitor.



Notes:

- After you deploy a Monitoring Session, you cannot edit its associated 5G SBI or PCAPNG application configurations. To modify them, undeploy the Monitoring Session, update the configuration, and redeploy.
- If a PCAPNG application instance is set as the Primary for a Monitoring Session, you cannot delete it while it holds that role. To delete or replace it, undeploy the Monitoring Session or reassign the Primary.

End-to End Solution Overview and Configuration:

For end-to-end configuration workflows, refer to the scenario-specific pages based on your deployment:

- [Configure PCC vTAP Traffic Flow](#) - SBI (L7-JSON) and non-SBI traffic from Ericsson PCC vTAPs. This is the most common deployment.
- [Configure CCx vTAP Traffic Flow](#) - SCP (L7-Native) traffic from Ericsson CCx vTAPs. Can be deployed independently or alongside SBI traffic.

For a full deployment that includes all traffic types, combine the SBI and SCP workflows into a single monitoring session on the 5G-SBI Node.

Upgrade and Migration

If you have an existing 5G-SBI and 5G-Cloud deployment, you can add the 5G-EVP application by inserting a new EVP Node between the Ericsson vTAPs and the 5G-SBI Node.

When you add the EVP Node, re-assign the ingress IP address from the 5G-SBI Node to the EVP Node. This ensures that the vTAPs send traffic to the EVP Node without requiring reconfiguration on the Ericsson side. Provision new IP addresses to connect the EVP egress to the 5G-SBI ingress. Both interfaces must be in the same subnet.

The 5G-SBI to 5G-Cloud pipeline remains unchanged during migration.

For step-by-step instructions, refer to the Upgrade and Migration Steps in [Configure PCC vTAP Traffic Flow](#) or [Configure CCx vTAP Traffic Flow](#).

NOTE: If the existing deployment has a source IP configured in the tunnel endpoint (TEP) configuration, remove it before deploying the EVP application.

Configure PCC Traffic Flow

This deployment scenario applies when your environment includes traffic from Ericsson PCC (Packet Core Controller) vTAPs. The Ericsson PCC sends SBI traffic (L7-JSON) and non-SBI traffic simultaneously through its vTAPs, these two traffic types always coexist on the same monitoring session. This is the most common deployment.

The 5G-EVP application receives all PCC traffic, reorders packets based on the embedded observed timestamp, and forwards sorted traffic to the 5G-SBI Node over UDP-GRE. On the 5G-SBI Node, the monitoring session processes traffic through three parallel paths:

Metadata (keys 0, 2) -The PCAPng application processes metadata for domain classification. This traffic stays internal and does not reach monitoring probes.

SBI traffic (key 1) - The PCAPng application processes the traffic and passes it to the 5G-SBI application. The processed traffic is forwarded to the egress tunnel.

Non-SBI traffic (keys 5, 7, 9, 11, 15, 21, 23) The PCAPng application processes the traffic and forwards it directly to the egress tunnel.

Monitoring Sessions Required

Monitoring Session	V Series Node	Traffic Handled
5G-EVP Monitoring Session	5G-EVP	All PCC traffic, packet ordering and optional DTLS decryption
5G-SBI Monitoring Session	5G-SBI	SBI (key 1) + Non-SBI (keys 5,7,9,11,15,21,23) + Metadata (keys 0,2)
5G-Cloud Monitoring Session	5G-Cloud	SCP synthesis (if applicable)

Prerequisites

Before you begin, complete the following:

- Deploy three V Series Nodes: 5G-EVP , 5G-SBI, and 5G-Cloud.
- If you plan to use multiple egress IPs on the 5G-EVP Node, configure the additional IP addresses in NetPlan on the VM. Refer to Configuring Multiple Egress IP Addresses.
- Create a separate monitoring domain for each V Series Node in GigaVUE-FM.
- Verify that the V Series 5GC add-on license is active.
- Configure NTP servers for the 5G-EVP Node (required when packet ordering is enabled).
- If you plan to use DTLS, upload the private key and certificate in GigaVUE-FM via Inventory > Security > SSL Key.

End to End Configuration

Monitoring Session 1: 5G-EVP

Create this monitoring session on the 5G-EVP V Series Node.

1. In GigaVUE-FM, go to the monitoring domain for the 5G-EVP V Series Node.
2. **Create** a new monitoring session.
3. Configure Multiple Egress IP Addresses.

To distribute traffic evenly from the 5G-EVP Node to the downstream V Series Node, configure multiple source IP addresses on the 5G-EVP VM.

- a. Log in to the 5G-EVP V Series Node via SSH.
- b. Create a new NetPlan configuration file with a higher index value:

```
sudo vi /etc/netplan/02-netcfg.yaml
```

- c. Add the additional IP addresses to the egress network interface.
- d. Save and close the file.
- e. Apply the NetPlan configuration:

```
sudo netplan apply
```

- f. Verify the IP addresses are configured:

```
addr show <iface name>
```

- g. In GigaVUE-FM, navigate to the 5G-EVP monitoring session.
- h. Select the 5G-EVP application and click Details.
- i. In the Egress UDP Tunnel section, enter all the configured IP addresses in the Tx Source IP Address field.
- j. From the Actions menu, select Deploy to redeploy the monitoring session.

NOTE: Configure the IP addresses in NetPlan before entering them in GigaVUE-FM. If the IP addresses do not exist on the VM, the egress tunnel fails to initialize. A maximum of 8 source IP addresses can be configured.

4. On the canvas, drag and drop an **Ingress REP**.
5. Drag and drop the **5G-EVP** application. Select **Details** and configure the Ingress UDP Tunnel, Egress UDP Tunnel, Packet Ordering Configuration, Diagnostics, and Logging sections.

Configure 5G-EVP Application

To configure the 5G-EVP application, drag and drop it onto the monitoring session canvas and select Details. The 5G-EVP application quick view appears. Enter or select the required information as described in the following tables.

Field	Description
Application	The name 5g-EVP appears by default.
Alias	Enter the alias name as 5gEVP .
Packet Ordering Config	
Packet Ordering	Toggle to enable or disable timestamp-based packet reordering. When enabled, the 5G-EVP application sorts packets based on the observed timestamp in the PCAPng Enhanced Packet Block before forwarding them to the downstream application.
Primary NTP Server*	Enter the IP address (IPv4 or IPv6) of the primary NTP server. The 5G-EVP application requires NTP time synchronization through chronyd for millisecond-accurate clock alignment. GigaVUE-FM sends this configuration to the V Series Node during each deployment. This field is mandatory when packet ordering is enabled. NOTE: Visible when Packet Ordering is enabled.
Secondary NTP Server	Enter the IP address (IPv4 or IPv6) of the secondary NTP server. This field is optional. The secondary NTP server provides failover if the primary NTP server becomes unreachable. NOTE: Visible when Packet Ordering is enabled.
Number of Buckets	Enter the number of time buckets for sorting. Default: 100. The value of Number of Buckets × Bucket Interval must not exceed 100. For example, if Bucket Interval is 5 ms, the maximum Number of Buckets is 20. If the configured values exceed this limit, the application returns an error.
Packets per Bucket	Enter the maximum number of packets each bucket can hold. Default: 20,000.
Bucket Interval (ms)	Enter the time span (in milliseconds) for each bucket. Minimum: 1 ms. Maximum: 5 ms. Default: 1 ms. The sorting window equals Number of Buckets × Bucket Interval. For example, 100 buckets × 1 ms = a 100 ms sorting window.
Packet Outside Bucket Interval	Select the action for packets that arrive with timestamps outside the current sorting window. Forward (recommended), sends the packet to the downstream application without reordering. Discard, drops the packet at the 5G-EVP application.
Monitored Flows	
Number of Egress Flows	Enter the maximum number of egress flows. Default: 512. Maximum: 16,384.
Egress Flow Timeout Value	Enter the timeout (in seconds) for egress flow entries. Default: 660.
Ingress UDPGRE Tunnel	

Listening IP	Specify the tunnel's local listen IP address to receive the packet.
Listening Port	Specify the tunnel's local listening port to bind to receive the packet. Enter the UDP port number. Default: 4754 (non-secure) or 4755 (DTLS). You can enter any valid port number.
RX Thread	Specify the RX value to receive the packet. Enter a value between 1 and 16. The default value is 8.
DTLS	Select Enable to receive DTLS-encrypted traffic, or Disable for plaintext UDP-GRE traffic.
DTLS Key	Select the key alias associated with the SSL certificate used for DTLS decryption.
Egress UDP Tunnel	
Tool IP	Egress Tunnels Endpoint, Destination IP address.
Tx Destination Port	Enter the destination port. This value must match the listen port on the downstream application. Default: 4754.
Tx Source IP List	Enter up to 8 source IP addresses for the egress tunnel. Configure these IPs in the VM's NetPlan before adding them here.
Tx Source Port	Enter the source port for the egress UDP-GRE tunnel.
Tx Thread	Enter the number of transmit threads. Range: 1-8.
Diagnostics	
Packet Disable	Enter a protocol key value to disable processing for a specific Ericsson protocol. Default: 0.
Tx Disable	Select true to disable packet transmission (for debugging), or false for normal transmission. Default: false.
Logging	
Log Level	Select the minimum severity of system events to log. Higher levels generate more detailed logs.
Packet Capture Log Level	Select the log level: all, receive, transmit, or none.
Message Log Level	Select the log level: error, warn, info, or debug. Default: error.
Log Directory	Thebpath where log files should be stored.

6. Drag and drop an **Egress REP**. This is a placeholder, no configuration is required.
7. Create links: **Ingress REP -> 5G-EVP -> Egress REP**.
8. From the **Actions** menu, select **Deploy**.

NOTE: You cannot disable both packet ordering and DTLS simultaneously. At least one must be enabled for the 5G-EVP application to function.

Monitoring Session 2: 5G-SBI

Create this monitoring session on the **5G-SBI** V Series Node (DPDK-based).

1. In GigaVUE-FM, go to the monitoring domain for the **5G-SBI** V Series Node.
2. Create a new monitoring session.
3. Create one UDP-GRE ingress tunnel for each Ericsson vTAP key value that you want to process. The following table lists the key values and their traffic types:

Key Value	Traffic Value
0,2	Metadata (domain classification)
1	SBI (L7-JSON) - AMF, SMF
5, 7, 9, 11, 15, 21, 23	Non-SBI

Path 1: Metadata (Keys 0 and 2)

4. Drag and drop the first PCAPng application for metadata processing. Select Details and configure the following:

Field	Description
Application	The name Pcapng appears by default.
Alias	Enter an Alias as required.
App Mode	Set App Mode to Primary to view and configure domain related options. NOTE: Primary mode is required to configure domain classification. When you set App Mode to Secondary, Domain Classification, Domain VLAN Mapping, and Flow Timeout fields are not visible.
Domain Classification	Enable the Domain Classification option to classify Ericsson vTAP traffic by domain.
Domain VLAN Mapping	• From the Domain VLAN Mapping list, select the VLAN mapping profile that maps Ericsson domains to VLAN IDs for per-domain tagging on the egress tunnel. • Click Add New to create a new 5G-Apps configuration. Refer to Adding CSV file for IP Mapping section in 5G-Service Based Interface Application for details. When Domain Classification is enabled, the selected Domain VLAN Mapping is used to tag packets per Ericsson domain with the configured VLAN ID (and, if applicable, a separate VLAN ID for failed SBI transactions) before sending traffic to the probes.
Flow Timeout	Set the Flow Timeout value in seconds to define how long an inactive Ericsson vTAP flow is kept before it is closed and its resources are released. Valid range: 360-1860 Default value: 660

- Link the ingress tunnels for key values 0 and 2 to this PCAPng instance.

NOTE: This PCAPng instance does not require an egress tunnel. It processes metadata only and does not forward traffic to probes. Only one PCAPng instance can be set to Primary mode per monitoring session.

Path 2: SBI Traffic (Key 1)

- Drag and drop the second PCAPng application for SBI traffic. Select Details and set App Mode to Secondary.
- Link the ingress tunnel for key value 1 to this PCAPng instance.
- Drag and drop the 5G-SBI application. Select Details and configure the following:

Field	Description
Application	The name 5g-sbi appears by default.
Alias	The name sbi5gAppTemplate appears by default.
Vendor Integrations	Select the option ericssonVTap from the drop-down list.
SBI Operational Mode	Select the SBI Monitoring Mode for 5G-SBI Network traffic. L7json is selected by default.
Destination IP	The Destination IP toggle determines how synthesized SCP mediated SBI transactions are tagged. You can choose from the following options: SCP - Sets the synthesized transaction's destination IP to the SCP IP address. This option is selected by default. Destination Network Function - Sets the synthesized transaction's destination IP to the IP address of the destination network function.
Ericsson vTAP Version	Select 1 or 2 from the drop-down list box.
MTU Packet Size	Select how packets should be sent to the tool: Full Packet - Sends the entire synthesized packet as a single packet without segmentation. The packet is fragmented at the egress TEP. MTU Size - Segments packets based on the configured tool port MTU value before sending them to the tool. You can specify a value between 1200 and 9200 bytes.
Incomplete SBI Transaction Domain Tag	Enable this option to tag unclassified SBI transactions with the dedicated 'Failed SBI Transaction' VLAN ID defined in the Domain table.

	The probe uses this tag to identify and troubleshoot these transactions more effectively. NOTE: This option appears only when at least one Primary PCAPng file is configured on a V Series node.
Indexed Headers	Enable the check box to index the HTTP2 headers in the 5G-SBI application.
Compressed Headers	Enable the check box to compress the HTTP2 headers in the 5G-SBI application.
TCP Flows	Specify the maximum number of TCP flows based on the VM form factor: • Small - Supports 128 to 2048 TCP flows • Medium - Supports 128 to 8192 TCP flows • Large - Supports 128 to 16384 TCP flows
TCP Flow Timeout	Specify the flow range value (in seconds) that determines how long a TCP flow remains valid in the application. • Minimum value: 0 • Maximum Value: 7200 • Default value: 1800
Number of Transaction Flows	Specify the maximum number of streams or flows based on the VM form factor: • Small - Supports 1 to 20480 Transaction flows • Medium - Supports 1 to 51200 Transaction flows • Large - Supports 1 to 122880 Transaction flows
Request Timeout	Specify the time (in seconds) for which the request packet waits for the response packet in a stream. • Minimum value: 1 • Maximum Value: 300 • Default value: 10
Response Timeout	Specify the time (in seconds) for which the response packet waits for the request packet in a stream. • Minimum value: 1 • Maximum Value: 300 • Default value: 2
IP Mapping	
Network Function Instance Mapping	Select the required CSV file from the drop-down list with required Network Function Instance ID (NFID) instance mapping. • Select an alias: Choose the alias name

	associated with the uploaded NFID table (CSV file). • Add a new alias: If no alias exists, click Add New to create one. Refer to Configure PCC Traffic Flow for details. NOTE: If duplicate entries are detected during mapping table upload, a validation error is displayed. After all other validation errors are resolved, select Save Anyway to save the file.
FQDN Mapping	Select the required CSV file from the drop-down list with required FQDN mapping. • Select an alias: Choose the alias name associated with the uploaded FQDN table (CSV file). • Add a new alias: If no alias exists, click Add to create one. Refer to Configure PCC Traffic Flow section for details. NOTE: If duplicate entries are detected during mapping table upload, a validation error is displayed. After all other validation errors are resolved, select Save Anyway to save the file.
Logging	
Transaction Log	Enable or disable 5G-SBI transaction logging. When enabled, transaction logs are written and rotated based on the configured Transaction Log File Interval.
Transaction Log Interval(Minutes)	Set the transaction log file interval in minutes. This defines how often a new Transaction Log CSV file is created. • Valid options: 5 or 60 minutes • Default: 60 This setting is used only when Transaction Log is enabled.

Stats Log	Enable or disable statistics logging for the 5G-SBI application. When enabled, statistics are written to the configured log folder and managed based on the Log Folder Size setting.
Log Folder Size(MB)	Specify the memory size (in MB) allocated to the log folder. This sets the maximum allowable size for the 5G-SBI log folder and applies to both transaction and statistics logs stored in the configured Log Folder Location. Maximum Value: 40960 MB.
Log Folder Location	Enter the file system path where 5G-SBI log files should be stored. This is the location for both transaction and statistics logs. Example: /home/user/log

- Link the SBI PCAPng instance (from Step 6) to the 5G-SBI application.

Path 3: Non-SBI Traffic (Keys 5, 7, 9, 11, 15, 21, 23)

- Drag and drop the third **PCAPng** application for non-SBI traffic. Select **Details** and set **App Mode** to **Secondary**.
- Link the ingress tunnels for non-SBI key values (5, 7, 9, 11, 15, 21, 23) to this PCAPng instance.

NOTE: Non-SBI traffic does not require a 5G-Cloud application. The PCAPng application reads the data from the Enhanced Packet Block and forwards it directly to the egress tunnel.

Create Egress Tunnels and Deploy

- Create one or more egress tunnels (VXLAN or L2GRE). If Domain Classification is enabled, enable Domain Tagging on the egress tunnel.
- Link the **5G-SBI** application output to the egress tunnel (for SBI traffic).
- Link the non-SBI **PCAPng** application output to the egress tunnel (for non-SBI traffic).
- Verify all links on the canvas:
 - Ingress tunnels (key 0, 2) -> PCAPng (Primary), no egress
 - Ingress tunnel (key 1) -> PCAPng (Secondary) -> 5G-Cloud -> Egress tunnel
 - Ingress tunnels (non-SBI keys) -> PCAPng (Secondary) -> Egress tunnel
- From the **Actions** menu, select **Deploy**.

Monitoring Session 3: 5G-Cloud

Create this monitoring session on the 5G-Cloud V Series Node (Linux-based).

1. In GigaVUE-FM, navigate to the monitoring domain for the 5G-Cloud V Series Node.
2. Create a new monitoring session.
3. Drag and drop an Ingress REP (placeholder, no configuration required).

4. Drag and drop the 5G-Cloud application. Select Details and configure the following:

Field	Description
Application	The name 5g-Cloud appears by default.
Alias	Enter the alias name as cloud5g .
Mode	From the drop-down list, select Ericsson SCP Transparent .
RX Tunnel	
Type	Specify the tunnel type. The default is VXLAN.
Listening IP	Specify the tunnel's local listen IP address to receive the packet.
Listening Port	Specify the tunnel's local listening port to bind to receive the packet. The application will listen to the traffic coming to the specified port. Enter a value between 1 and 65535.
Source Port	Specify the tunnel destination port from where the packets will be sent. Enter a value between 1 and 65535.
VNI Id	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215. The default value is zero.
RX Thread	Specify the RX value to receive the packet. Enter a value between 1 and 16. The default value is 8.
TX Tunnel	
Type	Specify the tunnel type. The available tunnel types are: • VXLAN • L2GRE
Tool IP	Specify the remote IP address to send the packet.
Destination Port	Specify the tunnel destination port to which the packet will be sent. Enter a value between 1 and 65535.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the tunnel source port to bind when sending the packet. Enter a value between 1 and 65535.
VNI Id (Applicable only when the selected tunnel type is VXLAN)	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215.
L2GRE Key (Applicable only when the selected tunnel type is L2GRE)	Specify the key for the L2GRE tunnel type. Enter a value between 0 and 4294967295.
Advanced Setting	
Tool MTU	Specify the tool port MTU.
Log Directory	Specify the path to store the log files.
Log Level	Select the severity log level of the events from the following options: • None • Fatal

	• Error • Notification • Information • Debug
SCP Config	
FQDN Mapping	Specify the alias name created for the uploaded FQDN table CSV file.
NF Instance Mapping	Specify the alias name created for the uploaded NFID table CSV file.
User Agent Mapping	Specify the alias name created for the uploaded User Agent table CSV file.
TCP Server Ports	Specify the TCP server port or port range to allow TCP communication endpoints.
SCP Advanced Config	
No. of TCP Flows	Specify the total number of concurrent TCP flows. Enter a value between 128 and 2048. The default value is 1024.
No. of Transaction Flows	Specify the total number of Transaction Stream Flows allocated for tracking active Transaction Streams. Enter a value between: • 128 and 26000 for V Series Node of extra large form factor (total memory $\geq$ 32GB). • 128 and 5500 for V Series Node of large form factor (total memory $<$ 32GB). The default value is 2048.
TCP Flow Timeout	Specify the TCP flow timeout ranging between 0 to 7200. The default value is 900.
SCP Transaction Timeout	Specify the SCP transaction timeout value ranging between 1 and 300. The default value is 10. Note: The recommended timeout value is between 10 and 20 seconds. An increase in the transaction timeout value will impact the total number of transactions that can be processed in parallel.
Minimum TCP Client Port	Specify the minimum value to be used for TCP client port ranging between 1023 and 65535. The default value is 32768.
Maximum TCP Client Port	Specify the maximum value to be used for client port ranging between 1023 and 65535. The default value is 36863.
SCP Processing Threads	Specify the number of worker threads for processing In-Out packets. Enter a value between 1 and 16. The default value is 8.
TCP Client Ports per Thread	Specify the number of TCP client ports for each worker thread. Enter a value between 100 and 8000. The default value is 1000.
Header Index	Enable or disable the header indexing. The default value is disabled.
Header Compression Code	Enable or disable the header compression code. The default value is disable.

Gigamon Header	Enable or disable the Gigamon Header. The default value is Enable.
Packet Capture Level	Select the packet capture level from the drop-down list: • All • Receive • Transmit • None
5G-Cloud Log Level	Select the required 5G-Cloud CSV log level from the drop down list. The default value is None. • All • Flow • Message • Transaction • None
HTTP2 Monitored Flows	
Number of Streams	Specify the number of monitored stream flows. Enter a value between 1024 and 16384. The default is 1024.
Request Timeout	Specify the HTTP/2 request timeout in seconds. Enter a value between 1 and 300. The default is 15 seconds.
Response Timeout	Specify the HTTP/2 response timeout in seconds. Enter a value between 1 and 300. The default is 2 seconds.
TCP Monitored Flows	
Number of Flows	Specify the number of monitored TCP flows. Enter a value between: • 1024 and 32768 for V Series Node of extra large form factor (total memory > 32GB). • 1024 and 2048 for V Series Node of lesser form factor. The default value is 2048.
Flow Timeout	Specify the timeout for TCP flows in seconds. Enter a value between 1 and 7200. The default value is 60 seconds.
Flow Reassembly Timeout	Specify the timeout for TCP flow reassembly in seconds. Enter a value between 1 and 7200. The default value is 500 seconds.

5. Drag and drop an Egress REP (placeholder, no configuration required).
6. Create links: Ingress REP -> 5G-Cloud -> Egress REP.
7. From the Actions menu, select Deploy.

**Notes:**

- After you deploy a Monitoring Session, you cannot edit its associated 5G SBI or PCAPng application configurations. To modify them, undeploy the Monitoring Session, update the configuration, and redeploy.



- If a PCAPng application instance is set as the Primary for a Monitoring Session, you cannot delete it while it holds that role. To delete or replace it, undeploy the Monitoring Session or reassign the Primary.

Adding CSV file for IP Mapping

To add the CSV file for IP mapping:

1. Go to **Inventory > VIRTUAL >** select your cloud platform, and then click **Settings > 5G-Apps**. The 5G-Apps Configuration page appears.
2. Click **New**. Enter the name for the CSV file in the **Alias** field.
3. From the **Type** drop-down list, select one of the following. You can also choose to download the template using the **Download Template** option and add the required entries.

- **5G-SBI Network Function Instance** - Add the CSV file containing a valid NF instance ID and a valid IPv4/IPv6 address for IP mapping in 5G-Ericsson.

Header details with an example:

- **instanceID** - e4d909c2-5d2f-4f7f-9bcb-12a3b6c4d789
- **ipAddress** - 1.1.1.1

- **5G-SBI FQDN** - Add the CSV file containing a valid FQDN ID and a valid IPv4/IPv6 address for IP mapping.

Header details with an example:

- **fqdnID** - amf.local
- **ipAddress** - 1.1.1.1
- **nfType** - SCP

- **Domain VLAN Mapping** - Add the CSV file containing a valid domain and a valid VLAN ID for IP mapping.

