



GigaVUE Application Intelligence Solutions Guide

GigaVUE-FM, GigaVUE HC Series

Product Version: 6.12

Document Version: 1.0

(See Change Notes for document updates.)

Copyright 2025 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
6.12	1.0	10/27/2025	The original release of this document with 6.12.00 GA.

Contents

GigaVUE Application Intelligence Solutions Guide	1
Change Notes	3
Contents	4
Application Intelligence	6
Application Intelligence Capabilities	6
How Application Intelligence Works	8
Deep Packet Inspection (DPI) Engine	8
User Defined Application	9
Fast Mode	9
View Application Protobook	10
Application Intelligence Deployment Overview	10
Required Licenses and Supportability	13
Licensing	13
Supported Platforms	14
Application Intelligence—Rules and Notes	15
Application Intelligence Session	16
Create an Application Intelligence Session in Physical Environment	16
View the Details of an Application Intelligence Session	26
View the Application Intelligence Dashboard	30
Application Filtering Intelligence	34
Large Flows in Application Filtering Intelligence	34
Application Session Filtering (ASF) and Buffer ASF	35
Enhanced Application Session Filtering	42
ASF and Buffer ASF Examples	42
Display ASF Statistics	61
Create Application Filtering Intelligence for Physical Environment	62
Handle Large Flows in Application Filtering Intelligence	65
Configure Application Filtering Intelligence with Slicing and Masking	67
Application Metadata Intelligence	69
Application Metadata Intelligence Capabilities	69
Import and Export Tool Templates	73
Create Custom Tool Templates	73
Create Application Metadata Intelligence for Physical Environment	76
Enable De-duplication in Application Filtering Intelligence or Application Metadata Intelligence	84

Create NetFlow Session for Physical Environment	85
NetFlow Dashboard	93
GigaVUE Enriched Metadata for Mobile Networks	95
View the Health Status of a Solution	98
Upgrading the Protocol Signature	101
Application Intelligence Feature Compatibility	102
AdditionalInfoAppx	103
Additional Sources of Information	103
Glossary	109

Application Intelligence

Application Intelligence, a suite of GigaSMART applications, is designed to meet the needs of NetOps, , SecOps, and DevOps teams. By delivering comprehensive visibility into applications and networks, it helps reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). This ultimately enhances the security and management of hybrid cloud infrastructures.

GigaVUE-FMAApplication Intelligence streamlines network telemetry by:

- Identifying and filtering applications and protocols in North-South and lateral network traffic.
- Generating metadata from applications and protocols involves creating detailed information about the transmitted data, including generating NetFlow/IPFIX for effective monitoring of standard information elements.

Additionally, Gigamon's Deep Observability Pipeline can enhance Security Information and Event Management (SIEM) and Observability tool deployments by :

- Adding deeper context to logs by providing full-stack visibility (L2-L7) for troubleshooting performance and security issues. This solution remains transparent to users, preventing easy tampering or falsification by threat actors.
- Providing visibility into traffic spanning unmanaged devices

Please note that this guide specifically covers configuring **Application Intelligence** for **GigaVUE HC Series** devices.

To configure Application Intelligence for virtual devices, you will need to, refer to **Application Intelligence** section in the **GigaVUE V Series Applications Guide**.

Application Intelligence Capabilities

Application Intelligence provides the following capabilities for both physical devices and virtual nodes:

- **Application Visualization (earlier known as Application Monitoring)** - Identifies and monitors all applications contributing to the network traffic, and reports on all applications, and their application families and tags and the total bandwidth they consume over a select period. Able to identify over 4000 applications. It displays the traffic statistics in bytes, packet and flows.
- **Application Filtering Intelligence**- Enables traffic filtering by layer 7 applications, which means you can filter out high-volume, low-risk traffic from reaching the tools and direct high-risk network traffic of interest to the right tool at the right time. You can select applications based on the application name, family or tags.

- **Application Metadata Intelligence** - Supports exporting up to 6000 attributes of metadata that provide relevant usage context for over 4000 applications, thus enabling you to rapidly identify indicators of compromise (IoC) for security analytics and forensics tools.
- **Application Metadata Explorer**-Enables exporting application metadata to cloud-native tools. It converts CEF records from Application Metadata Intelligence (AMI) into JSON or Parquet format. JSON records can be exported over HTTP, HTTPS or Kafka. It can also enrich metadata from user-plane traffic with control-plane metadata for mobile networks or enrich application metadata with key host environment details for cloud workloads. Refer to [Application Metadata Exporter](#) to know more.

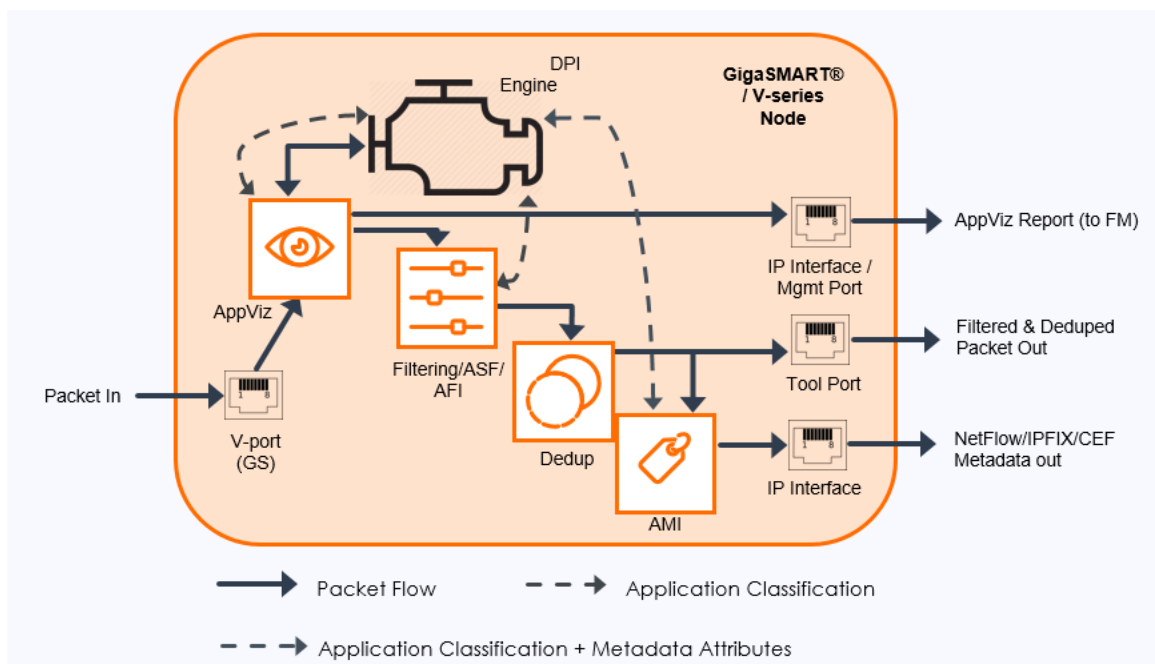
NOTE: Application Intelligence requires a separate GigaSMART engine or engines in group.

How Application Intelligence Works

Application Intelligence is an essential aspect of modern network management, enabling organizations to gain valuable insights into the behavior and performance of their applications. In the following sections, we will explore the key features and processes that make Application Intelligence an indispensable tool for managing today's complex network environments.

Deep Packet Inspection (DPI) Engine

Gigamon Application Intelligence uses the Deep Packet Inspection (DPI) engine to classify and filter applications and export application metadata. When packets arrive, the DPI engine analyzes the first few packets for each flow to classify the application. It then collects and exports the application statistics to GigaVUE-FM (destination port 2056) using the management interface by default.



Application Filtering Intelligence (AFI) relies on application classification to filter relevant applications. AFI can be combined with other GigaSMART Operations to further optimize the traffic before forwarding to the tools.