Refer the table below for example header details of the CSV file.

domainName	vlanID	failedSBITransactionVlanID
pc-mm	100	200
pc-sm	300	400
ccsm-5gc	500	
ccsm-cnhs	600	
ccrc-nrf	700	
nrfagent-nrf	800	

domainName	vlanID	failedSBITransactionVlanID
ccrc-nssf	900	
ccpc-pcf	1000	
ccpc-provisioning	1100	
ccdm-udr-5g	1200	
ccdm-provisioning	1300	
ccdm-udr-legacy	1400	
cces-nef	1500	
cces-ees	1600	
cces-apigm	1700	
sc-bsf	1800	
sc-scp	1900	
sc-sepp	2000	
others	2100	
unclassified	2200	

- Click **Choose File** in **File Name** field to upload the CSV file into GigaVUE-FM.
- Click **Validate** to validate the CSV file.
- Click **Save** to add the CSV file.

**Notes:**

- Failed SBI Transactions are applicable only for **pc-mm** and **pc-sm** domains.
- Each domain in the Domain table must use a unique VLAN ID and Failed SBI Transaction ID to allow the probes to distinguish traffic for each Ericsson domain.

Recommended VM Specifications

The configuration of the V Series application should be performed on large VMs.

V Series App	vCPUs	Memory	Disk Space
5G-EVP	20	32 GB	80 GB
5G-SBI	8	16 GB	80 GB
5G-Cloud	24	32 GB	80 GB

- Supported Ports: 1 Management interface, 1 ingress, and 1 egress interfaces.

- It is recommended to use SRIOV enabled drivers for better performance and higher throughput. Refer to [Configure GigaVUE Fabric Components using VMware ESXi](#) topic for more details.

FHA Dashboards for 5G Applications

After configuring the 5G-SBI application, you can monitor the statistics for Ericsson vTAP by the reports displayed in the Dashboard. To access the details, refer to [FHA Dashboards for 5G Applications](#).

Upgrade and Migration Steps

Follow these steps to add the 5G-EVP application to an existing deployment. If you are deploying as part of a new setup, skip this section.

1. Upgrade GigaVUE-FM to the current release.
2. Upgrade the existing 5G-SBI and 5G-Cloud V Series to the current release.
3. Deploy a new 5G-EVP V Series Node running the current release.
4. Reassign the ingress IP address from the 5G-SBI Node to the EVP Node ingress interface.
5. Provision a new IP address for the EVP Node egress interface.
6. Provision a new IP address for the 5G-SBI Node ingress interface. This must be in the same subnet as the EVP egress IP.
7. If the existing deployment has a source IP in the TEP configuration, remove it.
8. Configure the 5G-EVP monitoring session. Refer to [5G-EVP](#) for field descriptions.
9. Update the 5G-SBI monitoring session with the new ingress IP address.
10. Deploy both monitoring sessions from the Actions menu in GigaVUE-FM.

NOTE: The 5G-SBI to 5G-Cloud pipeline remains unchanged. No modifications are required on the 5G-Cloud Node.

Configure SCP Traffic Flow

Use this workflow when your deployment includes SCP (L7-Native) traffic from Ericsson CCx vTAPs. You can deploy this workflow independently or alongside the SBI traffic flow. The SCP traffic passes through a Load Balancing (LB) application for distribution before reaching the

5G-Cloud Node for L7-Native synthesis.

Monitoring Sessions Required

Monitoring Session	V Series Node	Traffic Handled
5G-EVP	5G-EVP	All traffic, packet ordering and optional DTLS decryption
SCP	5G-SBI	SCP ingress (keys 3,17,19) + Metadata (keys 0,2) + LB + multi-tap egress
5G-Cloud	5G-Cloud	SCP synthesis (L7-Native)

Prerequisites

Before you begin, complete the following:

- Deploy three V Series Nodes: 5G-EVP, 5G-SBI, and 5G-Cloud.
- Create a separate monitoring domain for each V Series Node in GigaVUE-FM.
- Verify that the V Series 5GC add-on license is active.
- Configure NTP servers for the 5G-EVP Node (required when packet ordering is enabled).
- If you plan to use DTLS, upload the private key and certificate in GigaVUE-FM via Inventory > Security > SSL Key.
- If you plan to use multiple egress IPs on the 5G-EVP Node, configure the additional IP addresses in NetPlan on the VM. Refer to Configuring Multiple Egress IP Addresses.
- Upload CSV Files for the 5G-Cloud Application
 - In GigaVUE-FM, go to Inventory > VIRTUAL.
 - Select your cloud platform.
 - Click Settings, and then click 5G-Apps.
 - Upload the FQDN, NF Instance, and User Agent CSV files.

End to End Configuration

Configure 5G-EVP Application

To configure the 5G-EVP application, drag and drop it onto the monitoring session canvas and select Details. The 5G-EVP application quick view appears. Enter or select the required information as described in the following tables.

Field	Description
Application	The name 5g-EVP appears by default.
Alias	Enter the alias name as 5gEVP .
Packet Ordering Config	
Packet Ordering	Toggle to enable or disable timestamp-based packet reordering. When enabled, the 5G-EVP application sorts packets based on the observed timestamp in the PCAPng Enhanced Packet Block before forwarding them to the downstream application.
Primary NTP Server*	Enter the IP address (IPv4 or IPv6) of the primary NTP server. The 5G-EVP application requires NTP time synchronization through chronyd for millisecond-accurate clock alignment. GigaVUE-FM sends this configuration to the V Series Node during each deployment. This field is mandatory when packet ordering is enabled. NOTE: Visible when Packet Ordering is enabled.
Secondary NTP Server	Enter the IP address (IPv4 or IPv6) of the secondary NTP server. This field is optional. The secondary NTP server provides failover if the primary NTP server becomes unreachable. NOTE: Visible when Packet Ordering is enabled.
Number of Buckets	Enter the number of time buckets for sorting. Default: 100. The value of Number of Buckets × Bucket Interval must not exceed 100. For example, if Bucket Interval is 5 ms, the maximum Number of Buckets is 20. If the configured values exceed this limit, the application returns an error.
Packets per Bucket	Enter the maximum number of packets each bucket can hold. Default: 20,000.
Bucket Interval (ms)	Enter the time span (in milliseconds) for each bucket. Minimum: 1 ms. Maximum: 5 ms. Default: 1 ms. The sorting window equals Number of Buckets × Bucket Interval. For example, 100 buckets × 1 ms = a 100 ms sorting window.
Packet Outside Bucket Interval	Select the action for packets that arrive with timestamps outside the current sorting window. Forward (recommended), sends the packet to the downstream application without reordering. Discard, drops the packet at the 5G-EVP application.
Monitored Flows	
Number of Egress Flows	Enter the maximum number of egress flows. Default: 512. Maximum: 16,384.
Egress Flow Timeout Value	Enter the timeout (in seconds) for egress flow entries. Default: 660.
Ingress UDPGRE Tunnel	

Listening IP	Specify the tunnel's local listen IP address to receive the packet.
Listening Port	Specify the tunnel's local listening port to bind to receive the packet. Enter the UDP port number. Default: 4754 (non-secure) or 4755 (DTLS). You can enter any valid port number.
RX Thread	Specify the RX value to receive the packet. Enter a value between 1 and 16. The default value is 8.
DTLS	Select Enable to receive DTLS-encrypted traffic, or Disable for plaintext UDP-GRE traffic.
DTLS Key	Select the key alias associated with the SSL certificate used for DTLS decryption.
Egress UDP Tunnel	
Tool IP	Egress Tunnels Endpoint, Destination IP address.
Tx Destination Port	Enter the destination port. This value must match the listen port on the downstream application. Default: 4754.
Tx Source IP List	Enter up to 8 source IP addresses for the egress tunnel. Configure these IPs in the VM's NetPlan before adding them here.
Tx Source Port	Enter the source port for the egress UDP-GRE tunnel.
Tx Thread	Enter the number of transmit threads. Range: 1-8.
Diagnostics	
Packet Disable	Enter a protocol key value to disable processing for a specific Ericsson protocol. Default: 0.
Tx Disable	Select true to disable packet transmission (for debugging), or false for normal transmission. Default: false.
Logging	
Log Level	Select the minimum severity of system events to log. Higher levels generate more detailed logs.
Packet Capture Log Level	Select the log level: all, receive, transmit, or none.
Message Log Level	Select the log level: error, warn, info, or debug. Default: error.
Log Directory	The path where log files should be stored.

Monitoring Session 2: SCP Traffic (5G-SBI Node)

Create this monitoring session on the 5G-SBI V Series Node. This session handles the ingress, PCAPng processing, and load balancing for SCP traffic before forwarding it to the 5G-Cloud Node.

1. In GigaVUE-FM, navigate to the monitoring domain for the 5G-SBI V Series Node.
2. Create a new monitoring session.
3. Create one UDP-GRE ingress tunnel for each SCP key value:

Key Value	Traffic Value
0,2	Metadata (domain classification)
3, 17, 19	SCP (L7-Native)

4. Drag and drop the first PCAPng application for metadata processing. Select Details and configure the following:

Field	Description
Application	The name Pcapng appears by default.
Alias	Enter an Alias as required.
App Mode	Set App Mode to Primary to view and configure domain related options. NOTE: Primary mode is required to configure domain classification. When you set App Mode to Secondary, Domain Classification, Domain VLAN Mapping, and Flow Timeout fields are not visible.
Domain Classification	Enable the Domain Classification option to classify Ericsson vTAP traffic by domain.
Domain VLAN Mapping	- From the Domain VLAN Mapping list, select the VLAN mapping profile that maps Ericsson domains to VLAN IDs for per-domain tagging on the egress tunnel. - Click Add New to create a new 5G-Apps configuration. Refer to Adding CSV file for IP Mapping section in 5G-Service Based Interface Application for details. When Domain Classification is enabled, the selected Domain VLAN Mapping is used to tag packets per Ericsson domain with the configured VLAN ID (and, if applicable, a separate VLAN ID for failed SBI transactions) before sending traffic to the probes.
Flow Timeout	Set the Flow Timeout value in seconds to define how long an inactive Ericsson vTAP flow is kept before it is closed and its resources are released. Valid range: 360-1860 Default value: 660

5. Link the ingress tunnels for key values 0 and 2 to this PCAPng instance.

NOTE: This PCAPng instance does not require an egress tunnel. Only one PCAPng instance can be set to Primary mode per monitoring session.

6. Drag and drop the second PCAPng application for SCP traffic. Select Details and set App Mode to Secondary.
7. Link the ingress tunnels for key values 3, 17, 19 to this PCAPng instance.
8. Drag and drop the LB (Load Balancing) application. Select Details and configure the hash field to greFlowid.
9. Link the SCP PCAPng instance (from Step 6) to the LB application.
10. Create a VXLAN egress tunnel with the Multi-Tunnel flag enabled. If Domain Classification is enabled, enable Domain Tagging on the egress tunnel.

NOTE: You create one egress tunnel. The system internally creates multiple taps for load distribution (minimum 1, maximum 16).

11. Link the LB application output to the egress tunnel.
12. Verify all links on the canvas:
 - Ingress tunnels (key 0, 2) -> PCAPng (Primary), no egress
 - Ingress tunnels (key 3, 17, 19) -> PCAPng (Secondary) -> LB -> Egress tunnel (multi-tap)
13. From the Actions menu, select Deploy.

Monitoring Session 3: 5G-Cloud

Create this monitoring session on the 5G-Cloud V Series Node (Linux-based).

1. In GigaVUE-FM, navigate to the monitoring domain for the 5G-Cloud V Series Node.
2. Create a new monitoring session.
3. Drag and drop an Ingress REP (placeholder, no configuration required).

4. Drag and drop the 5G-Cloud application. Select Details and configure the following:

Field	Description
Application	The name 5g-Cloud appears by default.
Alias	Enter the alias name as cloud5g .
Mode	From the drop-down list, select Ericsson SCP Transparent .
RX Tunnel	
Type	Specify the tunnel type. The default is VXLAN.
Listening IP	Specify the tunnel's local listen IP address to receive the packet.
Listening Port	Specify the tunnel's local listening port to bind to receive the packet. The application will listen to the traffic coming to the specified port. Enter a value between 1 and 65535.
Source Port	Specify the tunnel destination port from where the packets will be sent. Enter a value between 1 and 65535.
VNI Id	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215. The default value is zero.
RX Thread	Specify the RX value to receive the packet. Enter a value between 1 and 16. The default value is 8.
TX Tunnel	
Type	Specify the tunnel type. The available tunnel types are: • VXLAN • L2GRE
Tool IP	Specify the remote IP address to send the packet.
Destination Port	Specify the tunnel destination port to which the packet will be sent. Enter a value between 1 and 65535.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the tunnel source port to bind when sending the packet. Enter a value between 1 and 65535.
VNI Id (Applicable only when the selected tunnel type is VXLAN)	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215.
L2GRE Key (Applicable only when the selected tunnel type is L2GRE)	Specify the key for the L2GRE tunnel type. Enter a value between 0 and 4294967295.
Advanced Setting	
Tool MTU	Specify the tool port MTU.
Log Directory	Specify the path to store the log files.
Log Level	Select the severity log level of the events from the following options: • None • Fatal

	• Error • Notification • Information • Debug
SCP Config	
FQDN Mapping	Specify the alias name created for the uploaded FQDN table CSV file.
NF Instance Mapping	Specify the alias name created for the uploaded NFID table CSV file.
User Agent Mapping	Specify the alias name created for the uploaded User Agent table CSV file.
TCP Server Ports	Specify the TCP server port or port range to allow TCP communication endpoints.
SCP Advanced Config	
No. of TCP Flows	Specify the total number of concurrent TCP flows. Enter a value between 128 and 2048. The default value is 1024.
No. of Transaction Flows	Specify the total number of Transaction Stream Flows allocated for tracking active Transaction Streams. Enter a value between: • 128 and 26000 for V Series Node of extra large form factor (total memory $\geq$ 32GB). • 128 and 5500 for V Series Node of large form factor (total memory < 32GB). The default value is 2048.
TCP Flow Timeout	Specify the TCP flow timeout ranging between 0 to 7200. The default value is 900.
SCP Transaction Timeout	Specify the SCP transaction timeout value ranging between 1 and 300. The default value is 10. Note: The recommended timeout value is between 10 and 20 seconds. An increase in the transaction timeout value will impact the total number of transactions that can be processed in parallel.
Minimum TCP Client Port	Specify the minimum value to be used for TCP client port ranging between 1023 and 65535. The default value is 32768.
Maximum TCP Client Port	Specify the maximum value to be used for client port ranging between 1023 and 65535. The default value is 36863.
SCP Processing Threads	Specify the number of worker threads for processing In-Out packets. Enter a value between 1 and 16. The default value is 8.
TCP Client Ports per Thread	Specify the number of TCP client ports for each worker thread. Enter a value between 100 and 8000. The default value is 1000.
Header Index	Enable or disable the header indexing. The default value is disabled.
Header Compression Code	Enable or disable the header compression code. The default value is disable.

Gigamon Header	Enable or disable the Gigamon Header. The default value is Enable.
Packet Capture Level	Select the packet capture level from the drop-down list: • All • Receive • Transmit • None
5G-Cloud Log Level	Select the required 5G-Cloud CSV log level from the drop down list. The default value is None. • All • Flow • Message • Transaction • None
HTTP2 Monitored Flows	
Number of Streams	Specify the number of monitored stream flows. Enter a value between 1024 and 16384. The default is 1024.
Request Timeout	Specify the HTTP/2 request timeout in seconds. Enter a value between 1 and 300. The default is 15 seconds.
Response Timeout	Specify the HTTP/2 response timeout in seconds. Enter a value between 1 and 300. The default is 2 seconds.
TCP Monitored Flows	
Number of Flows	Specify the number of monitored TCP flows. Enter a value between: • 1024 and 32768 for V Series Node of extra large form factor (total memory > 32GB). • 1024 and 2048 for V Series Node of lesser form factor. The default value is 2048.
Flow Timeout	Specify the timeout for TCP flows in seconds. Enter a value between 1 and 7200. The default value is 60 seconds.
Flow Reassembly Timeout	Specify the timeout for TCP flow reassembly in seconds. Enter a value between 1 and 7200. The default value is 500 seconds.

5. Drag and drop an Egress REP (placeholder, no configuration required).
6. Create links: Ingress REP -> 5G-Cloud -> Egress REP.
7. From the Actions menu, select Deploy.

**Notes:**

- After you deploy a Monitoring Session, you cannot edit its associated 5G SBI or PCAPNG application configurations. To modify them, undeploy the Monitoring Session, update the configuration, and redeploy.



- If a PCAPNG application instance is set as the Primary for a Monitoring Session, you cannot delete it while it holds that role. To delete or replace it, undeploy the Monitoring Session or reassign the Primary.

Adding CSV file for IP Mapping

To add the CSV file for IP mapping:

1. Go to **Inventory > VIRTUAL >** select your cloud platform, and then click **Settings > 5G-Apps**. The 5G-Apps Configuration page appears.
2. Click **New**. Enter the name for the CSV file in the **Alias** field.
3. From the **Type** drop-down list, select one of the following. You can also choose to download the template using the **Download Template** option and add the required entries.

- **5G-SBI Network Function Instance** - Add the CSV file containing a valid NF instance ID and a valid IPv4/IPv6 address for IP mapping in 5G-Ericsson.

Header details with an example:

- **instanceID** - e4d909c2-5d2f-4f7f-9bcb-12a3b6c4d789
- **ipAddress** - 1.1.1.1

- **5G-SBI FQDN** - Add the CSV file containing a valid FQDN ID and a valid IPv4/IPv6 address for IP mapping.

Header details with an example:

- **fqdnID** - amf.local
- **ipAddress** - 1.1.1.1
- **nfType** - SCP

- **Domain VLAN Mapping** - Add the CSV file containing a valid domain and a valid VLAN ID for IP mapping.

Refer the table below for example header details of the CSV file.

domainName	vlanID	failedSBITransactionVlanID
pc-mm	100	200
pc-sm	300	400
ccsm-5gc	500	
ccsm-cnhs	600	
ccrc-nrf	700	
nrfagent-nrf	800	
ccrc-nssf	900	
ccpc-pcf	1000	
ccpc-provisioning	1100	

domainName	vlanID	failedSBITransactionVlanID
ccdm-udr-5g	1200	
ccdm-provisioning	1300	
ccdm-udr-legacy	1400	
cces-nef	1500	
cces-ees	1600	
cces-apigm	1700	
sc-bsf	1800	
sc-scp	1900	
sc-sepp	2000	
others	2100	
unclassified	2200	

- Click **Choose File** in **File Name** field to upload the CSV file into GigaVUE-FM.
- Click **Validate** to validate the CSV file.
- Click **Save** to add the CSV file.

**Notes:**

- Failed SBI Transactions are applicable only for **pc-mm** and **pc-sm** domains.
- Each domain in the Domain table must use a unique VLAN ID and Failed SBI Transaction ID to allow the probes to distinguish traffic for each Ericsson domain.

Recommended VM Specifications

The configuration of the V Series application should be performed on large VMs.

V Series App	vCPUs	Memory	Disk Space
5G-EVP	20	32 GB	80 GB
5G-SBI	8	16 GB	80 GB
5G-Cloud	24	32 GB	80 GB

- Supported Ports: 1 Management interface, 1 ingress, and 1 egress interfaces.
- It is recommended to use SRIOV enabled drivers for better performance and higher throughput. Refer to [Configure GigaVUE Fabric Components using VMware ESXi](#) topic for more details.

FHA Dashboards for 5G Applications

After configuring the 5G-SBI application, you can monitor the statistics for Ericsson vTAP by the reports displayed in the Dashboard. To access the details, refer to [FHA Dashboards for 5G Applications](#).

Upgrade and Migration Steps

Follow these steps to add the 5G-EVP application to an existing deployment. If you are deploying as part of a new setup, skip this section.

1. Upgrade GigaVUE-FM to the current release.
2. Upgrade the existing 5G-SBI and 5G-Cloud V Series to the current release.
3. Deploy a new 5G-EVP V Series Node running the current release.
4. Reassign the ingress IP address from the 5G-SBI Node to the EVP Node ingress interface.
5. Provision a new IP address for the EVP Node egress interface.
6. Provision a new IP address for the 5G-SBI Node ingress interface. This must be in the same subnet as the EVP egress IP.
7. If the existing deployment has a source IP in the TEP configuration, remove it.
8. Configure the 5G-EVP monitoring session. Refer to [Configure SCP Traffic Flow](#) for field descriptions.
9. Update the 5G-SBI monitoring session with the new ingress IP address.
10. Deploy both monitoring sessions from the Actions menu in GigaVUE-FM.

NOTE: The 5G-SBI to 5G-Cloud pipeline remains unchanged. No modifications are required on the 5G-Cloud Node.

5G-Cloud Application

5G-Core is a service-based architecture in which many control plane network functions are available and communication across these network functions happens through HTTP2 protocol. These HTTP2 transactions are mirrored using some specific network functions, which are in JSON-encoded format.

The 5G Cloud application supports synthesizing of L2, L3, L4, and HTTP2 headers from the JSON-encoded data of the 5G core network. Currently, Ericsson VTAP 5G core input format is supported in DPDK based platforms and in non-DPDK based platforms, Casa vTAP, Oracle SCP, Nokia SCP Inbound, and Nokia SCP Inbound/Outbound input formats are supported.

In non-DPDK mode, V Series Node supports processing of the HTTP2/HTTP2S input formats and extracts the actual packet in the 5G core, and then sends it out on the egress tunnel to probe using either VXLAN or L2GRE or UDP-GRE Tunnel. To achieve this, V Series supports two new applications:

- GVHTTP2
- 5G-Cloud

Supported Platforms

The application is supported on the following platforms:

- VMware ESXi
- OpenStack
- Third Party Orchestration

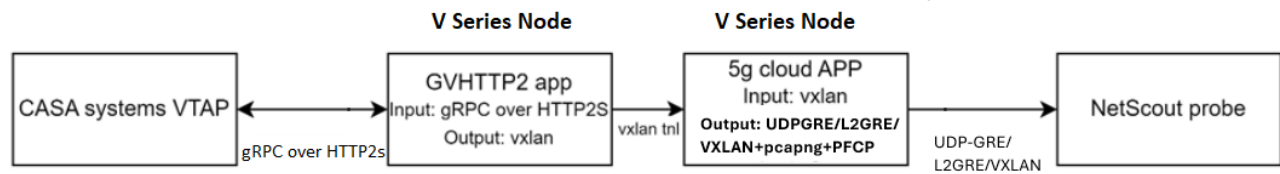
To know more about the configuration of GVHTTP2 and 5G-Cloud application for Casa vTAP, Oracle SCP, and Nokia SCP, refer to the following sections:

- [5G-Cloud Casa vTAP Support](#)
- [5G-Cloud Oracle and Nokia SCP Support](#)
- [5G-Cloud Ericsson SCP Support](#)
- [5G Cloud Nokia IMS Solution \(Non-SBI\)](#)

5G-Cloud Casa vTAP Support

V Series Node supports receiving data from 5G Casa network functions in the Casa vTAP input format. This augments the currently existing functionality of receiving data from Ericsson network functions in Ericsson vTAP format and receiving data from Nokia network functions in Nokia format. 5G-Cloud Casa vTAP is a non-service-based interface architecture in which input from the Casa vTAP system is processed, decoded, and sent out through an egress tunnel.

Casa systems vTAP network function mirrors the traffic in the 5G core and sends it out in gRPC encoded protobuf format. To convert the encoded protobufs to actual network traffic in 5G core, V Series Node supports two applications, GVHTTP2 and the 5G-Cloud.



GVHTTP2 Application

The first application, GVHTTP2, acts as an HTTP2 server. It receives the gRPC data over HTTP2 and establishes a TCP connection with the Casa vTAP system by acknowledging it. The application will extract the HTTP2 header and HTTP2 body, which are gRPC encoded, then encapsulate the data into a VXLAN header and send it out over the VXLAN tunnel to the next application, 5G-Cloud.

5G-Cloud Application

The 5G-Cloud application receives the VXLAN packet, decapsulates, and decodes the gRPC protobuf content. The application will extract the PFCP packets (N4 traffic) and convert the traffic into PCAPng format. It then sends the extracted packets to the NetScout tool probe over the UDP-GRE/L2GRE/VXLAN tunnels.

NOTE: Since the NetScout probe only understands Ericson vTAP format, which is UDP-GRE encapsulated in PCAPng format, the same is followed in the Casa vTAP system. As part of the 6.7 release, only N4 non-SBI traffic (PFCP) is supported.

Configuration of 5G-Cloud Casa vTAP

To configure the GVHTTP2 and 5G-Cloud applications in GigaVUE-FM, refer to the following sections:

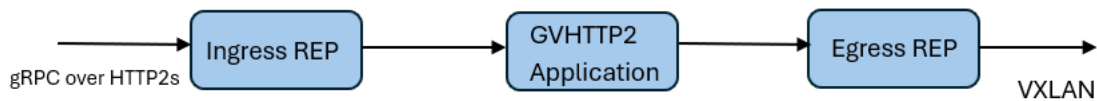
- [Configuration of GVHTTP2 Application for Casa vTAP](#)
- [Configuration of 5G-Cloud Application for Casa vTAP](#)

Configuration of GVHTTP2 Application for Casa vTAP

In GigaVUE-FM, you must do the following to add the GVHTTP2 application in the Monitoring Session of a Monitoring Domain:

1. Create an ingress REP (Raw End Point) to receive the gRPC data over TCP on top of HTTP2. Refer to *Create Raw Endpoint* section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) for more information on creating a REP.

2. Add the GVHTTP2 application in the Monitoring Session.
3. Create a link between ingress REP and the GVHTTP2 application.
4. Create egress REP.
5. Create a link between the GVHTTP2 application and egress REP.

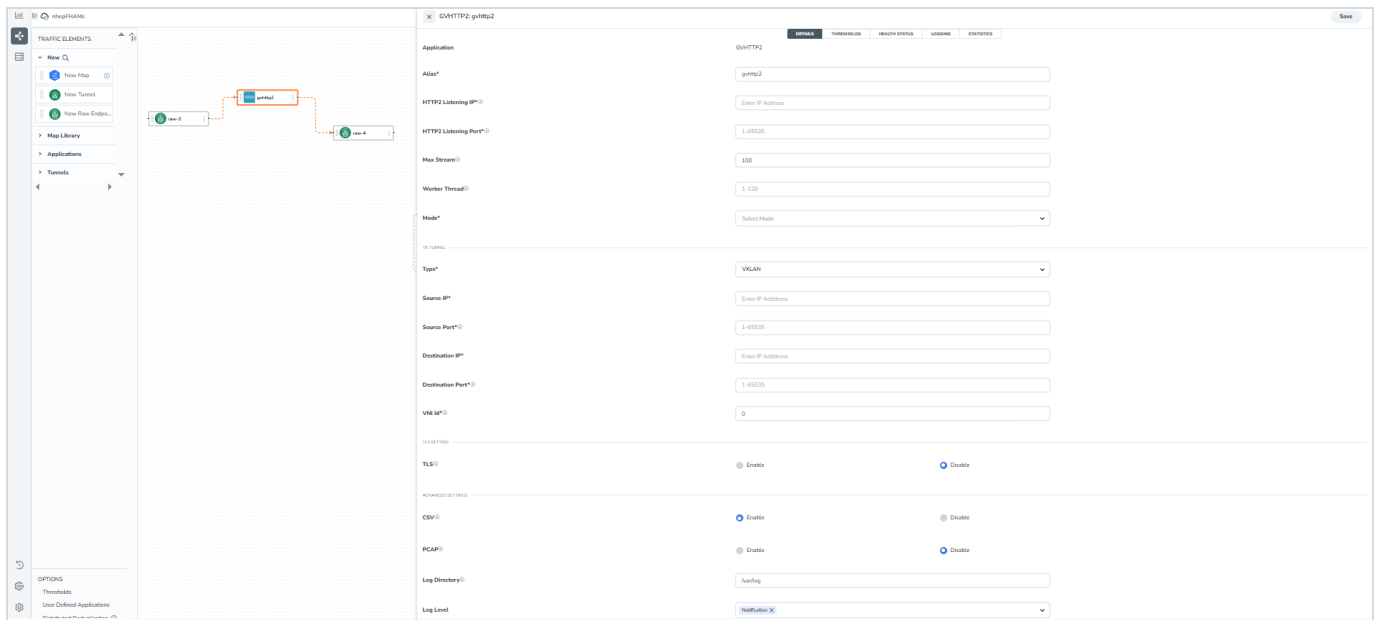


You can add a GVHTTP2 application to:

- **New Monitoring Session** - Add the GVHTTP2 application after creating a new Monitoring Session and when the GigaVUE-FM canvas appears. Refer to Create a Monitoring Session section in the respective GigaVUE Cloud Suite Deployment Guide.
- **Existing session** - Select any existing Monitoring Session and go to **TRAFFIC PROCESSING** tab. The GigaVUE-FM canvas appears.

To add a GVHTTP2 application:

1. In the canvas, drag and drop the GVHTTP2 application and select **Details**. The GVHTTP2 quick view appears.



2. On the application quick view, enter or select the required information as described in the following table:

Field	Description
Application	The name GVHTTP2 appears by default.
Alias	Enter the alias name as gvhttp2 .
HTTP2 Listening IP	Specify the HTTP2 IP address. The application will listen to the traffic on the specified IP address.
HTTP2 Listening Port	Specify the HTTP2 Port. The application will listen to the traffic on the specified port. Enter a value between 1 and 65535.
Max Stream	Specify the maximum number of concurrent streams in one HTTP2 session. Enter a value between 1 and 100. The default value is 100.
Worker Thread	Specifies the number of worker threads. Enter a value between 1 and 128. The default value is one.
Mode	Select Casa vTAP as mode from the drop-down menu.
TX Tunnel (Specifies the tunnel configuration from GVHTTP2 to 5G-Cloud)	
Type	Specify the tunnel type. VXLAN is selected by default.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the source port to bind for sending the packet. Enter a value between 1 and 65535.
Destination IP	Specify the destination IP address to which packets will be sent.
Destination Port	Specify the destination port where packets will be sent.
VNI id	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215. The default value is zero.
TLS Setting	
TLS	Select a TLS/SSL Monitor Mode from one of the following options: - Enable—When the monitor mode is enabled, the TLS/SSL decryption or encryption is off. - Disable—This is the default value. When the monitor mode is disabled, the TLS/SSL decryption or encryption is on.
Advanced Setting	
Log Directory	Specify the path to store the log files.
Log Level	In the log level drop-down list, select the severity log level of the events from the following options: - PCAP - CSV - Info - Detail - Full-Parse

Downloading Logs for GVHTTP2 application

You can view the log files of a V Series Node or download them as CSV or .txt file.

To download the log files to a local environment:

1. Go to **Traffic > VIRTUAL** > select your cloud platform.
2. Select the required Monitoring Session and click the **APPS LOGGING** link.
3. The **GVHTTP2 Logging** page displays the logs currently available. You can download the preferred logs by selecting the required Days, Timestamps, File Name, and Type (TextLog and FlowStats) details.
4. Select the log files to download, and then click **Download Files** from the **Actions** menu.
5. The system downloads the selected files to your local environment.

Configuration of 5G-Cloud Application for Casa vTAP

In GigaVUE-FM, you must do the following to configure the 5G-Cloud application in the Monitoring Session of a Monitoring Domain:

1. Create ingress REP to extract the HTTP2 body (gRPC content). Refer to *Create Raw Endpoint* section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) for more information on creating a REP.
2. Add the 5G-Cloud application in the Monitoring Session.
3. Create a link between ingress REP and the 5G-Cloud application.
4. Create egress REP.
5. Create a link between the 5G-Cloud application and egress REP.

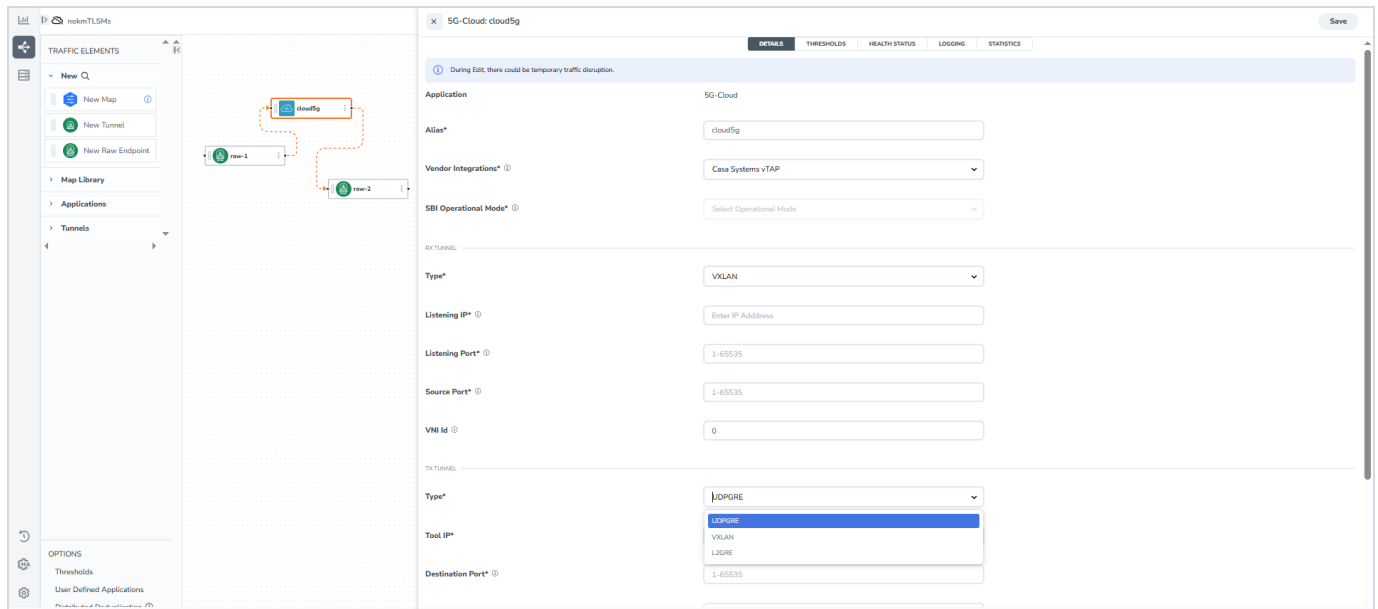


You can add a 5G-Cloud application to:

- **New Monitoring Session** - Add the 5G-Cloud application after creating a new Monitoring Session and when the GigaVUE-FM canvas appears. Refer to *Create a Monitoring Session* section in the respective GigaVUE Cloud Suite Deployment Guide.
- **Existing session** - Select any existing Monitoring Session and go to **TRAFFIC PROCESSING** tab. The GigaVUE-FM canvas appears.

To add a 5G-Cloud application:

1. In the canvas, drag and drop the 5G-Cloud application and select **Details**. The 5G-Cloud quick view appears.



2. On the application quick view, enter or select the required information as described in the following table:

Field	Description
Application	The name 5g-Cloud appears by default.
Alias	Enter the alias name as cloud5g .
Vendor Integrations	From the drop-down list, select Casa Systems vTAP .
RX Tunnel (Specifies the tunnel configuration from GVHTTP2 to 5G-Cloud)	
Type	Specify the tunnel type. VXLAN is selected by default.
Listening IP	Specify the tunnel's local listen IP address (TX tunnel destination IP address used in GVHTTP2) to receive the packet.
Listening Port	Specify the tunnel's local listening port to bind to receive the packet. The application will listen to the traffic coming to the specified port. Enter a value between 1 and 65535.
Source Port	Specify the tunnel destination port from where the packets will be sent. Enter a value between 1 and 65535.
VNI Id	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215. The default value is 0.
TX Tunnel	
Type	Select the tunnel type from the drop-down list. The available tunnel types are: • UDPGRE • VXLAN • L2GRE

Tool IP	Specify the remote IP address to which the packet will be sent.
Destination Port	Specify the tunnel destination port where the packet will be sent. Enter a value between 1 and 65535.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the tunnel source port to bind for sending the packet. Enter a value between 1 and 65535.
VNI ID (Applicable only when the selected tunnel type is VXLAN)	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215.
L2GRE Key (Applicable only when the selected tunnel type is L2GRE)	Specify the key for the L2GRE tunnel type. Enter a value between 0 and 4294967295.
Advanced Setting	
Tool MTU	Specify the tool port MTU. Note: For V Series Node version 6.8.00 and above, the range should be between 1400 and 8800. The default value is 8800. For V Series Node version below 6.8.00, range should be between 1500 and 8800. The default value is 8800.
Log Directory	Specify the path to store the log files.
Log Level	In the tunnel log level drop-down list, select the severity log level of the events from the following options: • None • Fatal • Error • Notification • Information • Debug

Downloading Logs for 5G-Cloud application

You can view the log files of a V Series Node or download them as CSV or .txt file.

To download the log files to a local environment:

1. Go to **Traffic > VIRTUAL** > select your cloud platform.
2. Select the required Monitoring Session and go to **TRAFFIC PROCESSING** tab. On the **cloud5g** application, click the  menu button and select **Details**. Go to **LOGGING** in the quick view. The **Logging** page displays the logs currently available.
3. The **CLOUD5G Logging** page displays the logs currently available. You can download the preferred logs by selecting the required Days, Timestamps, File Name, and Type (TextLog and FlowStats) details.
4. Select the log files to download, and then click **Download Files** from the **Actions** menu.

5. The system downloads the selected files to your local environment.

Limitations

- The 5G-Cloud application does not validate the VNI ID configured by the user in the GVHTTP2 application when processing the VXLAN packets.
- The VNI ID configured by the user will not be validated while processing the packets received on the ingress interface. So, the 5G-Cloud application will not drop the VXLAN received on the ingress interface if the VNI ID received in the packet does not match the VNI ID configured by the user.
- After deploying the Monitoring Session from GigaVUE-FM, users can only change the following configuration parameters for the GVHTTP2 application:
 - Server (Listen IP Address and Port Number)
 - VXLAN (Source IP and Port Number)
 - VXLAN (Destination IP and Port Number)
- After deploying the Monitoring Session from GigaVUE-FM, users can only change the following configuration parameters for the 5G-Cloud application:
 - Ingress VXLAN (Listen IP, Listen Port Number, and Source Port Number)
 - Egress UDP-GRE/L2GRE/VXLAN Tunnels (Destination IP Address, Destination Port, Source IP, and Source Port)

Rules and Notes

- On a V Series Node, only one application (GVHTTP2 or 5G-Cloud or AMX) can be deployed across Monitoring Sessions.
- GVHTTP2, 5G-Cloud, and AMX applications should not be combined with general GigaSMART applications in a Monitoring Session or across Monitoring Sessions.
- For GVHTTP2, 5G-Cloud, and AMX applications, the source and destination links should be Raw Endpoints.
- Support for GVHTTP2, 5G-Cloud, and AMX applications is limited to 'Customer Orchestrated Source' tapping type.
- The 5G-Cloud and GVHTTP2 applications require the "VBL-ADD-ADV5GC" or "VBL-ADD-5GC" license.
- To deploy a Monitoring Session, ensure that the 'HTTP2 Listening IP address' and 'TX Tunnel Source IP address' in GVHTTP2 corresponds to the IP addresses of one of the V Series Node interfaces.
- To deploy a Monitoring Session, ensure that the 'RX Tunnel Listening IP address' and 'TX Tunnel Source IP address' in 5G-Cloud correspond to the IP addresses of one of the V Series Node interfaces.
- To deploy a Monitoring Session, ensure that the TX Tunnel Destination IP address used in GVHTTP2 and the RX Tunnel Listening IP address used in 5G-Cloud are the same.

NOTE: For information on statistics details of Casa vTAP for GVHTTP2 and 5G-Cloud applications, refer to [Appendix - Casa vTap Statistics](#).

5G-Cloud Oracle and Nokia SCP Support

GigaVUE V Series Node supports receiving data from 5G network functions in Oracle SCP and Nokia SCP input formats. In both Oracle and Nokia SCP, 3GPP standard method is followed, which has all the standard network components implemented.

Oracle SCP

Oracle systems input format is HTTP2/HTTP2S POST over TCP with TLS enabled. In Oracle SCP, the 5G-Cloud application synthesizes the packets and egresses them to the tool port after it has received all the 4-leg transactions. Oracle SCP processing in the 5G-Cloud application supports converting the discovery and the 4-legged (consumer, SCP, and producer) transactions to packets as per 3GPP Model C and Model D.

Model C

The Consumer knows the producer and sends messages through SCP. Model C comprises of 4-legged transactions between the consumer, SCP, and the producer. The 5G-Cloud application converts the 4-legged transactions to packets and sends them to the probe.

Model D

SCP sends discovery messages to discover the producer after receiving the messages from the consumer. Model D comprises of 2-legged transactions between the consumer and the SCP, 4-legged transactions between the SCP, SCP discovery, and the NRF to find the producer, and the 2-legged transactions between the producer and the SCP. The 5G-Cloud application converts the 4-legged transactions between the consumer, SCP, and the producer to packets and sends them to the probe. The 5G-Cloud application also converts the discovery transactions between the SCP and the NRF and sends them to the probe.

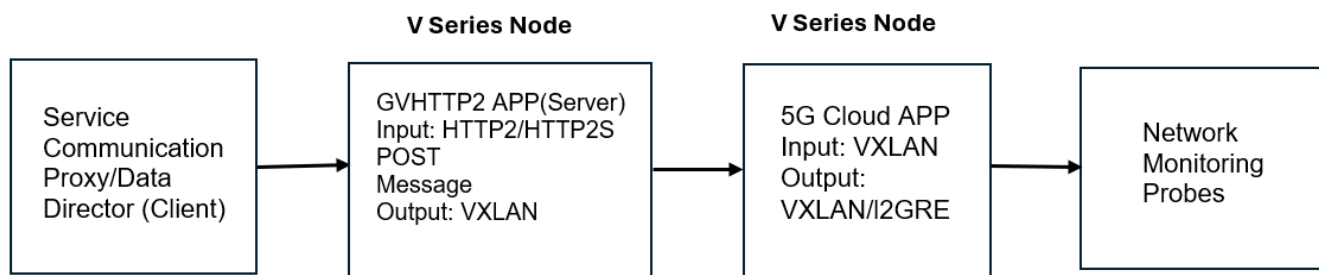
5G- Cloud application will ensure that both the discovery transaction and the 4-legged transaction are transmitted in order, to the connected tool or probe.

Nokia SCP

In Nokia SCP, traffic is mirrored between control functions using the HTTP2 protocol. This traffic is mirrored from a service called SCP (Service Control Proxy), a centralized point through which all the communications between all the control plane functions pass. SCP encrypts all the messages that are going across the control plane network functions and forwards that information in JSON-encoded format to GVHTTP2.

Both Model C and Model D transactions can be received from the SCP. However, Model D cannot be identified as Model D, because a separate message id is used for the discovery messages. In the case of Model D, SCP will include the Model D discovery transactions that happened with NRF along with the network function communication. Therefore, 6 transactions will be forwarded from SCP for a single request and response pair between any two network functions. The Model C transactions will be processed in 2 modes:

- **Transparent (2 legged):** The 5G-Cloud application will synthesize a direct transaction between the network functions. The 4-legged transactions received between the consumer, SCP, and the producer are synthesized to look like 2-legged transactions between the consumer and the producer.
- **Inbound and outbound (4 Legged):** The 5G-Cloud application will synthesize indirect transactions, meaning all transactions between any network function will go via SCP. All the transactions received in Model C or Model D are synthesized and sent to the probes.



GVHTTP2 Application

The first application, GVHTTP2, acts as an HTTP2 server, receives the data over HTTP2 frame and establishes a TCP connection with multiple Oracle SCP/DD or Nokia SCP pods. It receives the HTTP2 headers and stores them in a temporary buffer. Once it receives all the headers and body of that stream, it acknowledges back to the client. The application will extract the HTTP2 header and HTTP2 body, encapsulate the data into a VXLAN header, and send it out over the VXLAN tunnel to the next application, 5G-Cloud.

5G-Cloud Application

The 5G-Cloud application receives and decapsulates the VXLAN packet. It extracts the HTTP2 body, parses the SCP/DD JSON mirrored message, and associates the mirrored message transaction ID to track the complete transaction. It then synthesizes TCP Flow and HTTP2 Session representing full 5G CNF / SCP / 5G CNF transaction data and sends it out over L2GRE/VXLAN tunnel to the probe.

The 5G-Cloud application runs in Oracle SCP, Nokia SCP Transparent, and Nokia SCP Inbound-Outbound modes.

- In Nokia SCP Inbound-Outbound mode, both Inbound (between Consumer and SCP) and Outbound (between SCP and Producer) traffic is synthesized and sent to the connected Tool port. In Nokia SCP Transparent mode, only Inbound (between Consumer and SCP) traffic is processed and sent to the Tool Port.
- In the Nokia SCP Transparent mode, the 5G-Cloud Application will drop the Outbound traffic from the SCP (if received in the input).
- In the Nokia SCP Transparent mode, the Producer replaces the SCP in transactions between the Consumer and the SCP.
- In the Nokia SCP Transparent mode, authority header value will be replaced (if the replace authority configuration is enabled).

Configuration of 5G-Cloud Oracle/Nokia SCP

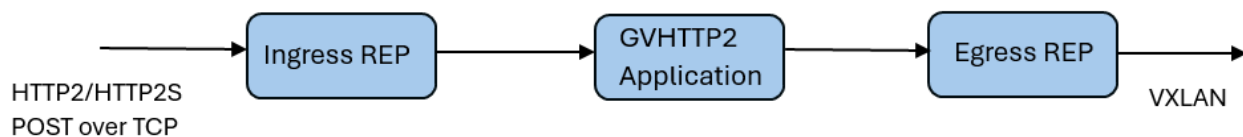
To configure the GVHTTP2 and 5G-Cloud applications in GigaVUE-FM, refer to the following sections:

- [Configuration of GVHTTP2 Application for Oracle SCP/Nokia SCP](#)
- [Configuration of 5G-Cloud Application for Oracle SCP/Nokia SCP](#)

Configuration of GVHTTP2 Application for Oracle SCP/Nokia SCP

In GigaVUE-FM, you must do the following to add the GVHTTP2 application in the Monitoring Session of a Monitoring Domain:

1. Create an ingress REP (Raw End Point) to receive the HTTP2/HTTP2S data over TCP. Refer to *Create Raw Endpoint* section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) for more information on creating a REP.
2. Add the GVHTTP2 application in the Monitoring Session.
3. Create a link between ingress REP and the GVHTTP2 application.
4. Create egress REP.
5. Create a link between the GVHTTP2 application and egress REP.



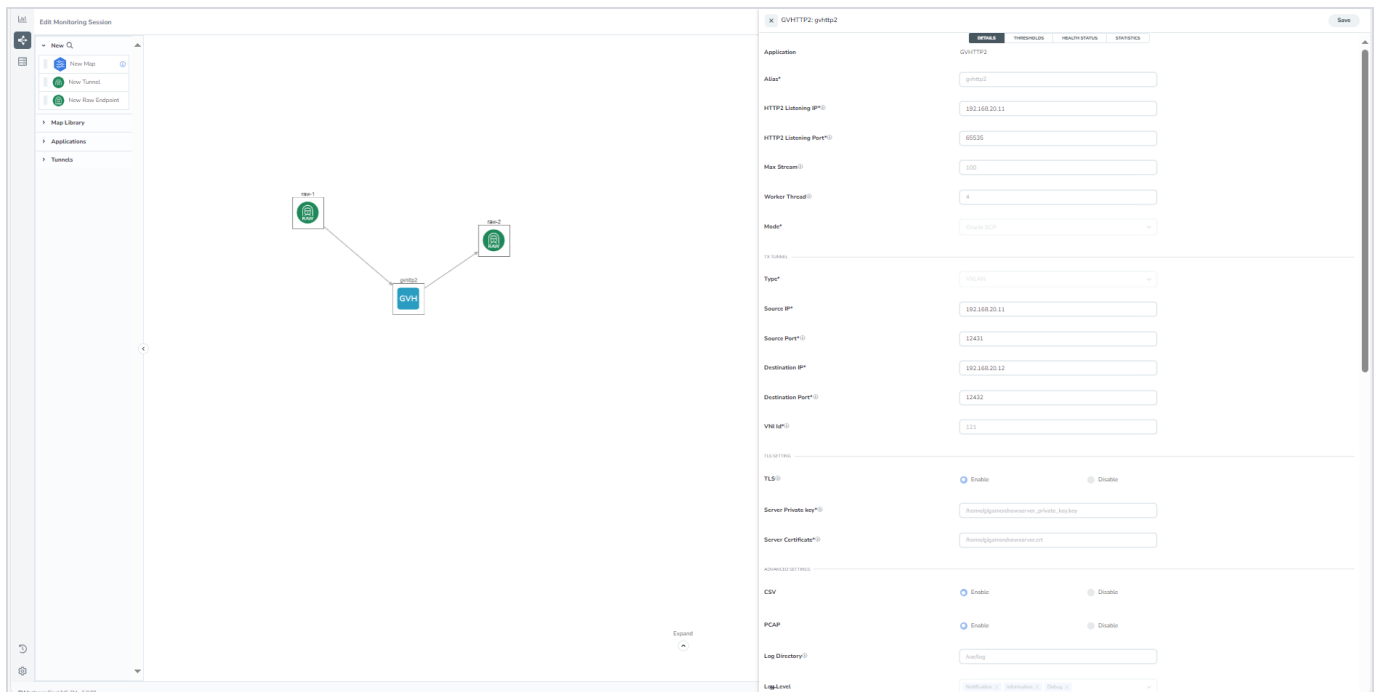
You can add a GVHTTP2 application to:

- New Monitoring Session - You can add the GVHTTP2 application after creating a new Monitoring Session and when the canvas appears.