Configuring AFI is optional for AMI. In the GigaVUE HC Series, if customers only install the AMI license, AFI will automatically be configured to pass all traffic. When AFI and AMI are combined, all applications passed by AFI are sent to AMI for generating NetFlow (v5,

v9)/IPFIX records or application metadata in IPFIX and CEF formats. IPFIX is suitable for flow correlation tools such as NPM, APM and NDR, while CEF is suitable for log aggregation tools such as SIEM and Observability tool.

The types of traffic that DPI can identify are as follows:

- **Raw Network Traffic**- The DPI engine can identify thousands of commercially available applications. The various classification methods are provided under **top menu > Help > Classification Methods**. Refer to [View Application Protobook](#). However, there can be instances where an application could be identified as follows:
 - **Unknown**: Application is reported as unknown when some packets in the flow are missing or when the DPI Engine can identify a packet as valid but does not identify any protocols in the packet flow e.g. non-IP packets.
 - **Unknown-TCP/UDP/SSL**: Lack of packet heuristics may prevent the DPI Engine from identifying an application. In which case, it can tag the application based on its known lower layer, such as unknown-TCP, unknown-UDP, and unknown-SSL.
 - **Classification-unknown**: Application is reported as classification-unknown when the DPI Engine is unable to identify any valid packets in the packet flow.
- **Tunneled Traffic**-The DPI engine can identify applications in overlay networks like GRE, VXLAN, MPLS, and GTP. It can analyze up to 16 outer headers to identify protocols and export their metadata based on the innermost packet header.
- **Encrypted Traffic** - DPI uses various techniques to identify applications over TLS, DTLS and QUIC.

User Defined Application

To monitor proprietary or internal applications, the DPI engine supports user-defined application signatures that can be created to define rules for identifying the applications (up to 120). This feature allows you to identify unclassified TCP, UDP, HTTP, and HTTPS applications, and extract their application name and the lower layer protocol attributes.

Fast Mode


The DPI engine supports a performance optimization functionality called “fast mode”. In this mode the performance is increased by the use of light parsers for processing the HTTP and DNS traffic. This affects the classification of applications over HTTP. Only limited applications based on HTTP can be classified. This affects the attribute extraction. For example, only some attributes are extracted for the HTTP traffic and no attributes are extracted for the DNS traffic. When the fast mode is enabled, the GigaVUE-FM automatically displays only the attributes that are supported. This is supported only in GigaVUE HC Series.