- Existing Monitoring Session - Click **Edit** on the existing Monitoring Session, and the GigaVUE-FM canvas appears.

To add a GVHTTP2 application:

- In the canvas, drag and drop the GVHTTP2 application and select **Details**. The GVHTTP2 quick view appears.



- On the application quick view, enter or select the required information as described in the following table:

Field	Description
Application	The name GVHTTP2 appears by default.
Alias	Enter the alias name as gvhttp2 .
HTTP2 Listening IP	Specify the HTTP2 IP address. The application will listen to the traffic on the specified IP address.
HTTP2 Listening Port	Specify the HTTP2 Port. The application will listen to the traffic on the specified port.
Max Stream	Specify the maximum number of concurrent streams in one HTTP2 session. Enter a value between 1 and 100. The default value is 100.
Worker Thread	Specifies the number of worker threads. Enter a value between 1 and 128. The default value is four.
Mode	Select Oracle SCP or Nokia SCP as mode from the drop-down menu.
TX Tunnel (Specifies the tunnel configuration from GVHTPP2 to 5G-Cloud)	
Type	Specify the tunnel type. VXLAN is selected by default.

Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the source port to bind for sending the packet. Enter a value between 1 and 65535.
Destination IP	Specify the destination IP address to which packets will be sent.
Destination Port	Specify the destination port where packets will be sent. Enter a value between 1 and 65535.
VNI Id	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215. The default value is zero.
TLS Setting	
TLS	Select a TLS/SSL Monitor Mode from one of the following options: ▪ Enable—When the monitor mode is enabled, the TLS/SSL decryption or encryption is off. ▪ Disable—This is the default value. When the monitor mode is disabled, the TLS/SSL decryption or encryption is on.
Server Private key*	Specify the server private key only when TLS is enabled.
Server Certificate*	Specify server certificate only when TLS is enabled.
Advanced Setting	
CSV	Enable or disable the CSV log level.
PCAP	Enable or disable the PCAP log level.
Log Directory	Specify the path to store the log files.
Log Level	In the log level drop-down list, select the severity log level of the events from the following options. The default value level is Notification. • Notification • Information • Debug

Download Logs - GVHTTP2 application

You can view the log files of a V Series Node or download them as .CSV or .txt file.

To download the log files to a local environment:

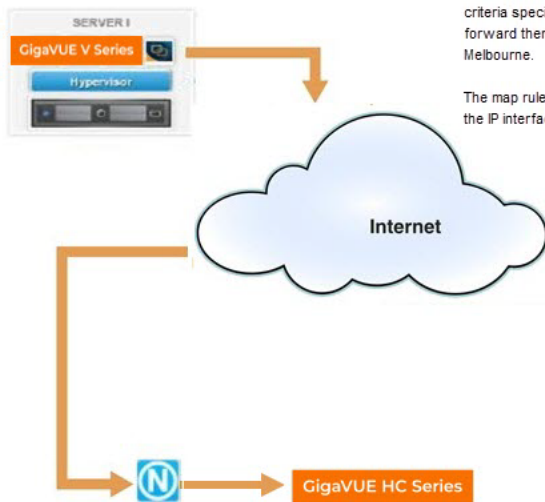
1. Go to **Traffic > VIRTUAL** > select your cloud platform.
2. Select the required Monitoring Session and click the **APPS LOGGING** link.
3. The **GVHTTP2 Logging** page displays the logs currently available. You can download the preferred logs by selecting the required Days, Timestamps, File Name, and Type (TextLog and FlowStats) details.
4. Select the log files to download, and then click **Download Files** from the **Actions** menu.
5. The system downloads the selected files to your local environment.

Configuration of 5G-Cloud Application for Oracle SCP/Nokia SCP

In GigaVUE-FM, you must do the following to configure the 5G-Cloud application in the Monitoring Session of a Monitoring Domain:

1. Create ingress REP to extract the HTTP2 body. Refer to *Create Raw Endpoint* section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) for more information on creating a REP.
2. Add the 5G-Cloud application in the Monitoring Session.
3. Create a link between ingress REP and the 5G-Cloud application.
4. Create egress REP.
5. Create a link between the 5G-Cloud application and egress REP.

GigaVUE V Series in Sydney



The GigaVUE V Series map rules in Sydney take virtual packets matching the criteria specified by the map rules, encapsulate them in UDP packets, and forward them across the Internet to the receiving GigaVUE HC Series in Melbourne.

The map rules include the destination IP address and UDP port (the address of the IP interface associated with the network port in Melbourne).

GigaVUE HC Series with GigaSMART in Melbourne

IP interface associated with network port 1/1/x3 in Melbourne decapsulates traffic arriving from Sydney and makes it available for standard GigaVUE packet distribution to local tool ports. The decapsulation operation bound to IP interface associated with network port 3 as part of a map specifies the listening UDP port matching the one configured in Sydney.

Adding 5G-Cloud Application in Oracle SCP/Nokia SCP

Prerequisites

The pre-requisite to add a 5G-Cloud Application in Oracle SCP/Nokia SCP is:

- You must upload CSV files containing a valid FQDN, NF Instance, and User Agent ID's and a valid IPv4/IPv6 addresses. To upload the CSV file, refer to [Adding CSV file for IP Mapping](#).

You can add a 5G-Cloud application to:

- New Monitoring Session - You can add the 5G-Cloud application after creating a new Monitoring Session and when the canvas appears.
- Existing session - Click **Edit** on the existing Monitoring Session, and the GigaVUE-FM canvas appears.

To add a 5G-Cloud application:

- In the canvas, drag and drop the 5G-Cloud application and select **Details**. The 5G-Cloud quick view appears.

The screenshot displays the GigaVUE-FM interface. On the left, the 'Edit Monitoring Session' canvas shows a network diagram with a central '5G-Cloud' application icon connected to two endpoints. On the right, the '5G-Cloud cloud5g' configuration form is open, showing the 'DETAILS' tab. The form includes the following fields:

- Application:** cloud5g
- Alias:** cloud5g
- Mode:** cloud5g
- RX TUNNEL:**
 - Type:** RX TUNNEL
 - Listening IP:** 192.168.20.12
 - Listening Port:** 12432
 - Source Port:** 12431
 - VNI id:** 121
- TX TUNNEL:**
 - Type:** TX TUNNEL
 - Test IP:** 192.168.10.16
 - Destination Port:** 4789
 - Source IP:** 192.168.10.12
 - Source Port:** 12433
 - L2ONE Key:** 122
- ADVANCED SETTINGS:**
 - Test MTU:** 8800
 - Log Directory:** /var/log
 - Log Level:** Debug
- SCP CONFIG:**
 - FQDN Mapping:** cloud5g
 - NF Instance Mapping:** cloud5g

- On the application quick view, enter or select the required information as described in the following table:

Field	Description
Application	The name 5g-Cloud appears by default.
Alias	Enter the alias name as cloud5g .
Mode	From the drop-down list, select the required mode from the following options: - Oracle SCP - Nokia SCP Transparent - Nokia SCP Inbound/Outbound
RX Tunnel (Specifies the tunnel configuration from GVHTPP2 to 5G-Cloud)	

Type	Specify the tunnel type. VXLAN is selected by default.
Listening IP	Specify the tunnel's local listen IP address (TX tunnel destination IP address used in GVHTTP2) to receive the packet.
Listening Port	Specify the tunnel's local listening port to bind to receive the packet. The application will listen to the traffic coming to the specified port. Enter a value between 1 and 65535.
Source Port	Specify the tunnel destination port from where the packets will be sent. Enter a value between 1 and 65535.
VNI Id	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215. The default value is zero.
TX Tunnel	
Type	Specify the tunnel type.
Tool IP	Specify the remote IP address to which the packet will be sent.
Destination Port	Specify the tunnel destination port where the packet will be sent. Enter a value between 1 and 65535.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the tunnel source port to bind for sending the packet. Enter a value between 1 and 65535.
VNI Id (Applicable only when the selected tunnel type is VXLAN)	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215.
L2GRE Key (Applicable only when the selected tunnel type is L2GRE)	Specify the key for the L2GRE tunnel type. Enter a value between 0 and 4294967295.
Advanced Setting	
Tool MTU	Specify the tool port MTU. Note: For V Series Node version 6.8.00 and above, the range should be between 1400 and 8800. The default value is 8800. For V Series Node version below 6.8.00, range should be between 1500 and 8800. The default value is 8800.
Log Directory	Specify the path to store the log files.
Log Level	In the tunnel log level drop-down list, select the severity log level of the events from the following options: • None • Fatal • Error • Notification • Information

	• Debug
SCP Config	
FQDN Mapping	Specify the alias name created for the uploaded FQDN table CSV file. You can also add new FQDN by utilizing the ADD button. Note: Header details: gigamon@test-5gc-new:/var/log/cloud5g_tabledir\$ cat FQDN.txt FQDN,IngressIP1,IngressIP2,IngressPort,EgrIP,NFType,NFLocation (The fields fqdnID and ingressIPAddress1 are mandatory. All other fields are optional) Examples - 5G-Cloud FQDN Entries: Oracle SCP: FQDN.txt:scp1.pp2.scp.5gc.mnc001.mcc208.3gppnetwork.org,10.64.104.30,10.64.104.36,9443,10.64.104.45,SCP,plolp Nokia SCP: s25scp01.scp.5gc.mnc003.mcc525.3gppnetwork.org,172.23.13.187,,8080,,SCP,plolp
NF Instance Mapping	Specify the alias name created for the uploaded NFID table CSV file. You can also add new NF Instance by utilizing the ADD button. Note: Header details: gigamon@test-5gc-new:/var/log/cloud5g_tabledir\$ cat NFID.txt NFID,IngressIP1,IngressIP2,IngressPort,EgrIP,NFType,NFLocation (The fields NFID and ingressIP1 are mandatory. All other fields are optional) Examples - 5G-Cloud NFID Entries: • Oracle SCP: NFID.txt:04fba086-6ac1-4472-9ee3-cf10e57849f8,10.64.107.85,10.64.107.79,8080,,SMF,plolp • Nokia SCP: 8b94c7ee-d750-4bcd-95be-634b31a5fa0d,172.23.14.4,,8080,,AMF,jeolp
User Agent Mapping	Specify the alias name created for the uploaded User Agent table CSV file. You can also add new User Agent by utilizing the ADD button. Note: Header details: gigamon@test-5gc-new:/var/log/cloud5g_tabledir\$ cat UA.txt UserAgent,IngressIP1,NFType,NFLocation (The fields useragentID and ingressIPAddress are mandatory. All other fields are optional) Examples - 5G-Cloud User Agent Entries: • Oracle SCP: pp5gs2nd15gcam01,10.64.106.67,AMF,jeolp • Nokia SCP: pp5gs2nd15gcam01,10.64.106.67,AMF,plolp pp5gs2nd15gcam02,10.64.106.107,AMF,plolp ofrpp25gcsmsf01,10.64.106.138,SMF,jeolp
SCP Advanced Config	
No. of TCP Flows	Specify the total number of concurrent TCP flows. Enter a value between 128 and 2048. The default value is 1024.
No. of Transaction Flows	Specify the total number of Transaction Stream Flows allocated for tracking active Transaction Streams. Enter a value between 128 and 5500. The default value is 2048.

TCP Flow Timeout	Specify the TCP flow timeout ranging between 0 to 7200. The default value is 900.
SCP Transaction Timeout	Specify the SCP transaction timeout value ranging between 1 and 300. The default value is 10. Note: The recommended timeout value is between 10 and 20 seconds. An increase in the transaction timeout value will impact the total number of transactions that can be processed in parallel.
Minimum TCP Client Port	Specify the minimum value to be used for TCP client port ranging between 1023 and 65535. The default value is 32768.
Maximum TCP Client Port	Specify the maximum value to be used for client port ranging between 1023 and 65535. The default value is 36863.
Header Index	Enable or disable the header indexing flag from the available options. The default value is disable.
Header Compression Code Note: HTTP/2 requests and responses typically contain a large number of redundant headers. HTTP/2 uses header compression to compress headers significantly.	Enable or disable the header compression code from the available options. The default value is disable.
Gigamon Header Note: Helps in the debugging process to identify all transactions.	Enable or disable the Gigamon Header from the available options. The default value is Enable.
Nokia Use 3gpp Target	Specify the value which upon detecting producer IP/FQDN, treats the 3gpp Target API Root to be predictive of the Producer IP if value is non-zero as either enable or disable. The default value

API Root (Applicable only when the selected mode is Nokia SCP Transparent)	is disable.
Nokia Replace Authority (Applicable only when the selected mode is Nokia SCP Transparent)	Specify the value which upon detecting producer IP/FQDN, treats the 3gpp Target API Root to be predictive of the Producer IP if the value is non-zero as either enable or disable. The default value is disable.
Packet Capture Level	Select the packet capture level from the drop-down list: • All • Receive • Transmit • None
5G-Cloud Log Level	Select the required 5G-Cloud CSV log level from the drop down list. The default value is None. • All • Flow • Message • Transaction • None

Download Logs - 5G-Cloud application

You can view the log files of a V Series Node or download them as .CSV or .txt file.

To download the log files to a local environment:

1. Go to **Traffic > VIRTUAL** > select your cloud platform.
2. Select the required Monitoring Session and click the **APPS LOGGING** link.
3. The **CLOUD5G Logging** page displays the logs currently available. You can download the preferred logs by selecting the required Days, Timestamps, File Name, and Type (TextLog and FlowStats) details.

4. Select the log files to download, and then click **Download Files** from the **Actions** menu.
5. The system downloads the selected files to your local environment.

Adding CSV file for IP Mapping

To add the CSV file for IP mapping:

1. Go to **Inventory > VIRTUAL >** select your cloud platform, and then click **Settings > 5G-Apps**. The 5G-Apps Configuration page appears.
2. Click **New**. Enter the name for the CSV file in the **Alias** field
3. Select any of the following from the **Type** as per the requirement:
 - **5G-Cloud FQDN** - Adding the CSV file containing a valid FQDN ID and a valid IPv4/IPv6 address for IP mapping. Adding FQDN is mandatory.
 - **5G-Cloud NF Instance** - Adding the CSV file containing a valid NF instance ID and a valid IPv4/IPv6 address for IP mapping.
 - **5G-Cloud UA** - Adding the CSV file containing a valid user agent ID and a valid IPv4/IPv6 address for IP mapping.
4. Click **Choose File** in **FileName** field to upload the CSV file into GigaVUE-FM.
5. Click **Validate** to validate the CSV file.
6. Click **Save** to add the CSV file.

NOTE: For Oracle SCP, configuration of FQDN Mapping, NF Instance Mapping, and User Agent Mapping are mandatory. For Nokia SCP Transparent and Nokia SCP Inbound/Outbound, configuration of FQDN Mapping is mandatory.

Limitations

- The following configuration parameters for the GVHTTP2 application are non-editable and can be configured only during the initial configuration:
 - Mode
 - TX Tunnel – txType
 - Worker thread
 - RX VNI Id
 - Max Streams
 - TLS configuration
 - Log Level
 - Log Directory
- The following configuration parameters for the 5G-Cloud application are non-editable and can be configured only during the initial configuration:
 - Mode

- TX Tunnel – txType
- RX Tunnel - rxType
- RX VNI Id
- Tool MTU
- Log Directory
- Log Level
- Header Index
- Header Compression Code
- Packet capture log level
- SCP log level
- Gigamon Header
- FQDN Mapping
- NF Instance Mapping
- User Agent Mapping

Rules and Notes

- The 5G-Cloud and GVHTTP2 applications require the "VBL-250T-ADD-5GC" license.
- It is recommended to use SRIOV enabled drivers for better performance and higher throughput. Refer to **Procedure to deploy V Series Node in VMware ESXi with SR-IOV Adapte** topic in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration guide for more details.
- On a V Series Node, only one application (GVHTTP2 or 5G-Cloud or AMX) can be deployed across Monitoring Sessions.
- GVHTTP2, 5G-Cloud, and AMX applications should not be combined with general GigaSMART applications in a Monitoring Session or across Monitoring Sessions.
- For GVHTTP2, 5G-Cloud, and AMX applications, the source and destination links should be Raw Endpoints.
- Support GVHTTP2, 5G-Cloud, and AMX applications is limited to 'Customer Orchestrated Source' tapping type.
- Configuration of GVHTTP2 and 5G-Cloud in V Series Node will fail in versions less than v6.7.00.
- To deploy a Monitoring Session, ensure that the 'HTTP2 Listening IP address' and 'TX Tunnel Source IP address' in GVHTTP2 correspond to the IP addresses of one of the GigaVUE V Series Node interfaces.
- To deploy a Monitoring Session, ensure that the 'RX Tunnel Listening IP address' and 'TX Tunnel Source IP address' in 5G-Cloud correspond to the IP addresses of one of the GigaVUE V Series Node interfaces.
- To deploy a Monitoring Session, ensure that the TX Tunnel Destination IP address used in GVHTTP2, and the RX Tunnel Listening IP address used in 5G-Cloud are the same.

- When you have already deployed the 5G-Cloud application with all the table files uploaded, you should undeploy and redeploy the Monitoring Session again with the updated files to update the table.
- In the GVHTTP2 application, when the TLS/SSL configuration is enabled, the private key and certificate path must be configured.
- Before upgrading GigaVUE V Series Node, user should undeploy the Monitoring Session where the GVHTTP2 application is deployed and take the backup of the SSL certificate and private key files. Following the upgrade, user should manually install/copy the private key and the certificate file in GigaVUE GigaVUE V Series Node and redeploy the GVHTTP2 application.
- To upload the table configuration file in CSV format, go to Inventory -> Virtual ->Settings -> 5G-Apps, enter the alias, type the CSV file name, and upload it.
- To download the files, go to Inventory -> Virtual ->Settings -> 5G-Apps and select the alias name to be downloaded.
- From release version 6.9.00, the maximum Transaction Flow value for GigaVUE V Series Nodes with memory less than 32 GB is 5500. For V Series Nodes classified as extra-large with memory greater than 32 GB, the maximum Transaction Flow value is 26000.
- From release version 6.9.00, to make use of the multithreading support for egress/ingress tunnels in GVHTTP2/5G-Cloud applications, you should update the thread count after the GigaVUE V Series Node is upgraded.
- The configuration of the 5G-Cloud application should be performed on extra-large VMs.
 - Configuration specifications for extra large VM:
 - vCPUs: 12-20
 - RAM: 32 GB
 - Disk: 160 GB
 - Supported Ports: Management Ports, Tunneling Ports, and 2 Data Ports

FHA Dashboards for 5G-Cloud Applications

After configuring the GVHTTP2 and 5G-Cloud applications, you can monitor the statistics for Oracle SCP and Nokia SCP by the reports displayed in the Dashboard.

To access the details, refer to **FHA Dashboards for 5G-Cloud Applications** topic in GigaVUE Fabric Management Guide.

5G-Cloud Ericsson SCP Support

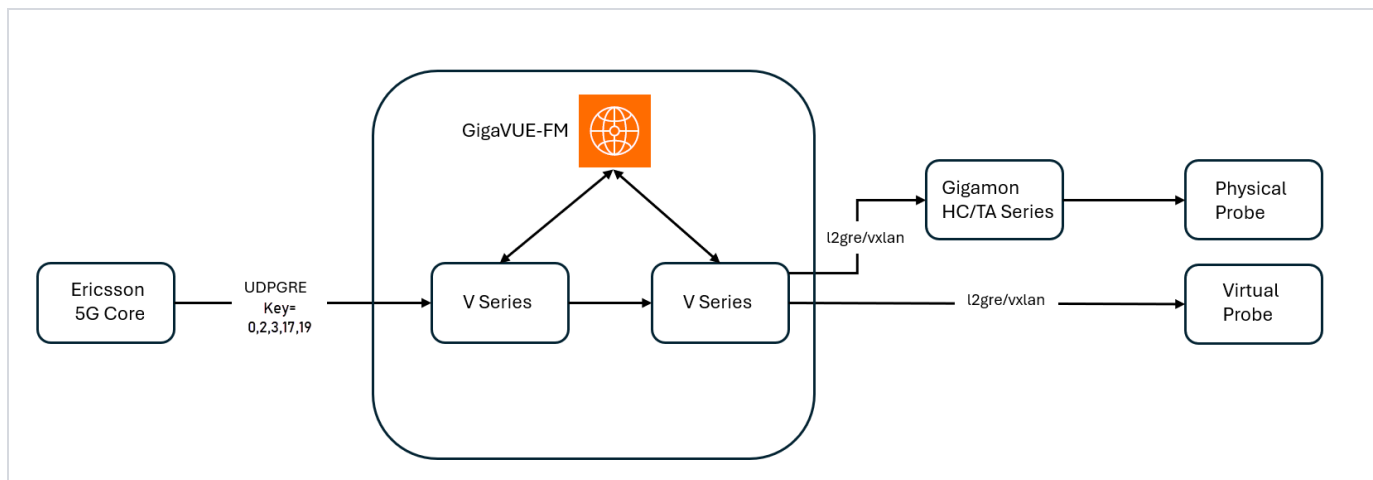
The 5G Core follows a service-based architecture where control plane network functions communicate using the HTTP2 protocol. In Ericsson SCP Mode, HTTP2 transactions are mirrored through the Service Communication Proxy (SCP) and encapsulated using UDP-GRE for further processing.

Ericsson SCP

In **Ericsson vTAP**, traffic is tapped from the Packet Core Controller (PCC), including AMF and SMF, in Layer 7 HTTP SBI JSON format. The 5G SBI application supports this PCC traffic, ensuring efficient processing and monitoring. Refer to [5G-Service Based Interface Application](#).

In **Ericsson SCP** mode, the Service Communication Proxy (SCP) mirrors 5G SBI traffic within the Cloud Core Signaling Controller, capturing communication between multiple network functions via SCP.

The 5G-Cloud application in GigaVUE V Series Nodes is enhanced to receive and process traffic from the Ericsson SCP and forward it to the monitoring tools. This setup supports both configuration and visualization through GigaVUE-FM integration.



Traffic from the Ericsson 5G Core is encapsulated using UDP-GRE tunnels, with specific keys 3, 17, and 19 to identify different traffic flows from SCP. GigaVUE-FM serves as the centralized management platform orchestrating the visibility fabric, which includes the V Series Nodes. The V Series Nodes inspect, aggregate, and process the incoming packets.

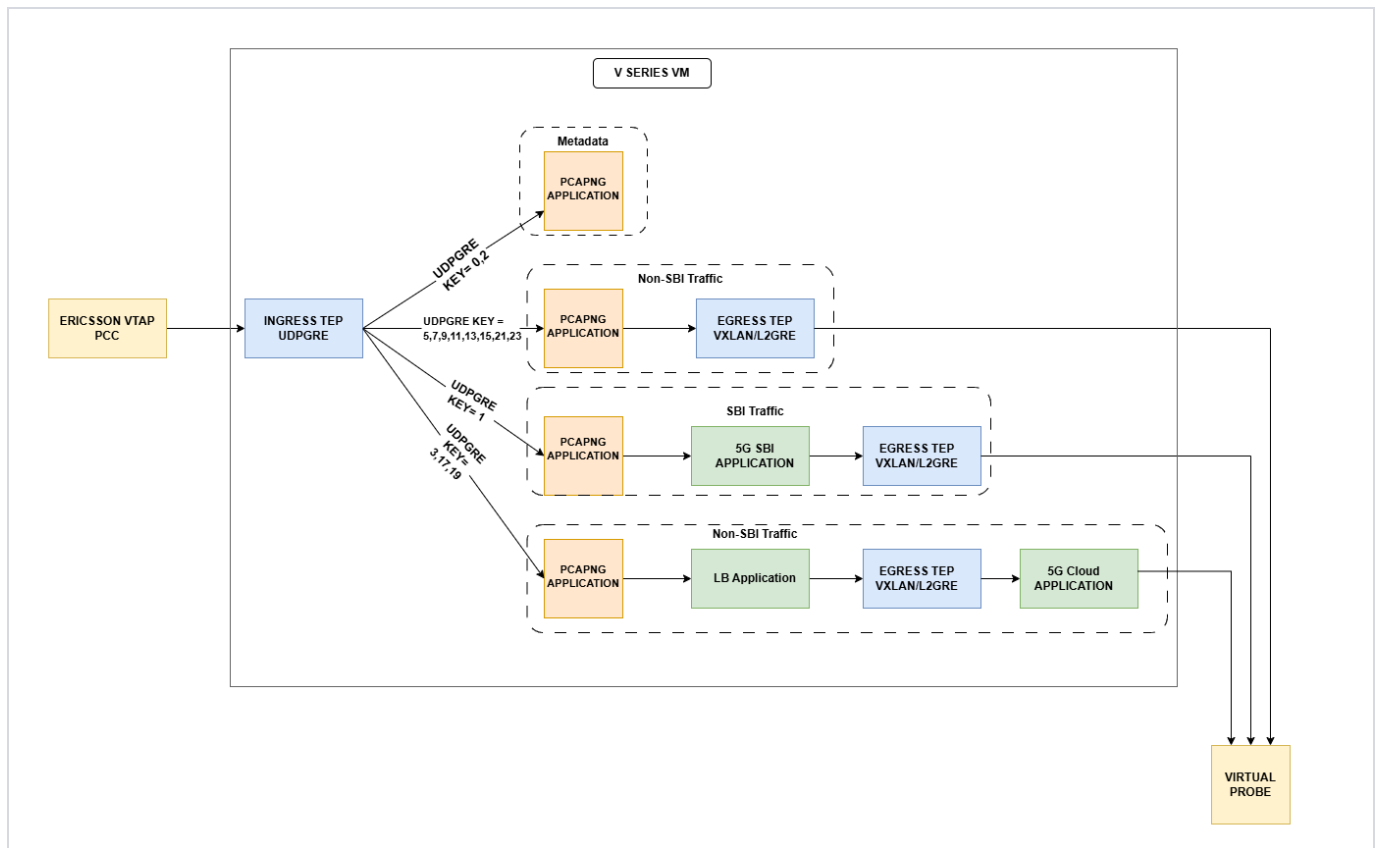
After processing, traffic is encapsulated using L2GRE or VXLAN tunneling protocols and forwarded to either physical or virtual probes as follows:

- **Physical Probe:** If IP connectivity is not available, the traffic is sent to a GigaVUE HC/GigaVUE TA Series device, which serves as a traffic aggregator and distributor. The device decapsulates and distributes the traffic to the probe.
- **Virtual Probe:** If IP connectivity is available, the processed traffic is forwarded directly to virtual probe for detailed traffic inspection and analytics.

This end-to-end solution ensures comprehensive visibility into 5G network traffic, facilitating efficient monitoring and performance analysis across both physical and cloud-based infrastructures.

How Ericsson SCP Solution works

The following image shows the block diagram of the data flow in the V Series Nodes.



The encapsulated traffic enters the system, and based on the key values, is passed through a PCAP-NG, 5G SBI, and LB application to capture and monitor the data.

For traffic mirroring and flow processing in Ericsson VTap 5G Core network with key value 1, refer to [5G-Service Based Interface Application](#)

When traffic is processed through keys 3, 17, and 19, the **PCAPng** application reads and validates various blocks within received PCAPng files before forwarding them to the Load Balancing application. It processes data based on the packet type, which includes a combination of the following blocks.

1. Mandatory Blocks:
 - Section Header Block (SHB)
2. Optional Blocks:
 - Interface Description Block (IDB)
 - Enhanced Packet Block (EPB)
 - Simple Packet Block

- Name Resolution Block
- Interface Statistics Block

Also, the PCAPng application classifies domains by using Ericsson vTAP metadata and a configured domain table. Each Ericsson domain (for example, pc-mm, pc-sm, ccsn-5gc, ccrc-nrf, nrfagent-nrf, ccpc-pcf, sc-scp, sc-sepp) maps to a VLAN ID. The V Series applies this VLAN ID on the egress tunnel so downstream probes can distinguish traffic by Ericsson domain.

The domain table can also include others and unclassified to handle traffic that does not match known domains or cannot be classified. Refer to [PCAPng Application](#) for more details.

The **Load Balancing** application efficiently distributes traffic with different flow IDs across multiple cores, enabling parallel processing of packets with distinct stream IDs. It ensures that request and response frames with the same stream ID are processed sequentially within the same core, preventing race conditions where these frames might otherwise be handled in parallel across different cores. Refer to [Load Balancing](#).

The extracted data is encapsulated within a VXLAN and routed to the 5G-Cloud application. The 5G-Cloud application processes VXLAN packets by first decapsulating them to extract the HTTP2 headers and body. It then parses the EEVTAP TCP mirrored message and maps the transaction ID to track the full transaction.

After synthesizing the TCP flow and HTTP2 session to represent the complete 5G CNF/SCP/5G CNF transaction data, it forwards the data over an L2GRE/VXLAN tunnel to the probe.

You should enable VLAN Tagging on the egress tunnel (VXLAN or L2GRE) used with the domain-classification PCAPng instance so the tunnel applies the VLAN ID from the Domain VLAN Mapping table for each Ericsson domain. Refer to [Create Ingress and Egress Tunnels](#).



Notes:

- Ericsson SCP will process only Model C traffic.
- You can deploy traffic ingress applications together in a single V Series Node and Monitoring Session. However, for the 5G-Cloud and egress applications, you must deploy a separate Monitoring Session and V Series Node.
- You can configure either a single-tep or multi-tep setup for the egress tunnel. Switching between these configurations is not allowed; to make changes, you must undeploy and redeploy the Monitoring Session.
- Ensure that all V Series Nodes within a single Monitoring Domain are running the same version. Mixing different versions in the same Monitoring Domain may lead to inconsistencies when configuring Monitoring Session traffic elements.

Configuration of 5G-Cloud Ericsson SCP

In GigaVUE-FM, you must do the following to configure the 5G-Cloud application in the Monitoring Session of a Monitoring Domain in the V Series:

V Series Node 1:

S.No	Steps	Refer to
1	Configure UDP-GRE Ingress TEP to receive the HTTP2 messages. Note: You should configure individual UDP-GRE tunnels for each of the following key values: - Key Value 1: Ericsson vTAP - Key Values 3 and 17: Ericsson SCP	Create Ingress and Egress Tunnel (VMware vCenter) Create Ingress and Egress Tunnels (OpenStack) Create Ingress and Egress Tunnel (Third Party Orchestration)
2	Configure PCAPng application and link ingress TEP and PCAPng application instances in the Monitoring Session. NOTE: For Domain tagging configuration, refer to Configure the PCAPng Application for Domain Tagging section in PCAPng Application .	PCAPng Application
3	Configure LB application and link LB application and PCAPng application instances in the Monitoring Session.	Load Balancing
4	Create a VXLAN egress TEP. NOTE: Enable the Domain Tagging option when creating an egress tunnel to tag packets with the Ericsson domain specific VLAN IDs.	Create Ingress and Egress Tunnel (VMware vCenter) Create Ingress and Egress Tunnels (OpenStack) Create Ingress and Egress Tunnel (Third Party Orchestration)
5	Create a link between egress TEP and LB application.	

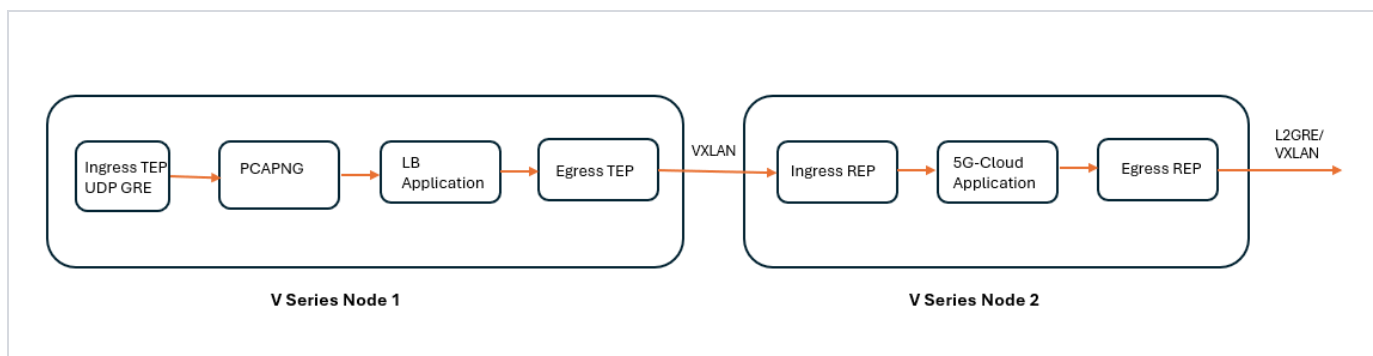


Note: When upgrading GigaVUE-FM with a Monitoring Session in V Series Node 1 to version 6.12 from an earlier release, follow these steps to ensure a successful migration:

- Undeploy the existing V Series Node 1 Monitoring Session.
- Delete any Egress VXLAN TEPs with the Multi-Tunnel feature enabled.
- Recreate the Egress VXLAN TEP with the required configuration and enable the Multi-Tunnel flag.
- Establish a Link connection between the LB application and the Egress VXLAN TEP.
- Deploy the Monitoring Session.

V Series Node 2:

S.No	Steps	Refer to
1	Create a ingress REP to extract the HTTP2 body.	Create Raw Endpoint (VMware vCenter) Create Raw Endpoint (OpenStack) Create Raw Endpoint (Third Party Orchestration)
2	Create a link between the VXLAN egress TEP and ingress REP.	
3	Add the 5G-Cloud application in the Monitoring Session.	5G-Cloud Application
4	Create a link between ingress REP and the 5G-Cloud application.	
5	Create egress REP.	Create Raw Endpoint (VMware vCenter) Create Raw Endpoint (OpenStack) Create Raw Endpoint (Third Party Orchestration)
6	Create a link between the 5G-Cloud application and egress REP.	



Add 5G-Cloud Application in Ericsson SCP

Pre-requisite:

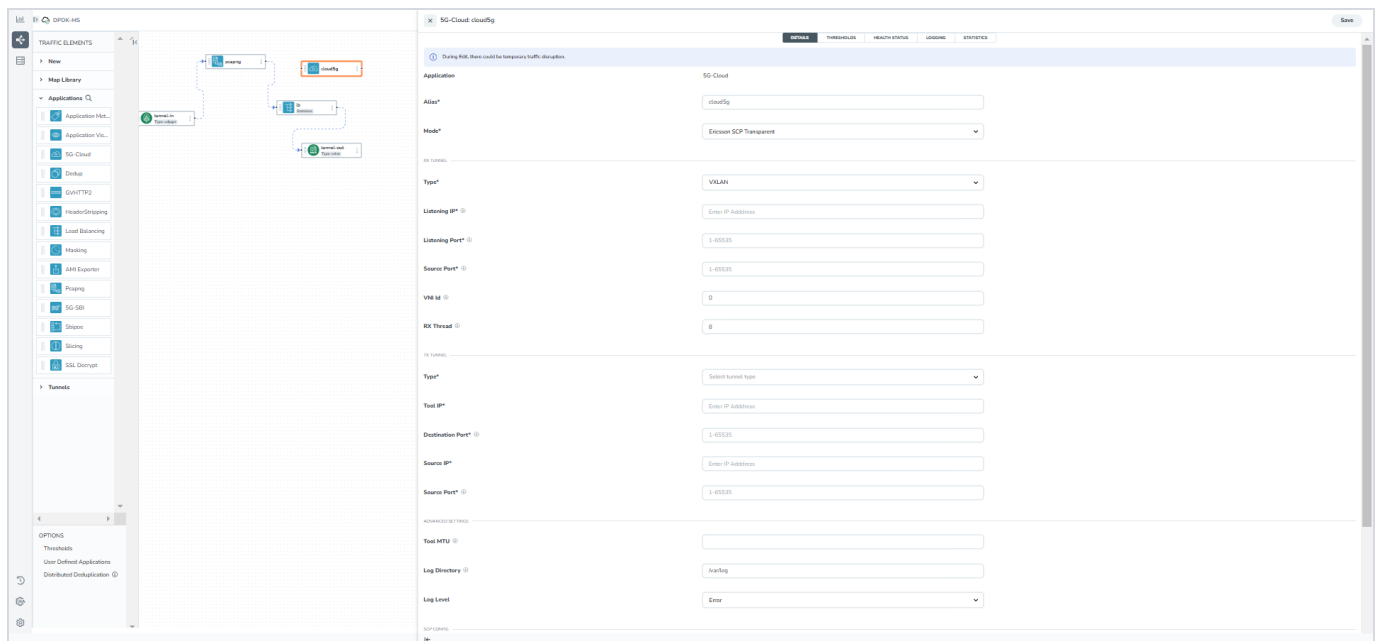
- You must upload CSV files containing a valid FQDN, NF Instance, and User Agent IDs and a valid IPv4/IPv6 address. Refer to [Add CSV file for IP Mapping](#).

You can add a 5G-Cloud application to:

- New Monitoring Session - Add the 5G-Cloud application after creating a new Monitoring Session and when the GigaVUE-FM canvas appears. Refer to Create a Monitoring Session section in the respective GigaVUE Cloud Suite Deployment Guide.
- Existing session - Select any existing Monitoring Session and go to **TRAFFIC PROCESSING** tab. The GigaVUE-FM canvas appears.

To add a 5G-Cloud application:

1. In the canvas, drag and drop the 5G-Cloud application and select **Details**. The 5G-Cloud quick view appears.



2. On the application quick view, enter or select the required information as described in the [5G Cloud Ericsson SCP - Field References](#).

NOTE: It is recommended to maintain a 60-90 second delay when undeploying and deploying a Monitoring Session in GigaVUE-FM.

Download Logs - 5G-Cloud application

You can view the log files of a V Series Node or download them as .CSV or .txt files.

To download the log files to a local environment:

1. Go to **Traffic > VIRTUAL** > select your cloud platform.
2. Select the required Monitoring Session and click **Details** on the 5G-Cloud application. Go to **LOGGING** in the quick view. The **Logging** page displays the logs currently available.
3. Select the required Days, Timestamps, File Name, and Type (TextLog and FlowStats) details.
4. Select the log files to download, and then click **Download > Files**. The system downloads the selected files to your local environment.

Add CSV file for IP Mapping

To add the CSV file for IP mapping:

1. Go to **Inventory > VIRTUAL >** select your cloud platform, and then click **Settings > 5G-Apps**. The 5G-Apps Configuration page appears.
2. Click **New**. Enter the name for the CSV file in the **Alias** field
3. From the Type drop-down list, select one of the following:
 - o **5G-Cloud FQDN** - Add the CSV file containing a valid FQDN ID and a valid IPv4/IPv6 address for IP mapping.
 - o **5G-Cloud NF Instance** - Add the CSV file containing a valid NF instance ID and a valid IPv4/IPv6 address for IP mapping.
 - o **5G-Cloud UA** - Add the CSV file containing a valid user agent ID and a valid IPv4/IPv6 address for IP mapping.
4. Click **Choose File** in the **FileName** field to upload the CSV file to GigaVUE-FM.



Notes - Header details of the CSV file:

- **FQDN Mapping:** gigamon@vseries:/var/log/cloud5g_tabledir\$ cat FQDN.txt (The fields fqdnID and ingressIPaddress1 are mandatory. All other fields are optional)
 - o Header details: FQDNid,IngressIP1,IngressIP2,IngressPort,EgressIP,NFType,NFLocation
 - o Example: s25scp01.scp.5gc.mnc003.mcc525.3gppnetwork.org,170.00.13.187,,8080,,SCP,plolp
- **NF Instance Mapping:** gigamon@vseries:/var/log/cloud5g_tabledir\$ pwd NFID.txt (The fields NFID and ingressIP1 are mandatory. All other fields are optional)
 - o Header details: NFID,IngressIP1,IngressIP2,IngressPort,EgressIP,NFType,NFLocation
 - o Example: 8b94c7xx-d700-4xcd-90be-634x11a5xx0d,100.23.14.4,,8080,,AMF,plolp
- **User Agent Mapping:** gigamon@vseries:/var/log/cloud5g_tabledir\$ pwd UA.txt (The fields useragentID and ingressIPaddress are mandatory. All other fields are optional)
 - o Header details: UserAgent,IngressIP1,NFType,NFLocation
 - o Example: xx5gs20015gcay01,192.64.10.67,AMF,plolp

The fields fqdnID and ingressIPaddress1 are mandatory. All other fields are optional.

5. Click **Validate** to validate the CSV file.
6. Click **Save** to add the CSV file.

FHA Dashboards for 5G-Cloud Applications

After configuring the 5G-Cloud application, you can monitor the statistics for Ericsson SCP by the reports displayed in the Dashboard. To access the details, refer to [FHA Dashboards for 5G-Cloud Applications](#).

5G Cloud Ericsson SCP - Field References

Field	Description
Application	The name 5g-Cloud appears by default.
Alias	Enter the alias name as cloud5g .
Mode	From the drop-down list, select Ericsson SCP Transparent .
RX Tunnel	
Type	Specify the tunnel type. The default is VXLAN.
Listening IP	Specify the tunnel's local listen IP address to receive the packet.
Listening Port	Specify the tunnel's local listening port to bind to receive the packet. The application will listen to the traffic coming to the specified port. Enter a value between 1 and 65535.
Source Port	Specify the tunnel destination port from where the packets will be sent. Enter a value between 1 and 65535.
VNI Id	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215. The default value is zero.
RX Thread	Specify the RX value to receive the packet. Enter a value between 1 and 16. The default value is 8.
TX Tunnel	
Type	Specify the tunnel type. The available tunnel types are: • VXLAN • L2GRE
Tool IP	Specify the remote IP address to send the packet.
Destination Port	Specify the tunnel destination port to which the packet will be sent. Enter a value between 1 and 65535.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the tunnel source port to bind when sending the packet. Enter a value between 1 and 65535.
VNI Id (Applicable only when the selected tunnel type is VXLAN)	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215.
L2GRE Key (Applicable only when the selected tunnel type is L2GRE)	Specify the key for the L2GRE tunnel type. Enter a value between 0 and 4294967295.
Advanced Setting	
Tool MTU	Specify the tool port MTU.
Log Directory	Specify the path to store the log files.
Log Level	Select the severity log level of the events from the following options: • None • Fatal • Error • Notification

	• Information • Debug
SCP Config	
FQDN Mapping	Specify the alias name created for the uploaded FQDN table CSV file.
NF Instance Mapping	Specify the alias name created for the uploaded NFID table CSV file.
User Agent Mapping	Specify the alias name created for the uploaded User Agent table CSV file.
TCP Server Ports	Specify the TCP server port or port range to allow TCP communication endpoints.
SCP Advanced Config	
No. of TCP Flows	Specify the total number of concurrent TCP flows. Enter a value between 128 and 2048. The default value is 1024.
No. of Transaction Flows	Specify the total number of Transaction Stream Flows allocated for tracking active Transaction Streams. Enter a value between: • 128 and 26000 for V Series Node of extra large form factor (total memory $\geq$ 32GB). • 128 and 5500 for V Series Node of large form factor (total memory < 32GB). The default value is 2048.
TCP Flow Timeout	Specify the TCP flow timeout ranging between 0 to 7200. The default value is 900.
SCP Transaction Timeout	Specify the SCP transaction timeout value ranging between 1 and 300. The default value is 10. Note: The recommended timeout value is between 10 and 20 seconds. An increase in the transaction timeout value will impact the total number of transactions that can be processed in parallel.
Minimum TCP Client Port	Specify the minimum value to be used for TCP client port ranging between 1023 and 65535. The default value is 32768.
Maximum TCP Client Port	Specify the maximum value to be used for client port ranging between 1023 and 65535. The default value is 36863.
SCP Processing Threads	Specify the number of worker threads for processing In-Out packets. Enter a value between 1 and 16. The default value is 8.
TCP Client Ports per Thread	Specify the number of TCP client ports for each worker thread. Enter a value between 100 and 8000. The default value is 1000.
Header Index	Enable or disable the header indexing. The default value is disabled.
Header Compression Code	Enable or disable the header compression code. The default value is disable.
Gigamon Header	Enable or disable the Gigamon Header. The default value is Enable.
Packet Capture Level	Select the packet capture level from the drop-down list: • All • Receive • Transmit • None

5G-Cloud Log Level	Select the required 5G-Cloud CSV log level from the drop down list. The default value is None. • All • Flow • Message • Transaction • None
HTTP2 Monitored Flows	
Number of Streams	Specify the number of monitored stream flows. Enter a value between 1024 and 16384. The default is 1024.
Request Timeout	Specify the HTTP/2 request timeout in seconds. Enter a value between 1 and 300. The default is 15 seconds.
Response Timeout	Specify the HTTP/2 response timeout in seconds. Enter a value between 1 and 300. The default is 2 seconds.
TCP Monitored Flows	
Number of Flows	Specify the number of monitored TCP flows. Enter a value between: • 1024 and 32768 for V Series Node of extra large form factor (total memory > 32GB). • 1024 and 2048 for V Series Node of lesser form factor. The default value is 2048.
Flow Timeout	Specify the timeout for TCP flows in seconds. Enter a value between 1 and 7200. The default value is 60 seconds.
Flow Reassembly Timeout	Specify the timeout for TCP flow reassembly in seconds. Enter a value between 1 and 7200. The default value is 500 seconds.

5G Cloud Nokia HEP3 Support

Nokia HEP3 (Homer Encapsulation Protocol Version 3) method is supported by Nokia for network functions across 3G, 4G, 5G and the IMS core. HEP3 efficiently organizes and encodes data for various network protocols and enhances the functionality of Nokia's core network solutions by accommodating diverse packet requirements.

The 5G-Cloud application supports processing the Nokia HEP3 format from the **IMS** network functions and 3G, 4G network functions. Non-SBI traffic is received as a TCP stream with HEP3 encoding by the 5G Cloud application. The 5G-Cloud application receives encapsulated traffic from the IMS vTAP in HEP3 over TCP, using either clear text or mTLS. Non-SBI control traffic is decoded from HEP3, emphasizing data handling without IP translation.

Nokia Cloud Mobility Manager (**CMM**), including AMF and MME, generates SBI and Non-SBI traffic over HTTP2 using clear text / TLS. The gvHTTP2 application receives this traffic and forwards it to the 5G-Cloud application. The 5G-Cloud synthesizes SBI payloads into L2GRE/VXLAN packets, enabling seamless monitoring across 5G core interfaces.

In **Nokia SCP** mode, the traffic is mirrored between the 5G control functions using HTTP2 protocol, which is mirrored from a service called SCP (Service Communication Proxy). The 5G-Cloud application receives the JSON encoded data from the VXLAN ingress TEPs. Refer to [Nokia SCP](#).