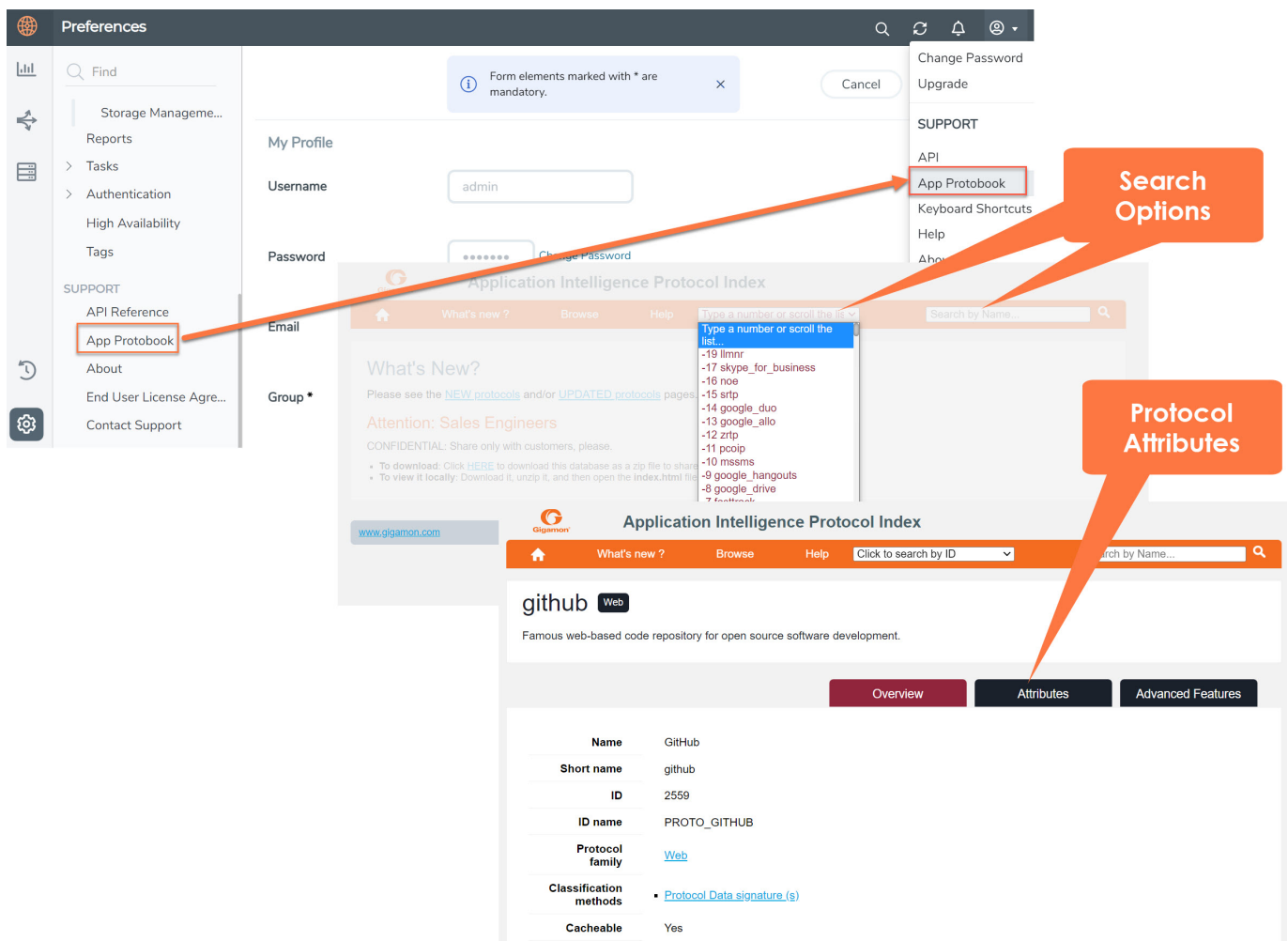
NOTE: In the protobook, you can check if a specific application supports the fast mode or not, by navigating to the **Attributes** tab of the specific application. If the **Basic DPI Support** field is yes, then the application supports the fast mode option.

View Application Protobook

Protobook provides a complete list of supported protocols and their attributes of metadata. These protocols can also be viewed as groups by Tags, Family and Classification method.

You can access the Application Protobook from the GigaVUE-FM in the following ways:

- On the left navigation pane, click  then click the "App Protobook" link under the **Support** section OR
- Go to **admin > App Protobook**



The screenshot displays the GigaVUE-FM interface. On the left, the 'Support' section is expanded, and 'App Protobook' is selected. The main area shows the 'Application Intelligence Protocol Index' page. A search bar is visible at the top right of the index page. Below the index, the details for the 'github' protocol are shown, including a table of attributes.

Name	Value
Name	GitHub
Short name	github
ID	2559
ID name	PROTO_GITHUB
Protocol family	Web
Classification methods	Protocol Data signature (s)
Cacheable	Yes

Application Intelligence Deployment Overview

This simplified deployment model illustrates the end-to-end traffic flow. The solution can be deployed via GigaVUE-FM or GigaVUE Cloud Suite for Third Party Orchestration and will be monitored through GigaVUE-FM.