The system supports the following Nokia source functions and traffic types:

- 5G Cloud Nokia HEP3 IMS Integration (Non-SBI)
- 5G Cloud Nokia HEP3 CMM Integration (SBI and Non-SBI)

Supportability Table

The supportability table provides a quick reference to the supported Nokia functions:

Source Functions	Traffic Type	Protocols	Reference
3G, 4G, IMS	Non-SBI	HEP3 over TCP with Clear Text / mTLS	5G Cloud Nokia HEP3 IMS Support
CMM (AMF, MME)	SBI and Non-SBI	HEP3 over HTTP2 over TCP with Clear Text / TLS (via gvHTTP2)	5G Cloud Nokia HEP3 CMM Support

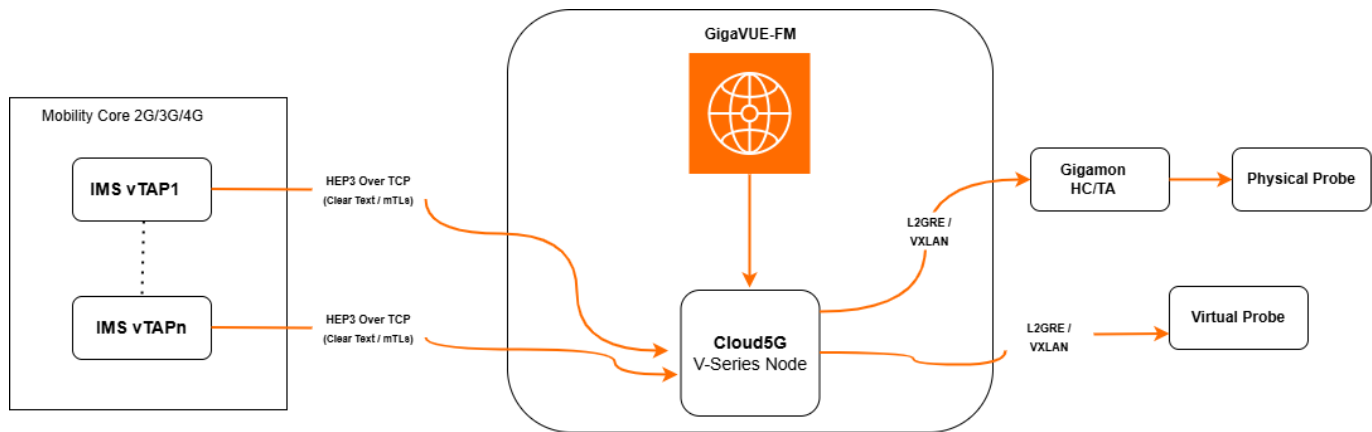
5G Cloud Nokia IMS Solution (Non-SBI)

Nokia HEP3 (Homer Encapsulation Protocol Version 3) is a binary encapsulation format that Nokia uses for control-plane traffic in the IMS core and across 3G and 4G network functions. HEP3 efficiently encodes protocol metadata and payloads so that Nokia core network solutions can handle diverse packet types.

In this solution, the 5G-Cloud application processes non-SBI IMS control traffic that Nokia vTAPs export as HEP3 over TCP, in clear text or protected with mTLS. 5G-Cloud also supports non-SBI HEP3 traffic from 3G and 4G network functions. It terminates the TCP session, decodes the HEP3 payloads, and exposes the non-SBI control traffic for monitoring without performing IP address translation.

How Nokia HEP3 IMS Solution works

The following image shows the ingress and egress data flow through the V Series Node for Nokia HEP3 IMS solution.



Traffic from client vTAP systems (in clear text or secured with mTLS) travels over TCP to the V Series node. The 5G-Cloud application receives this TCP traffic, terminates the TCP connections, decodes the HEP3 payloads, and synthesizes the data for monitoring.

GigaVUE-FM serves as the centralized management platform that orchestrates the visibility fabric, including the 5G-Cloud V Series nodes. The V Series nodes inspect, aggregate, and process the incoming traffic. After processing, the nodes encapsulate the traffic using L2GRE or VXLAN tunneling protocols and forward it to probes as follows:

Physical probe- If IP connectivity is not available, the node sends traffic to a GigaVUE HC or GigaVUE TA Series device, which aggregates and distributes traffic to the probe after decapsulation.

Virtual probe- If IP connectivity is available, the node forwards the processed traffic directly to the virtual probe for detailed inspection and analytics.

This end-to-end solution provides comprehensive visibility into 5G IMS control-plane traffic and supports efficient monitoring and performance analysis across both physical and cloud-based infrastructures.

Configure Nokia IMS HEP3 Solution (Non-SBI)

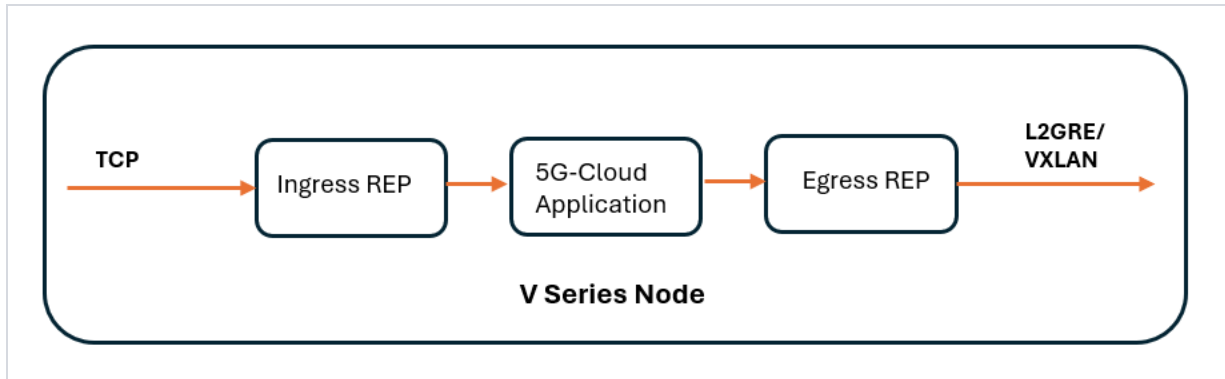
In GigaVUE-FM, you must do the following to add the 5G-Cloud IMS integration to either a new or existing monitoring session of a Monitoring Domain:

Pre-requisite:

Before starting, ensure that:

- You have deployed the V Series nodes and added them to a monitoring domain in GigaVUE-FM.

- IMS vTAPs can reach the V Series node over TCP on the HEP3 collector IP address and port.
- You must upload CSV files containing a valid FQDN and a valid IPv4/IPv6 address. Refer to [Add CSV file for IP Mapping](#).



1. Create New or Use Existing Monitoring Session

In GigaVUE-FM, go to the monitoring domain that will carry IMS HEP3 traffic. You can add the 5G-Cloud application, to a new or existing monitoring session of a Monitoring Domain.

- **New Monitoring Session** - Add the 5G-Cloud application after creating a new Monitoring Session and when the GigaVUE-FM canvas appears. Refer to [Create a Monitoring Session](#) section in the respective GigaVUE Cloud Suite Deployment Guide.
- **Existing Monitoring Session** - Select any existing Monitoring Session and go to **TRAFFIC PROCESSING** tab. The GigaVUE-FM canvas appears.

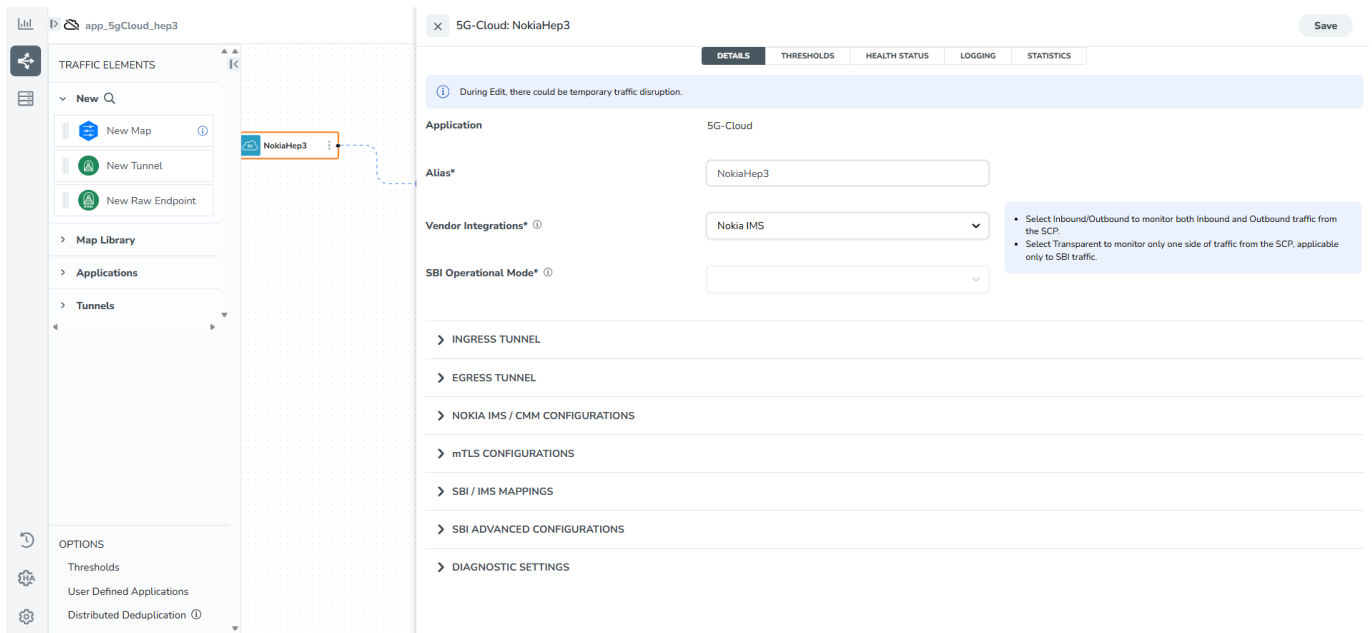
2. Create an ingress REP to receive the data over TCP

- On the canvas, create an ingress raw endpoint (REP) on the V Series node to receive HEP3/TCP from the IMS vTAPs.
- Configure the listening IP address and TCP port that the vTAPs use as the HEP3 collector.
- Refer to [Create Raw Endpoint \(VMware vCenter\)](#), [Create Raw Endpoint \(OpenStack\)](#), or [Create Raw Endpoint \(Third Party Orchestration\)](#) for platform-specific steps.

3. Configure Nokia HEP3 in 5G-Cloud Application

To add a 5G-Cloud application:

1. In the canvas, drag and drop the 5G-Cloud application and select **Details**. The 5G-Cloud quick view appears.



- On the application quick view, enter or select the required information as described in the [Reference - Configuration Table](#).

NOTE: It is recommended to maintain a 60-90 second delay when undeploying and deploying a Monitoring Session in GigaVUE-FM.

Reference - Configuration Table

Field	Description
Application	The name 5g-Cloud appears by default.
Alias	Enter the required alias name. (for example: NokiaHep3)
Vendor Integrations	From the drop-down list, select Nokia IMS .
SBI Operational Mode	The Operational Mode is grayed out when you select Nokia CMM or Nokia IMS.
Ingress Tunnel	
Type	Specify the tunnel type. The default is TCP.
Listening IP	Specify the tunnel's local listen IP address to receive packets.
Listening Port	Specify the tunnel's local listening port to bind for receiving packets. The application listens to the traffic on the specified port. Enter a value between 1 and 65535.
Source Port	Specify the tunnel destination port to send packets. Enter a value between 1 and 65535.
Egress Tunnel	
Type	Specify the tunnel type. Available tunnel types are: - VXLAN - L2GRE

Tool IP	Specify the remote IP address to which you want to send the packets.
Destination Port	Specify the tunnel destination port to send the packets. Enter a value between 1 and 65535.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the tunnel source port to bind when sending packets. Enter a value between 1 and 65535.
Tool MTU	Specify the tool port MTU: - For V Series Node version 6.8.00 and above, enter a value between 1400 and 8800. The default value is 8800. - For V Series Node version below 6.8.00, enter a value between 1500 and 8800. The default value is 8800.
VNI ID (Applicable only when the selected tunnel type is VXLAN)	Specify the ID for VXLAN traffic. Enter a value between 0 and 16777215.
L2GRE Key (Applicable only when the selected tunnel type is L2GRE)	Specify the key for the L2GRE tunnel type. Enter a value between 0 and 4294967295.
Nokia IMS / CMM Configuration	
Number of Ingress TCP Connections	Specify the number of concurrent TCP connections VTAP can establish. Enter a value between 128 and 2048. The default value is 1024.
Number of Egress TCP Flows	Specify the total number of TCP flows allocated for tracking non-SBI traffic. - For V Series Node (extra-large form factor, total memory ≥ 32 GB): 1024 – 16000000 - For V Series Node (large form factor, total memory < 32 GB): 1024 – 16384. - Default value: 4096.
Egress TCP Flow Timeout	Specify the timeout value for an Egress TCP flow in seconds. Enter a value between 30 and 7200 seconds. The default is 900 seconds. NOTE: If no packets are received within the configured time, the TCP flow will terminate due to a timeout.
Number of Receiver Threads	Specify the number of receiver threads for processing incoming packets. Enter a value between 1 and 128. The default value is 8.
Number of Egress SCTP Flows	Specify the total number of SCTP flows allocated to track non-SBI traffic. Enter a value between 128 and 20000000. The default value is 1024.
Egress SCTP Flow Timeout	Specifies the timeout value for an Egress SCTP flow in seconds. Enter a value between 30 and 7200. The default value is 900 seconds. NOTE: If no packets are received within the configured time, the SCTP flow will terminate due to a due to timeout.
mTLS Configuration	
mTLS	Use the toggle button to enable or disable mTLS encryption and

	decryption in Monitor Mode.
mTLS key	- If mTLS encryption is enabled, select the mTLS key alias for the SSL certificate from the drop-down list. - To create a key alias, click Add next to the text box. For further details, refer to Configure SSL Decrypt.
SBI / IMS Mappings Refer to Add CSV file for IP Mapping section for more details.	
FQDN Mapping	Use this option to provide mappings between Fully Qualified Domain Names and IP addresses for all Network Functions in the network. Select an alias: Choose the alias name associated with the uploaded FQDN table (CSV file) from the drop-down list. Add a new alias: If no alias exists, click Add to create one.
Network Function Instance Mapping (Optional)	Use this option to provide mappings between NF Instance IDs and IP addresses for all Network Functions in the network. Select an alias: Choose the alias name associated with the uploaded NFID table (CSV file) from the drop-down list. Add a new alias: If no alias exists, click Add to create one.
User Agent Mapping (Optional)	Use this option to provide mappings between User Agents and IP addresses for all Network Functions in the network. Select an alias: Choose the alias name associated with the uploaded User Agent table (CSV file) from the drop-down list. Add a new alias: If no alias exists, click Add to create one.
Service Mapping (Optional)	Use this option to map ephemeral attribute values to standard service attributes and define service-specific actions. Select an alias: Choose the alias name associated with the uploaded Service Mapping table (CSV file) from the drop-down list. Add a new alias: If no alias exists, click Add to create one. None: Select None to clear any previously selected Service Map entry. Refer to Reference - Service Map Field Definitions section for example details.
SBI Advanced Configuration	
NOTE: The below configurations apply only to SBI traffic and will not be used for non-SBI traffic.	
TCP Server Ports	Specify the TCP server port or port range to enable TCP communication between endpoints. - Valid port range: 1-65535. - Maximum number of ports: 1024. NOTE: TCP communication is allowed only on the configured ports.
Number of TCP Flows	Specify the total number of TCP Flows allocated for tracking active TCP Flows. - Valid range: 128-2048 - Default value: 1024
Number of Transaction Flows	Specify the total number of Transaction Stream flows allocated for

	tracking active Transaction. Refer to Recommend Form Factor for VMware vCenter (Instance Types) for more details. Streams: • Large Form Factor VMs (total memory < 32GB): 128-5500. • Extra Large Form Factor VMs (total memory ≥ 32GB): 128-26000 • Default value: 2048
TCP Flow Timeout	Specify the TCP flow timeout value. • Valid range: 0-7200 • Default value: 900
SCP Transaction Timeout	Specify the Transaction timeout value. • Valid range: 1-300 • Default value: 10
Minimum TCP Client Port	Specify the starting port number for Synthesize Flow. • Valid range: 1023-65535 • Default value: 32768
Maximum TCP Client Port	Specify the end port number for the Synthesize Flow. • Valid range: 1023-65535 • Default value: 36863
SCP Processing Threads	Specify the number of worker threads for processing In-Out packets. • Valid range: 1-16 • Default value: 8
TCP Client Ports per Thread	Specify the number of TCP client ports for each worker thread. • Valid range: 100-8000 • Default value: 1000
Header Index	Enable or disable the header indexing. The default option is disabled.
Header Compression Code	Enable or disable the header compression code. The default option is disable.
Gigamon Header	Enable or disable the Gigamon Header. The default option is Enable.
Diagnostic Settings	
Log Directory	Specify the path to store the log files.
Application Log Level	Select the severity log level of the events from the following options: • None • Fatal • Error • Notification • Information • Debug

Packet Capture Level	Select the packet capture level from the drop-down list: • All • Receive • Transmit • None
Packet Capture Timestamp	Select the required timestamp used to save the Egress PCAPs. The available timestamps are: • Observed Timestamp • System Timestamp NOTE: Timestamp option is disabled if the Packet capture level is set to None.
Message Trace Log Level	Select the 5G-Cloud CSV log level from the drop-down list. • All • Flow • Message • Transaction • None (Default Value)

4. Create links between the ingress REP, 5G-Cloud, and egress REP

- On the canvas, draw a link from the ingress raw endpoint to the 5G-Cloud application.
- Create an egress raw endpoint (REP) for the target probe or GigaVUE HC/TA device (using the same raw endpoint procedures as in Step 2).
- Draw a link from the 5G-Cloud application to the egress raw endpoint.

5. Deploy the Monitoring Session

- After adding all the required elements to the canvas, to deploy the session do the following:
- From the **Actions** menu, select **Deploy**.

After successful deployment on all the V Series Nodes, the status appears as **Success** on the **Monitoring Sessions** page.

6. View the Deployment Report

- You can view the Monitoring Session Deployment Report in the **SOURCES** and **V SERIES NODES** tab.
- When you select the **Status** link, the Deployment Report is displayed.
- When the deployment is incorrect, the Status column displays one of the following errors:
 - a. **Success:** Not deployed on one or more instances due to V Series Node failure.
 - b. **Failure:** Not deployed on all V Series Nodes or Instances.

7. Download Logs - 5G-Cloud application

You can view the log files of a V Series Node or download them as .CSV or .txt files.

To download the log files to a local environment:

- Go to **Traffic > VIRTUAL** > select your cloud platform.
- Select the required Monitoring Session and go to **TRAFFIC PROCESSING** tab. On the **cloud5g** application, click the  menu button and select **Details**. Go to **LOGGING** in the quick view. The **Logging** page displays the logs currently available.
- Select the required Days, Timestamps, File Name, and Type (TextLog and FlowStats) details.
- Select the log files to download, and then click **Download > Files**. The system downloads the selected files to your local environment.

Add CSV file for IP Mapping

To add the CSV file for IP mapping:

1. Go to **Inventory > VIRTUAL** > select your cloud platform, and then click **Settings > 5G-Apps**. The 5G-Apps Configuration page appears.
2. Click **New**. Enter the name for the CSV file in the **Alias** field.
3. From the **Type** drop-down list, select one of the following. You can also choose to download the template using the **Download Template** option and add the required entries.
 - o **5G-Cloud FQDN** - Add the CSV file containing a valid FQDN ID and a valid IPv4/IPv6 address for IP mapping.

Header Details	Example
FQDNID	abc.xyz.com
IngressIP1	1.1.1.1
IngressIP2	2.2.2.2
IngressPort	100
EgressIP	3.3.3.3
NFType	SMF
NFLocation	US
IMSIP	1001:0008:85a2:0000:0000:8f1e:0340:7110
IMSIntfName	100 200
IMSMask	96
IMSType	nep

**Notes:**

- The fields fqdnID and ingressIPAddress1 are mandatory. All other fields are optional.
- The fields imsipaddress, imsinterfacename, imsmask and imstype are applicable only when the Integrated solution Vendor is "Nokia HEP3".

- **5G-Cloud NF Instance** - Add the CSV file containing a valid NF instance ID and a valid IPv4/IPv6 address for IP mapping.

Header Details	Example
NFID	amf.local
ingressIPAddress1	1.1.1.1
ingressIPAddress2	2.2.2.2
IngressPort	100
egressIPAddress	3.3.3.3
NFType	AMF
NFLocation	US

NOTE: The fields NFID and ingressIP1 are mandatory. All other fields are optional.

- **5G-Cloud UA** - Add the CSV file containing a valid user agent ID and a valid IPv4/IPv6 address for IP mapping.

Header Details	Example
useragentid	nef.nb.5gc.mc005.mcc580.yournetwork
ingressIPAddress	1.1.1.1
NFType	AMF
NFLocation	US

NOTE: The fields useragentID and ingressIPAddress are mandatory. All other fields are optional.

- **5G-Cloud Service Map** - Add the CSV file containing valid ephemeral port details and a valid IPv4/IPv6 address for IP mapping. Refer to [Reference - Service Map Field Definitions](#) for header details and examples.
4. Click **Choose File** in the **File Name** field to upload the CSV file into GigaVUE-FM.
 5. Click **Validate** to validate the CSV file.
 6. Click **Save** to add the CSV file.

NOTE:

- When a new mapping table is uploaded, the system validates the relevant fields for duplicate entries.
- If duplicate values are detected, a validation error is displayed.
- For the following tables: **5G-Cloud FQDN**, **5G-Cloud NF Instance** and **5G-Cloud UA**, the mapping file can still be saved with duplicate entries after all other validation errors are resolved by selecting **Save Anyway**.

Recommended VM Specifications

The configuration of the 5G-Cloud Nokia HEP3 application should be performed on extra-large and large VMs.

- Configuration specifications for Extra Large VM:
 - vCPUs: 26
 - Memory: 32 GB
 - Disk Space: 80 GB

NOTE: Nokia HEP3 configuration on extra-large VMs is supported only through the Third-Party Orchestration method.

- Configuration specifications for Large VM:
 - vCPUs: 8
 - Memory: 16 GB
 - Disk Space: 80 GB
- Supported Ports: 1 Management interface, 1 ingress, and 1 egress interfaces.

- It is recommended to use SRIOV enabled drivers for better performance and higher throughput. Refer to [Configure GigaVUE Fabric Components using VMware ESXi](#) topic for more details.

Reference - Service Map Field Definitions

Service mapping normalizes SIP traffic by converting vendor-specific or ephemeral ports to standard SIP service ports (such as 5060). GigaVUE-FM matches incoming SIP control messages against configurable rules and, when a rule applies, rewrites the source and/or destination port before forwarding the traffic. This ensures that monitoring tools that rely on standard SIP ports continue to work without any changes.

Refer below for field specific details:

NOTE: All fields except sipMessageType, srcPortMap, and dstPortMap are mandatory.

1. **srcIP** - Source IP address of the SIP traffic, as carried in HEP3. You can specify a single IPv4 / IPv6 address, a prefix, or ipany to match any address.

Example:

- ipany – matches SIP traffic from any source IP.
- 1.1.1.1 – matches only traffic coming from 1.1.1.1.

2. **dstIP** - Destination IP address of the SIP traffic. You can specify a single IPv4 / IPv6 address, a prefix, or ipany to match any address.

Example:

- ipany – any destination IP.
- 2.2.2.2 – match traffic going to 2.2.2.2.

3. **srcPort** - Source port number of the SIP traffic. You can use a specific port to target a known source, or portany to match all source ports.

Example:

- portany – match SIP traffic regardless of the source port.
- 5060 – match only when the source port is 5060.

4. **dstPort** - Destination port number of the SIP traffic.

Example:

- portany – any destination port.
- 5060 – only traffic with destination port 5060.

5. **protocolFamily** - Identifies the IP family of the traffic.

Example:

- IPv4 SIP traffic.
- IPv6 SIP traffic.

6. **transportProtocol** - Identifies the L4 transport protocol (TCP or UDP).

NOTE: This field accepts only tcp or udp; it does not support integer values.

7. **applicationProtocol** - Encodes the application protocol type carried in the HEP3 encapsulation.

Example:

- 1 – match SIP messages.

8. **interfaceName** - Identifies the Nokia interface number on which the traffic is received.

Example:

- 90 – match traffic received on Nokia HEP3 vTAP interface 90 (IMS Non-SBI).

9. **Direction** - Traffic direction from the node's point of view.

Example:

- ingress – apply this rule only to traffic arriving at the node.
- egress – apply this rule only to traffic sent out from the node.

10. **sipMessageType** - Tells whether the SIP message is a request or a response.

Example:

- request – map ports only for SIP requests.
- response – map ports only for SIP responses.

11. **action** - Specifies what the 5G Cloud application does with matching traffic.

Example:

- portmap – change source and/or destination ports as specified in srcPortMap / dstPortMap.
- discard – drop matching traffic.
- ignore – match but do not modify the ports.

12. **srcPortMap** - Applies only to server response frames. Use a valid port number in response frames (sipMessageType = response) and set it to portany for request frames.