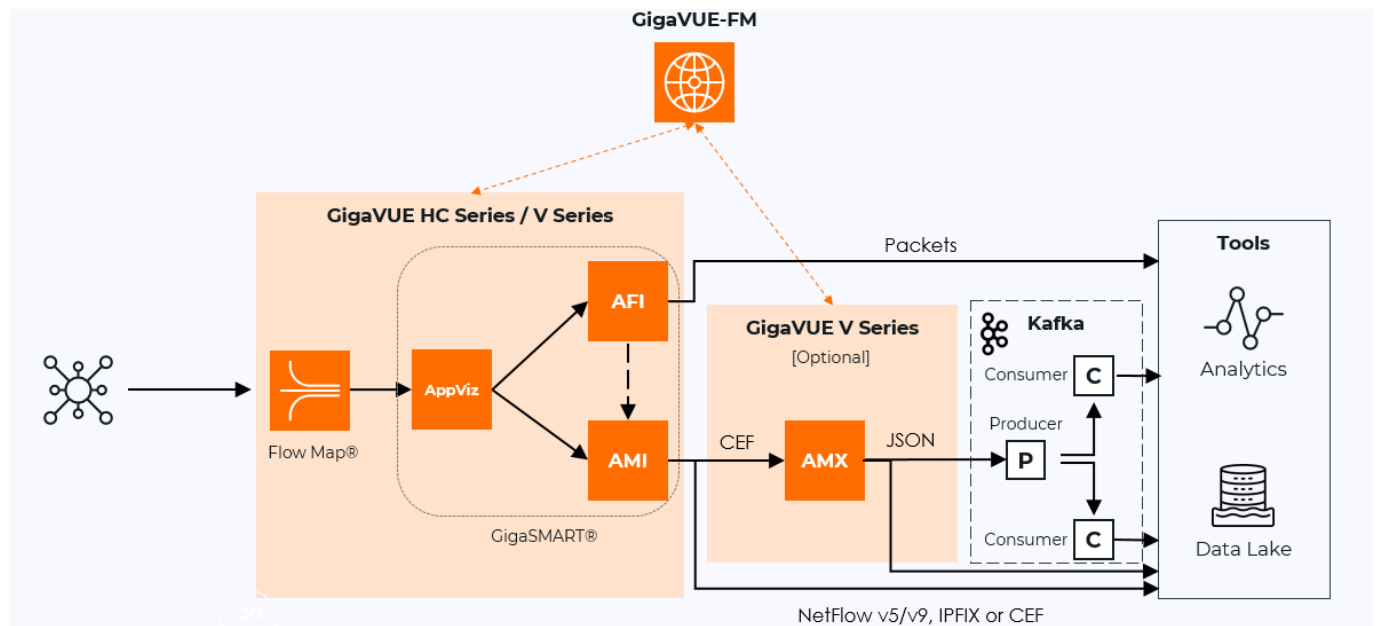


Figure 1 Application Intelligence Solution illustrates how the Application Intelligence solution works.