Example:

- 5060 – set the source port to 5060 for matching SIP responses.
- portany – keep the original source port.

13. **dstPortMap** - Applies onto client-to-server request frames. Use a valid port number in request frames (sipMessageType = request) and set it to portany for response frames.

Example:

- 7777 – set the destination port to 7777 for matching SIP requests.
- portany – keep the original destination port.

FHA Dashboards for 5G-Cloud Applications

After configuring the 5G-Cloud application, you can monitor the statistics for Nokia HEP3 by the reports displayed in the Dashboard. To access the details, refer to [FHA Dashboards for 5G-Cloud Applications](#).

5G Cloud Nokia HEP3 CMM Solution (SBI and Non-SBI)

Nokia 5G network functions use the HEP3 binary format to encode and send packets. HEP3 supports both HTTP2 and TCP protocols, enabling efficient traffic transmission across core network functions. This solution supports traffic processing from Nokia Cloud Mobility Manager (CMM), and the Service Communication Proxy (SCP).

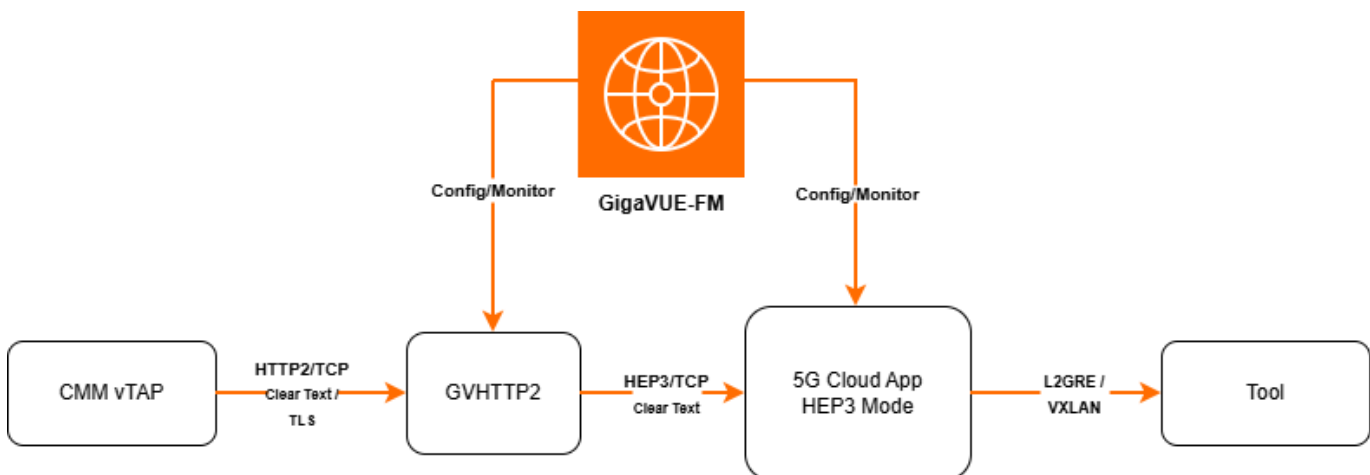
Cloud Mobility Manager (CMM) includes AMF and MME network functions. It generates both Service-Based Interface (SBI) and non-SBI traffic and sends it over HTTP2. The gvHTTP2 application receives CMM traffic and forwards it to the 5G Cloud application, which synthesizes SBI and non-SBI payloads into L2GRE/VXLAN packets before sending them to probes. This approach provides extended visibility across 5G core interfaces and enables operators to monitor both SBI and non-SBI traffic seamlessly.

How Nokia HEP3 CMM Solution works

Nokia vTAP systems in the mobility core send HEP3 data over both HTTP2 and TCP.

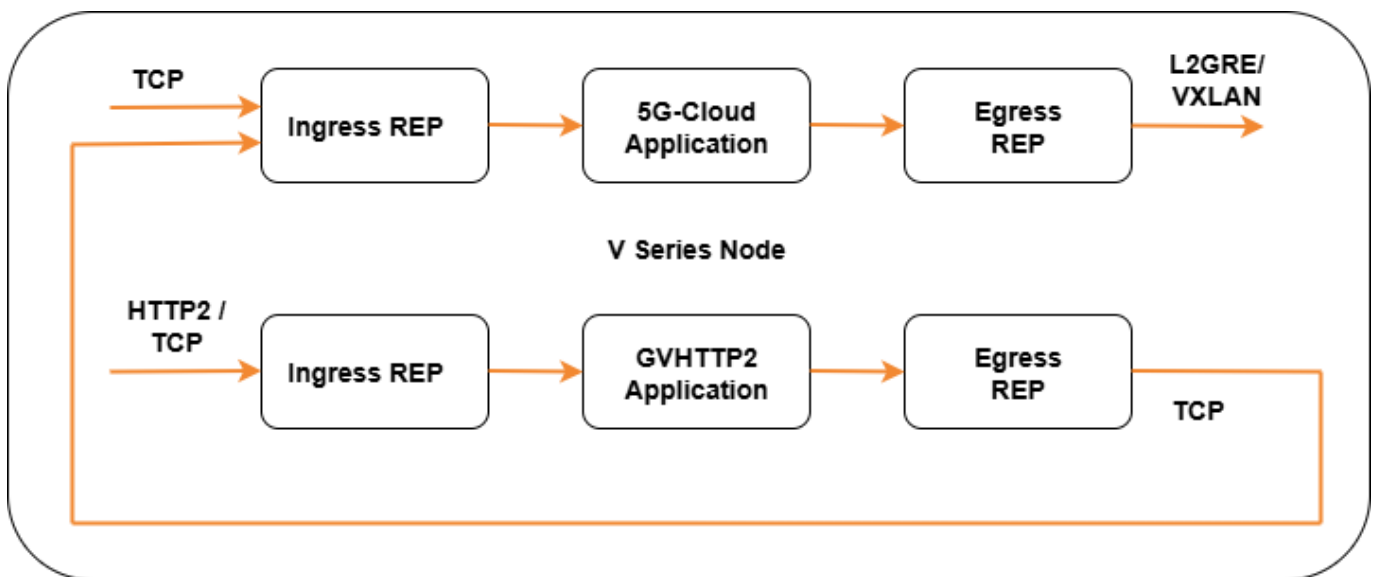
Nokia CMM Solution

The following image shows the ingress and egress data flow through the V Series node for the Nokia HEP3 CMM solution.



The Cloud Mobility Manager (CMM) function includes key control-plane elements such as AMF and MME. CMM generates both SBI and non-SBI traffic, making it central to mobility management in the 5G Core.

- CMM vTAPs export SBI and non-SBI control-plane traffic as HEP3 over HTTP2/TCP, in either clear text or TLS-protected sessions.
- The gvHTTP2 application on the V Series node listens on the configured HTTP2 IP address and port, terminates HTTP2 sessions from CMM, and extracts the encapsulated HEP3 payloads.
- gvHTTP2 sends the processed HEP3 payloads to the 5G-Cloud application over TCP by using a dedicated Nokia HEP3 over TCP tunnel between the gvHTTP2 and 5G-Cloud V Series nodes.
- 5G-Cloud receives HEP3/TCP from gvHTTP2, terminates the TCP connections, decodes the HEP3 payloads, and synthesizes SBI and non-SBI flows into a format that monitoring tools can consume without IP address translation.
- The V Series node encapsulates the synthesized traffic using L2GRE or VXLAN and then forwards it to:
 - Physical probe, through a GigaVUE HC or GigaVUE TA Series device that aggregates and decapsulates the traffic, or
 - Virtual probe, directly over IP when connectivity is available.



Configure Nokia CMM HEP3 Solution (SBI and Non-SBI)

In GigaVUE-FM, you must do the following to add the 5G-Cloud CMM integration to either a new or existing monitoring session of a Monitoring Domain:

Pre-requisite:

- You must upload CSV files containing a valid FQDN and a valid IPv4/IPv6 address. Refer to [Add CSV file for IP Mapping](#).

1. **Create New or Use Existing Monitoring Session**

In GigaVUE-FM, go to the monitoring domain that will carry IMS HEP3 traffic. You can add the 5G-Cloud application, to a new or existing monitoring session of a Monitoring Domain.

- **New Monitoring Session** - Add the 5G-Cloud application after creating a new Monitoring Session and when the GigaVUE-FM canvas appears. Refer to Create a Monitoring Session section in the respective GigaVUE Cloud Suite Deployment Guide.
- **Existing Monitoring Session** - Select any existing Monitoring Session and go to **TRAFFIC PROCESSING** tab. The GigaVUE-FM canvas appears.

2. Add gvHTTP2 and connect it to CMM vTAPs.

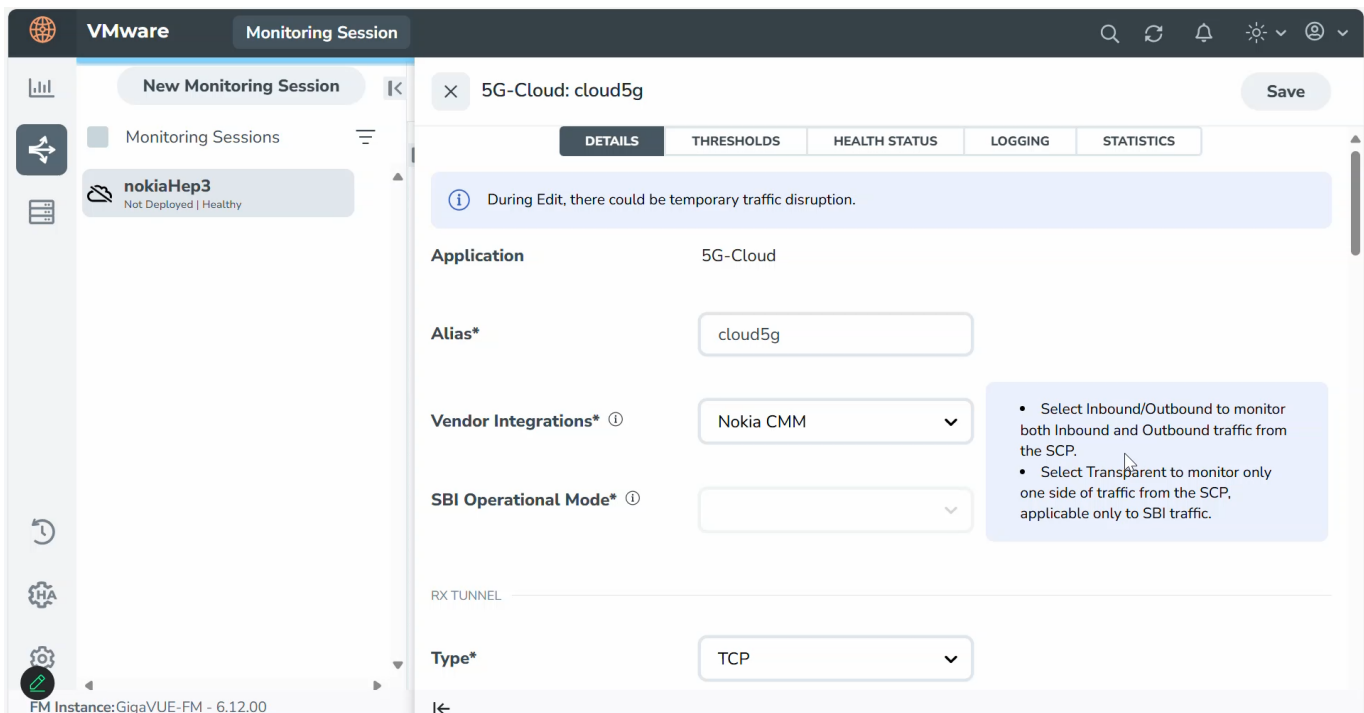
- On the canvas, drag and drop the gvHTTP2 application onto the V Series node.
- Select the gvHTTP2 node and click Details to open the quick view.
- Configuration of GvHTTP2 Application for CMM vTAP

Field	Description
Application	The name gvhttp2 appears by default.
Alias	Enter the alias name as gvhttp2 .
Vendor Integrations	From the drop-down list, select Nokia CMM .
HTTP2 Listening IP	Specify the HTTP2 IP address. The application will listen to the traffic on the specified IP address.
HTTP2 Listening Port	Specify the HTTP2 Port. The application will listen to the traffic on the specified port.
Max Stream	Specify the maximum number of concurrent streams in one HTTP2 session. Enter a value between 1 and 100. The default value is 100.
Worker Thread	Specify the number of parallel threads that can be sued to process the requests. Enter a value between 1 and 16. The default value is 1.
TX Tunnel	
Type	Specify the tunnel type as Nokia HEP3 over TCP from the dropdown for Nokia CMM.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the tunnel source port to bind when sending the packet. Enter a value between 1 and 65535.
Destination IP	Specify the tunnel destination port to which the packet will be sent. Enter a value between 1 and 65535.
Destination Port	Specify the tunnel destination port to which the packet will be sent. Enter a value between 1 and 65535.
Number of Egress TCP Connections	Specify the number of concurrent TCP connections GvHTTP2 can establish. Enter the value from 1 to 200. The default value is 4.
TLS Config	
TLS	Enable or disable TLS encryption or decryption using the toggle button.
Server Private key	Enter the path where the private key is stored.
Server Certificate	Enter the path where the certificate is stored.
Advanced Setting	
CSV	Enable this option to capture all stats counters for GvHTTP2.

PCAP	Enable this option to capture the packets at egress.
Log Directory	Specify the path to store the log files.
Log Level	Select the severity log level of the events from the following options: • None • Fatal • Error • Notification • Information • Debug

3. Add the 5G-Cloud application and connect it to gvHTTP2

- On the canvas, drag and drop the 5G-Cloud application onto the V Series node.
- Place 5G-Cloud downstream of gvHTTP2.
- Draw a link from gvHTTP2 to 5G-Cloud so that gvHTTP2 forwards HEP3/TCP to 5G-Cloud.
- Select the 5G-Cloud node and click Details to open the quick view.



NOTE: It is recommended to maintain a 60-90 second delay when undeploying and deploying a Monitoring Session in GigaVUE-FM.

4. Configuration of 5G-Cloud Application for CMM vTAP

Field	Description
Application	The name 5g-Cloud appears by default.
Alias	Enter the required alias name. (for example: NokiaHep3)
Vendor Integrations	From the drop-down list, select Nokia CMM .
SBI Operational Mode	The Operational Mode is grayed out when you select Nokia CMM or Nokia IMS.
Ingress Tunnel	
Type	Specify the tunnel type. The default is TCP.
Listening IP	Specify the tunnel's local listen IP address to receive packets.
Listening Port	Specify the tunnel's local listening port to bind for receiving packets. The application listens to the traffic on the specified port. Enter a value between 1 and 65535.
Source Port	Specify the tunnel destination port to send packets. Enter a value between 1 and 65535.
Egress Tunnel	
Type	Specify the tunnel type. Available tunnel types are: • VXLAN • L2GRE
Tool IP	Specify the remote IP address to which you want to send the packets.
Destination Port	Specify the tunnel destination port to send the packets. Enter a value between 1 and 65535.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the tunnel source port to bind when sending packets. Enter a value between 1 and 65535.
Tool MTU	Specify the tool port MTU: • For V Series Node version 6.8.00 and above, enter a value between 1400 and 8800. The default value is 8800. • For V Series Node version below 6.8.00, enter a value between 1500 and 8800. The default value is 8800.
VNI ID (Applicable only when the selected tunnel type is VXLAN)	Specify the ID for VXLAN traffic. Enter a value between 0 and 16777215.
L2GRE Key (Applicable only when the selected tunnel type is L2GRE)	Specify the key for the L2GRE tunnel type. Enter a value between 0 and 4294967295.
Nokia IMS / CMM Configuration	
Number of Ingress TCP Connections	Specify the number of concurrent TCP connections VTAP can establish. Enter a value between 128 and 2048. The default value is 1024.
Number of Egress TCP Flows	Specify the total number of TCP flows allocated for tracking non-SBI traffic. • For V Series Node (extra-large form factor, total memory ≥ 32 GB):

	1024 – 16000000 - For V Series Node (large form factor, total memory < 32 GB): 1024 – 16384. - Default value: 4096.
Egress TCP Flow Timeout	Specify the timeout value for an Egress TCP flow in seconds. Enter a value between 30 and 7200 seconds. The default is 900 seconds. NOTE: If no packets are received within the configured time, the TCP flow will terminate due to a timeout.
Number of Receiver Threads	Specify the number of receiver threads for processing incoming packets. Enter a value between 1 and 128. The default value is 8.
Number of Egress SCTP Flows	Specify the total number of SCTP flows allocated to track non-SBI traffic. Enter a value between 128 and 2000000. The default value is 1024.
Egress SCTP Flow Timeout	Specifies the timeout value for an Egress SCTP flow in seconds. Enter a value between 30 and 7200. The default value is 900 seconds. NOTE: If no packets are received within the configured time, the SCTP flow will terminate due to a due to timeout.
mTLS Configuration	
mTLS	Use the toggle button to enable or disable mTLS encryption and decryption in Monitor Mode.
mTLS key	- If mTLS encryption is enabled, select the mTLS key alias for the SSL certificate from the drop-down list. - To create a key alias, click Add next to the text box. For further details, refer to Configure SSL Decrypt.
SBI / IMS Mappings	
Refer to Add CSV file for IP Mapping section for more details.	
FQDN Mapping	Use this option to provide mappings between Fully Qualified Domain Names and IP addresses for all Network Functions in the network. Select an alias: Choose the alias name associated with the uploaded FQDN table (CSV file) from the drop-down list. Add a new alias: If no alias exists, click Add to create one.
Network Function Instance Mapping (Optional)	Use this option to provide mappings between NF Instance IDs and IP addresses for all Network Functions in the network. Select an alias: Choose the alias name associated with the uploaded NFID table (CSV file) from the drop-down list. Add a new alias: If no alias exists, click Add to create one.
User Agent Mapping (Optional)	Use this option to provide mappings between User Agents and IP addresses for all Network Functions in the network. Select an alias: Choose the alias name associated with the uploaded User Agent table (CSV file) from the drop-down list. Add a new alias: If no alias exists, click Add to create one.
Service Mapping (Optional)	Use this option to map ephemeral attribute values to standard service attributes and define service-specific actions.

	• Select an alias: Choose the alias name associated with the uploaded Service Mapping table (CSV file) from the drop-down list. • Add a new alias: If no alias exists, click Add to create one. • None: Select None to clear any previously selected Service Map entry.
SBI Advanced Configuration	
NOTE: The below configurations apply only to SBI traffic and will not be used for non-SBI traffic.	
TCP Server Ports	Specify the TCP server port or port range to enable TCP communication between endpoints. • Valid port range: 1-65535. • Maximum number of ports: 1024. NOTE: TCP communication is allowed only on the configured ports.
Number of TCP Flows	Specify the total number of TCP Flows allocated for tracking active TCP Flows. • Valid range: 128-2048 • Default value: 1024
Number of Transaction Flows	Specify the total number of Transaction Stream flows allocated for tracking active Transaction. Refer to Recommend Form Factor for VMware vCenter (Instance Types) for more details. Streams: • Large Form Factor VMs (total memory < 32GB): 128-5500. • Extra Large Form Factor VMs (total memory ≥ 32GB): 128-26000 • Default value: 2048
TCP Flow Timeout	Specify the TCP flow timeout value. • Valid range: 0-7200 • Default value: 900
SCP Transaction Timeout	Specify the Transaction timeout value. • Valid range: 1-300 • Default value: 10
Minimum TCP Client Port	Specify the starting port number for Synthesize Flow. • Valid range: 1023-65535 • Default value: 32768
Maximum TCP Client Port	Specify the end port number for the Synthesize Flow. • Valid range: 1023-65535 • Default value: 36863
SCP Processing Threads	Specify the number of worker threads for processing In-Out packets. • Valid range: 1-16 • Default value: 8
TCP Client Ports per Thread	Specify the number of TCP client ports for each worker thread. • Valid range: 100-8000 • Default value: 1000

Header Index	Enable or disable the header indexing. The default option is disabled.
Header Compression Code	Enable or disable the header compression code. The default option is disable.
Gigamon Header	Enable or disable the Gigamon Header. The default option is Enable.
Diagnostic Settings	
Log Directory	Specify the path to store the log files.
Application Log Level	Select the severity log level of the events from the following options: • None • Fatal • Error • Notification • Information • Debug
Packet Capture Level	Select the packet capture level from the drop-down list: • All • Receive • Transmit • None
Packet Capture Timestamp	Select the required timestamp used to save the Egress PCAPs. The available timestamps are: • Observed Timestamp • System Timestamp NOTE: Timestamp option is disabled if the Packet capture level is set to None.
Message Trace Log Level	Select the 5G-Cloud CSV log level from the drop-down list. • All • Flow • Message • Transaction • None (Default Value)

5. Create the egress raw endpoint and tool link

- On the canvas, create an egress raw endpoint (REP) on the V Series node that connects to your probe or GigaVUE HC/TA device.
- Draw a link from the 5G-Cloud application to the egress REP so that 5G-Cloud forwards encapsulated L2GRE/VXLAN traffic to the tool.

6. Deploy the monitoring session

- On the Monitoring Sessions page, select the session.
- From the Actions menu, select Deploy.
- Wait for deployment to complete on all V Series nodes.
- Confirm that the session Status shows Success.
- If the status shows Failure or partial success, open the SOURCES and V SERIES NODES tabs and click the Status link to view the deployment report.

Download Logs - 5G-Cloud / GvHTTP2 Application

You can view the log files of a V Series Node or download them as .CSV or .txt files.

To download the log files to a local environment:

1. Go to **Traffic > VIRTUAL** > select your cloud platform.
2. Select the required Monitoring Session and go to **TRAFFIC PROCESSING** tab. On the **cloud5g / gvhttp2** application, click the  menu button and select **Details**. Go to **LOGGING** in the quick view. The **Logging** page displays the logs currently available.
3. Select the required Days, Timestamps, File Name, and Type (TextLog and FlowStats) details.
4. Select the log files to download, and then click **Download > Files**. The system downloads the selected files to your local environment.

Add CSV file for IP Mapping

To add the CSV file for IP mapping:

1. Go to **Inventory > VIRTUAL** > select your cloud platform, and then click **Settings > 5G-Apps**. The 5G-Apps Configuration page appears.
2. Click **New**. Enter the name for the CSV file in the **Alias** field
3. From the Type drop-down list, select **5G-Cloud FQDN**. You can also choose to download the template using the **Download Template** option and add the required entries.
4. Click **Choose File** in the **FileName** field to upload the CSV file into GigaVUE-FM. Add the CSV file containing a valid FQDN ID and a valid IPv4/IPv6 address for IP mapping.



Notes - Header details of the CSV file:

FQDN Mapping: gigamon@vseries:/var/log/cloud5g_tabledir\$ cat FQDN.txt



- Header details:
FQDNid,IngressIP1,IngressIP2,IngressPort,EgressIP,NFType,NFLocation,IMSIP,IMSIntfName,IMSMask,IMSType
- Example:
s25scp01.scp.5gc.mnc003.mcc525.3gppnetwork.org,170.00.13.187,,8080,,SCP,plolp,2000:4000:124:a0d9:ac1:4::,92,303 314 315,sbc

The fields fqdnID and ingressIPAddress1 are mandatory. All other fields are optional.

The fields imsipaddress, imsinterfacename, imsmask and imstype are applicable only when the Integrated solution Vendor is "Nokia HEP3".

5. Click **Validate** to validate the CSV file.
6. Click **Save** to add the CSV file.

Recommended VM Specifications (5G-Cloud)

The configuration of the 5G-Cloud Nokia HEP3 application should be performed on extra-large and large VMs.

- Configuration specifications for Extra Large VM:
 - vCPUs: 26
 - Memory: 32 GB
 - Disk Space: 80 GB

NOTE: Nokia HEP3 configuration on extra-large VMs is supported only through the Third-Party Orchestration method.

- Configuration specifications for Large VM:
 - vCPUs: 8
 - Memory: 16 GB
 - Disk Space: 80 GB
- Supported Ports: 1 Management interface, 1 ingress, and 1 egress interfaces.
- It is recommended to use SRIOV enabled drivers for better performance and higher throughput. Refer to [Configure GigaVUE Fabric Components using VMware ESXi](#) topic for more details.

Recommended VM Specifications (GvHTTP2)

The configuration of the gvpttp2 application should be performed on large VMs.

- Configuration specifications for Large VMs:
 - vCPUs: 20
 - Memory: 16 GB
 - Disk Space: 80 GB

- Supported Ports: 1 Management interface, 1 ingress, and 1 egress interfaces.
- It is recommended to use SRIOV enabled drivers for better performance and higher throughput. Refer to [Configure GigaVUE Fabric Components using VMware ESXi](#) topic for more details.

Slicing

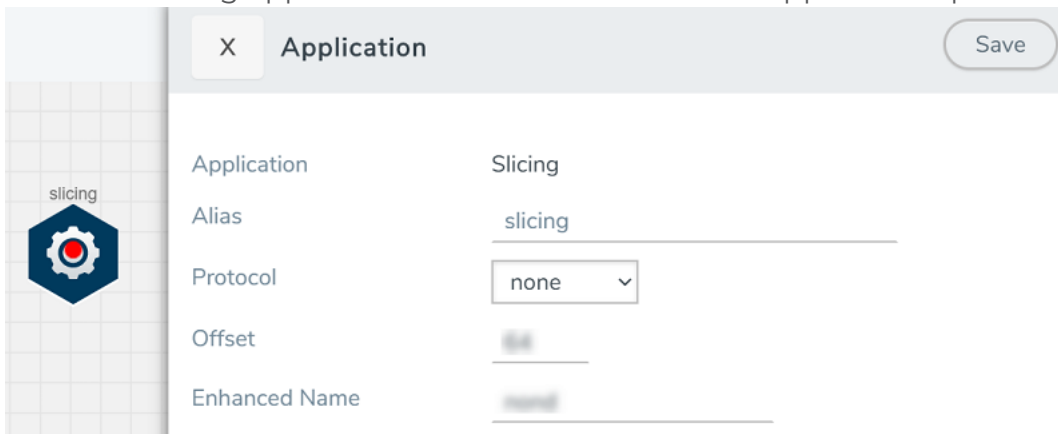
Packet Slicing allows you to truncate packets after a specified header and slice length, preserving the portion of the packet required for monitoring purposes. Slicing operations are typically configured to preserve specific packet header information, allowing effective network analysis without the overhead of storing full packet data.

Packets can have multiple variable-length headers, depending on where they are captured, the different devices that have attached their own headers along the way, and the protocols in use (for example, IPv4 versus IPv6). Because of this, slicing operations with a hard-coded offset will not typically provide consistent results.

To address this, the Slicing application lets you configure Packet Slicing using protocols that allow you to start slicing from a particular number of bytes after a specific packet header (IPv4, IPv6, UDP, and so on). The Slicing application parses through Layer 4 (TCP/UDP) to identify the headers in use, slicing based on the variable offset identified for a particular header instead of a hard-coded number of bytes.

To add a Slicing application:

1. Drag and drop **Slicing** from **APPLICATIONS** to the graphical workspace.
2. Click the Slicing application and select **Details**. The Application quick view appears.



Application	
Application	Slicing
Alias	slicing
Protocol	none
Offset	64
Enhanced Name	none

3. In the Application quick view, enter the information as follows:

Component	Description
Alias	Enter a name for the application.
Protocol	The following are the protocols that you can select for from the protocol drop-down list: - o None – Slice starting a specific number of bytes from the start of the packet. - o IPV4 – Slice starting a specified number of bytes after the IPv4 header. - o IPV6 – Slice starting a specified number of bytes after the IPv6 header. - o UDP – Slice starting a specified number of bytes after the UDP header. - o TCP – Slice starting a specified number of bytes after the TCP header. - o FTP – Identify using TCP port 20 and slice payloads using offset from the TCP header. - o HTTPS – Identify using TCP port 443. Slice encrypted payloads using offset from the TCP header. - o SSH – Identify using TCP port 22. Slice encrypted payloads using offset from the TCP header. The Slicing application can provide slicing for GTP tunnels, provided the user payloads are unencrypted. Both GTPv1 and GTPv2 are supported – GTP' (GTP prime) is not supported. Keep in mind that only GTP-u (user plane packets) are sliced. Control plane packets (GTP-c) are left unmodified because of their importance for analysis. - o GTP – Slice starting a specified number of bytes after the outer GTP header. - o GTP-IPV4 – Slice starting a specified number of bytes after the IPv4 header inside the encapsulating GTP packet. - o GTP-UDP – Slice starting a specified number of bytes after the UDP header inside the encapsulating GTP packet. - o GTP-TCP – Slice starting a specified number of bytes after the TCP header inside the encapsulating GTP packet.
Offset	Specify the length of the packet that must be sliced.

4. Click **Save**.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

Appendix - Casa vTap Statistics

This section provides the stats details for GVHTTP2 and 5G-Cloud applications. For more information on counter details, refer to the respective application on the [GigaVUE API Reference](#) page.

NOTE: Currently, the following stats are not supported in GigaVUE-FM. You should login to the corresponding V Series Node to execute the commands.

GVHTTP2 Application

The following table provides information on the counter details and their usage for the GVHTTP2 application:

S.No	Counter Name	Counter Description
1	http2TransactionsSuccessful	Total HTTP2 Transaction successes that occurred in the GVHTTP2 Server.
2	http2StreamInitializeCount	Total HTTP2 New Streams that have been observed by the GVHTTP2 Server.
3	http2StreamCloseCount	Total HTTP2 Streams that have been successfully completed by the GVHTTP2 Server.
4	http2StreamPrepareResponseCount	Total calls to ask GVHTTP2 to prepare a response for inbound stream transactions.
5	http2StreamOnHeaderCount	Total calls to GVHTTP2 when a header value for a given stream has been observed.
6	http2StreamOnDataChunkCount	Total calls to GVHTTP2 when a data chunk for a given stream has been observed.
7	http2StreamOnRecvFrameCount	Total calls to GVHTTP2 when Receive Frame has occurred for any HTTP2 frame.
8	http2StreamOnRecvFrameEndStreamCount	Total calls to GVHTTP2 when the last HTTP2 Frame has been received indicating that the end of the stream has occurred.
9	http2GETRequests	Total HTTP2 GET Requests received by the GVHTTP2 Server.
10	http2POSTRequests	Total HTTP2 POST Requests received by the GVHTTP2 Server.
11	http2PUTRequests	Total HTTP2 PUT Requests received by the GVHTTP2 Server.

S.No	Counter Name	Counter Description
12	http2OtherRequests	Total HTTP2 Requests not GET, POST, or PUT received by the GVHTTP2 Server.
13	http2ValidURI	Total HTTP2 Requests that have valid PATH for the current GVHTTP2 Mode.
14	http2NewSessions	Total TCP Sessions newly initiated by Client applications connecting to the GVHTTP2 Server.
15	http2TerminateSessions	Total TCP Sessions that have been terminated by the Client applications connecting to the GVHTTP2 Server.
16	http2OpenSessions	Total TCP Open / Accept Sessions received by Client Applications connecting to the GVHTTP2 Server.
17	http2CloseSessions	Total TCP Sessions that have closed either by Client Applications or GVHTTP2 Server.
18	vxlantxPackets	Total number of packets that have been successfully transmitted to the VXLAN TX Tunnel.
19	vxlantxBytes	Total number of bytes that have been successfully transmitted to the VXLAN TX Tunnel.
20	vxlantxThreadCount	Total number of thread cycles that occurred during the interval.
21	http2TransactionsFailed	Total HTTP2 Transaction failures that occurred in the GVHTTP2 Server.
22	http2StreamTimeouts	Total times when the start of a new HTTP2 Stream has occurred but is not completed within the predefined timeout.
23	http2StreamHeaderOverflows	Total events where header has been received, but there is no space in the GVHTTP2 server code to accept the Header Value.
24	http2StreamBufferOverflows	Total events where data frames have been received, but there is no space in the GVHTTP2 server code to accept the data frame.
25	http2InvalidURI	Total HTTP2 Requests that have invalid PATH for the current GVHTTP2 Mode.
26	http2SSLConnectionFailures	Total SSL Connection Failures that occur when the GVHTTP2 Server receives a TCP Connection but fails SSL negotiation.
27	http2SocketFailures	Total Socket Failures either in mTLS or Clear Text mode.
28	vxlantxSocketSendErrors	Total number of packets that could not be transmitted to the VXLAN TX Tunnel because of socket error.
29	vxlantxSocketSizeErrors	Total number of packets that could not be transmitted to the VXLAN TX Tunnel because the

S.No	Counter Name	Counter Description
		size of the packet is too large.
30	vxlanThreadTimeouts	Total number of calls to select that timed out waiting for received data. This is not an error.
31	vxlanRXPackets	Total number of RX Packets received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that have been created in the VXLAN thread.
32	vxlanRXBytes	Total number of RX Bytes received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that have been created in the VXLAN thread.
33	vxlanRXDrops	Total number of RX Packets received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that have been dropped by the VXLAN thread because there are no more RX descriptors in the ingress queue of the VXLAN thread.
34	vxlanRXOversized	Total number of RX Packets received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that the VXLAN thread has dropped because the RX message size is too large.
35	vxlanQueueCurrBufferIn	Buffer index of the queue slot for a current packet to be inserted into the VXLAN Thread RX Queue.
36	vxlanQueueCurrBufferOut	Buffer index of the queue slot for a current packet to be removed from the VXLAN Thread RX Queue.
37	vxlanQueueNumBuffers	Total number of buffers in the VXLAN RX Queue.
38	vxlanQueueMaxQueueSize	Total number of packets that were in the VXLAN RX Queue during the current interval.
39	vxlanQueueBufferSize	Size of each RX Packet buffer in the VXLAN RX Queue.
40	vxlanQueuePacketsQueuedIn	Total number of packets that have been put into the VXLAN RX Queue.
41	vxlanQueuePacketsQueuedOut	Total number of packets that have been removed from the VXLAN RX Queue.
42	vxlanQueuePacketsQueuedFull	Total number of packets that attempted to be queued when the VXLAN RX Queue was full.
43	nghttp2Errors	Total errors that occur within the nghttp2 library used by the GVHTTP2 server application.
44	pcapRXPackets	Total number of RX Packets received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that have been created in the PCAP thread.

S.No	Counter Name	Counter Description
45	pcapRXBytes	Total number of RX Bytes received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that have been created in the PCAP thread.
46	pcapRXDrops	Total number of RX Packets received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that have been dropped by the PCAP thread because there are no more RX descriptors in the ingress queue of the PCAP thread.
47	pcapRXOverSized	Total number of RX Packets received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that the PCAP thread has dropped because the RX message size is too large.
48	pcapRXErrors	Total number of RX Packets received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that the PCAP thread has dropped because of an error.
49	pcapQueueCurrBufferIn	Buffer index of the queue slot for a current packet to be inserted into the PCAP Thread RX Queue.
50	pcapQueueCurrBufferOut	Buffer index of the queue slot for a current packet to be removed from the PCAP Thread RX Queue.
51	pcapQueueNumBuffers	Total number of buffers in the PCAP RX Queue.
52	pcapQueueMaxQueueSize	Total number of packets that were in the PCAP RX Queue during the current interval.
53	pcapQueueBufferSize	Size of each RX Packet buffer in the PCAP RX Queue.
54	pcapQueuePacketsQueuedIn	Total number of packets that have been put into the PCAP RX Queue.
55	pcapQueuePacketsQueuedOut	Total number of packets that have been removed from the PCAP RX Queue.
56	pcapQueuePacketsQueuedFull	Total number of packets that attempted to be queued when the PCAP RX Queue was full.
57	pcapFiles	Total number of PCAP Files written during this interval.
58	pcapOpenErrors	Total number of file errors that occurred while trying to create new PCAP Files during this interval.
59	pcapWriteErrors	Total number of file errors that occurred while trying to write data to PCAP Files during this interval.
60	pcapFlushErrors	Total number of file errors that occurred while trying to flush cached data to PCAP Files during

S.No	Counter Name	Counter Description
		this interval.
61	pcapCloseErrors	Total number of file errors that occurred while trying to close PCAP Files during this interval.
62	pcapPackets	Total number of PCAP Packets written during the interval.
63	pcapBytes	Total number of PCAP Bytes written during the interval.
64	diskLoggingThreadTimeouts	Total number of calls to delay waiting to receive data in the PCAP file thread. This is not an error.
65	diskLoggingThreadCount	Total number of thread cycles that occurred during the interval.

5G-Cloud Application

The following table provides information on the counter details and their usage for the 5G-Cloud application:

S.No	Counter Name	Counter Description
1	rxPkts	Total number of RX Packets / Messages from the GVHTTP2 Application.
2	txPkts	Total number of packets that have been successfully transmitted to the UDPGRE TX Tunnel.
3	rxPktBytes	Total number of RX Bytes for messages from the GVHTTP2 Application.
4	txPktBytes	Total number of bytes that have been successfully transmitted to the UDPGRE TX Tunnel.
5	rxDrops	Total number of RX Packets received from inbound VXLAN Tunnel by the 5G-Cloud Application from the GVHTTP2 Server APP that have been dropped by the PCAP thread because there are no more RX descriptors in the ingress queue of the PCAP thread.
6	txDrops	Total number of Tx Packets that have been dropped by the 5G-Cloud APP because there are no more RX descriptors in the egress queue.
7	rxThreadCount	Total number of receive thread cycles that occurred during the interval.
8	txThreadCount	Total number of Transmit thread cycles that

S.No	Counter Name	Counter Description
		occurred during the interval.
9	rxSelectTimeouts	Total number of calls to select that timed out waiting for received data. This is not an error.
10	txThreadTimeout	Total number of calls to egress Queue (Timed Semaphore wait) that timed out waiting for received data. This is not an error.
11	rxIPv4Pkts	Total number of IPv4 Packets received by the 5G-Cloud Application (this counter is not used currently).
12	rxIPv6Pkts	Total number of IPv6 Packets received by the 5G-Cloud Application (this counter is not used currently).
13	rxTcpPkts	Total number of TCP Packets received by the 5G-Cloud Application (this counter is not used currently).
14	rxNonTcpPkts	Total number of Non-TCP Packets received by the 5G-Cloud Application (this counter is not used currently).
15	rxVlanPkts	Total number of VLAN Packets received by the 5G-Cloud Application (this counter is not used currently).
16	rxPktsTooShort	Total Number of Incomplete Packets received by the 5G-Cloud Application (this counter is not used currently).
17	rxSelectNoEvents	Total Number of Errors while reading the packet data from the ingress Socket.
18	rxOversizedBuffers	Total number of RX Packets received by the 5G-Cloud Application from the GVHTTP2 Server that have been dropped because the RX message size is too large.
19	rxRecvFromNonCritical	Total number of socket timeout (timed out without Receiving any packet) for the ingress Interface.
20	rxErrors	Total number of Rx Packets dropped by the 5G-Cloud Application because of an error in Processing the Packet.
21	rxProtocolIDErrors	Total number of Rx Packets dropped by the 5G-Cloud Application because of error in IP Protocol ID (this counter is used only when L2GRE is used as ingress Tunnel Type hence it is not used currently).
22	rxIPProtocolErrors	Total number of Rx Packets dropped by the 5G-Cloud Application because of an error in IP Protocol (this counter is used only when L2GRE is

S.No	Counter Name	Counter Description
		used as ingress Tunnel Type; hence, it is not used currently).
23	rxIPPayloadLengthErrors	Total number of Rx Packets dropped by the 5G-Cloud Application because of an error in IP payload length (this counter is not used currently).
24	txSocketErrors	Total number of packets that could not be transmitted to the UDPGRE TX Tunnel because of socket error.
25	elPkts	Total number of Packets successfully written into the log files.
26	elFiles	Total number of files opened successfully to log the packets.
27	elErrors	Total number of errors while opening the file to write the packets.

Appendix-5G Cloud Nokia HEP3 Support (SBI)

The following table provides information on the counter details and their usage for the 5G-Cloud application:

S.No	Counter Name	Counter Description
1	sslAccept	Total TCP Open / Accept Sessions received by Client Applications connecting to the Server.
2	sslAcceptSSLPending	Total number of times SSL Connection is temporary suspension of the handshake, awaiting further action from the application's client hello callback.
3	sslAcceptSSLWantedRead	Total number of times SSL Connection needs to read more data from the network to proceed, but no data is currently available for reading.
4	sslAcceptSSLWantWrite	Total number of times there was error in writing complete data to the socket.
5	sslAcceptSSLAcceptFailure	Total number of times a new SSL connection is not accepted because of certificate, protocol or other errors.
6	sslRecvSuccess	Total number of times a new SSL connection has been accepted successfully.
7	sslRecvBytes	Total number of RX Bytes received from the

S.No	Counter Name	Counter Description
		vTAP in SSL Mode.
8	sslRecvSSLPending	Total number of times SSL Connection establishment is which indicates that TLS handshake routine is interrupted by client hello callback.
9	sslRecvSSLWantRead	Total number of times read operation is retried when data is available for reading.
10	sslRecvSSLWantWrite	Total number of times write operation is retried when data is available for writing.
11	sslRecvSSLReadFailures	Total number of times TLS/SSL connection has been closed cleanly by the peer while handshake is in progress.
12	sslBadCert	Total number of times there is error in establishing SSL connection with client because certificates are rejected by the peer.
13	sslCertVerifyFailure	Total number of times where client attempting to establish a secure connection (using SSL/TLS) with a server could not verify the server's SSL certificate.
14	sslUnknownProtocol	Total number of times there is error in establishing SSL connection with client because when the server cannot recognize or negotiate SSL/TLS protocol version.
15	sslHandshakeFailure	Total number of times there is error in establishing SSL connection with client because Handshake could not negotiate a cipher/protocol.
16	sslAlertUnknownCA	Total number of times there is error in establishing SSL connection with client because Certificate authority not recognized.
17	sslNoSharedCipher	Total number of times there is error in establishing SSL connection with client because no cipher overlap with peer.

GRE-In-UDP Tunnel Decapsulation

The GRE-In-UDP tunnel is a new tunnel type that supports decapsulating the GRE-in-UDP headers in the vTAP captured data packets. The decapsulation of the tunnel headers is common for both control and data packets. However, the control packets (with JSON

metadata format) are dropped based on the GRE Key value '0'. The data packets (either fragmented or unfragmented) are handled as follows:

S. No	Process	Description
1	Reassembly of fragmented data packets (if fragmented packets are received)	The fragmented packets are reassembled based on standard IP header-based reassembly using the following fields: • More Fragments (MF) field in IPv4 packets • Identification field in IPv6 packets
2	Decap tunnel lookup	The ingress packet fields are parsed to find a matching Tunnel End Point (TEP) based on the following header fields: • Destination IP • Source IP • UDP port numbers • GRE key
3	Decapsulation of headers	If a matching TEP is found, the encapsulation headers in the packet are removed and the packet is forwarded to the PCAPng application. Refer to the PCAPng Application section for more details.

Additional Sources of Information

This appendix provides additional sources of information. Refer to the following sections for details:

- [Documentation](#)
- [Documentation Feedback](#)
- [Contact Technical Support](#)
- [Contact Sales](#)
- [The VUE Community](#)

Documentation

©This table lists all the guides provided for GigaVUE Cloud Suite software and hardware. The first row provides an All-Documents Zip file that contains all the guides in the set for the release.

NOTE: In the online documentation, view [What's New](#) to access quick links to topics for each of the new features in this Release; view [Documentation Downloads](#) to download all PDFs.

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.14 Hardware and Software Guides	
DID YOU KNOW?	If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing Edit > Advanced Search from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware	how to unpack, assemble, rackmount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
GigaVUE-HC1 Hardware Installation Guide	
GigaVUE-HC3 Hardware Installation Guide	
GigaVUE-HC1-Plus Hardware Installation Guide	
GigaVUE-HCT Hardware Installation Guide	
GigaVUE-TA25 Hardware Installation Guide	
GigaVUE-TA25E Hardware Installation Guide	
GigaVUE-TA100 Hardware Installation Guide	

GigaVUE Cloud Suite 6.14 Hardware and Software Guides	
GigaVUE-TA200 Hardware Installation Guide	
GigaVUE-TA200E Hardware Installation Guide	
GigaVUE-TA400 Hardware Installation Guide	
GigaVUE-TA400E Hardware Installation Guide	
GigaVUE-OS Installation Guide for DELL S4112F-ON	
G-TAP A Series 2 Installation Guide	
GigaVUE M Series Hardware Installation Guide	
GigaVUE-FM Hardware Appliances Guide	
Software Installation and Upgrade Guides	
GigaVUE-FM Installation, Migration, and Upgrade Guide	
GigaVUE-OS Upgrade Guide	
GigaVUE V Series Migration Guide	
Fabric Management and Administration Guides	
GigaVUE Administration Guide	covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide	how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
GigaVUE Application Intelligence Solutions Guide	
GigaVUE Inline Solutions Guide(NEW) (previously included in the GigaVUE Fabric Management Guide)	
Cloud Guides	
how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms	
GigaVUE V Series Applications Guide	
GigaVUE Cloud Suite Deployment Guide - AWS	
GigaVUE Cloud Suite Deployment Guide - Azure	
GigaVUE Cloud Suite Deployment Guide - OpenStack	
GigaVUE Cloud Suite Deployment Guide - Nutanix	
GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)	
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)	

GigaVUE Cloud Suite 6.14 Hardware and Software Guides	
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration	
Universal Cloud TAP - Container Deployment Guide	
Gigamon Containerized Broker Deployment Guide	
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions	
GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions	
Reference Guides	
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices	
GigaVUE-OS Security Hardening Guide	
GigaVUE Firewall and Security Guide	
GigaVUE Licensing Guide	
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices	
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices	
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)	
Factory Reset Guidelines for GigaVUE-FM and GigaVUE-OS Devices Sanitization guidelines for GigaVUE Fabric Management Guide and GigaVUE-OS devices.	
Release Notes	
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release Note: Release Notes are not included in the online documentation. Note: Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software and Docs page on to My Gigamon . Refer to How to Download Software and Release Notes from My Gigamon .	
In-Product Help	
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.	

How to Download Software and Release Notes from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Release Notes** page on to [My Gigamon](#). Use the My Gigamon Software & Docs page to download:

- Gigamon Software installation and upgrade images,
- Release Notes for Gigamon Software, or
- Older versions of PDFs (pre-v5.7).

To download release-specific software, release notes, or older PDFs:

1. Log in to [My Gigamon](#).
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.6.xx.

NOTE: My Gigamon is available to registered customers only. Newer documentation PDFs, with the exception of release notes, are all available through the publicly available online documentation.

Documentation Feedback

We are continuously improving our documentation to make it more accessible while maintaining accuracy and ease of use. Your feedback helps us to improve. To provide feedback and report issues in our documentation, send an email to:

documentationfeedback@gigamon.com

Please provide the following information in the email to help us identify and resolve the issue. Copy and paste this form into your email, complete it as able, and send. We will respond as soon as possible.

Documentation Feedback Form		
About You	Your Name	
	Your Role	
	Your Company	

For Online Topics	Online doc link	<i>(URL for where the issue is)</i>
	Topic Heading	<i>(if it's a long topic, please provide the heading of the section where the issue is)</i>
For PDF Topics	Document Title	<i>(shown on the cover page or in page header)</i>
	Product Version	<i>(shown on the cover page)</i>
	Document Version	<i>(shown on the cover page)</i>
	Chapter Heading	<i>(shown in footer)</i>
	PDF page #	<i>(shown in footer)</i>
How can we improve?	Describe the issue	<i>Describe the error or issue in the documentation. (If it helps, attach an image to show the issue.)</i>
	How can we improve the content? Be as specific as possible.	
	Any other comments?	

Contact Technical Support

For information about Technical Support: Go to **Settings**  **> Support > Contact Support** in GigaVUE-FM.

You can also refer to <https://www.gigamon.com/support-and-services/contact-support> for Technical Support hours and contact information.

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to contact Gigamon channel partner or Gigamon sales representatives.

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

Email Gigamon at inside.sales@gigamon.com for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

The VÜE Community

The **VÜE Community** is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the VÜE Community site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

The VÜE Community is a great way to get answers fast, learn from experts and collaborate directly with other members around your areas of interest.

Register today at community.gigamon.com

Questions? Contact our Community team at community@gigamon.com.

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

follower in clustering node relationship (formerly slave or non-master)

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

root timing; transmits sync info to clocks in its network segment (formerly grandmaster)

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)