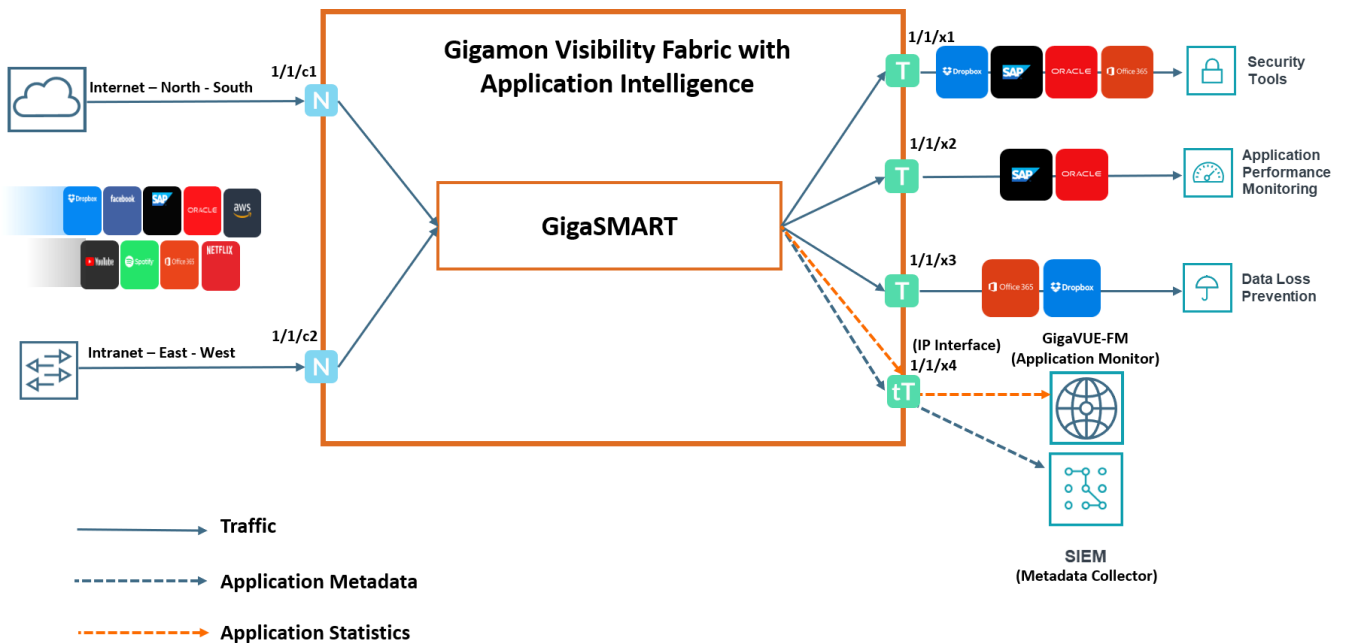


Figure 1 Application Intelligence Solution

The Gigamon device that is configured with the Application Intelligence capability receives the traffic through the network ports. Application Visualization (earlier it was known as Application Monitoring) exports applications related information to GigaVUE-FM from GigaVUE HC Series that renders the information on the Application Intelligence Dashboard.

Based on the pass or drop rules configured in the maps, Application Filtering Intelligence lets relevant applications be forwarded to the tools. In this example, you can see that except some of the audio or video streaming applications such as Spotify®, YouTube, and Netflix, other applications are sent to the security tool. This is because the audio or video streaming applications are high-volume, low-risk traffic. The threat detection tool need not inspect such traffic. Hence, these applications are dropped based on the configured drop rules

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.

Required Licenses and Supportability

This section outlines the necessary licenses, examines supportability, and assesses compatibility to ensure seamless operation and compliance with requirements.

Licensing

- Application Filtering Intelligence — Application Filtering Intelligence with Application Visualization capability.
- Application Metadata Intelligence — Application Metadata Intelligence with Application Visualization capability.
- NetFlow/IPFIX — NetFlow/IPFIX generation for IPv4 and IPv6. This allows to export only the standard elements and not application metadata.
- NetVUE
- NetVUE PLUS
- SecureVUE
- SecureVUE PLUS
- Zero Trust Architecture

NOTE: These licenses are valid for a year. After the expiration date, the system does not allow you to add new configuration or make any configuration updates but allows traffic flow for two weeks.

The following table provides details about the features available with the license:

License	Application Visualization	Application Filtering Intelligence	Application Metadata Intelligence	NetFlow/IPFIX
Application Filtering Intelligence	✓	Default Filtering Features available. ¹	✓	✓
Application Metadata Intelligence	✓	Default Filtering Features available. ²	✓	✓
NetFlow/IPFIX (NFI) (GigaVUE HC SeriesGen3)	✗	✗	✗	✓ NOTE: NetFlow/IPFIX supports exporting standard information elements in NetFlow v5/v9, IPFIX and CEF

License	Application Visualization	Application Filtering Intelligence	Application Metadata Intelligence	NetFlow/IPFIX
				formats.
NetVUE PLUS (GigaVUE HC Series Gen2)	✓	✓	✗	✗
SecureVUE PLUS (GigaVUE HC Series Gen2)	✓	✓	✓	✓
Zero Trust Architecture (GigaVUE HC Series Gen2) & (GigaVUE HC Series Gen3)	✓	✓	✓	✓

¹By default, pass-all map is created in Application Filtering Intelligence session with null port. You can also define the pass and/or drop application rules and advanced GigaSMART rules, if required.

² By default, pass-all map is created in Application Filtering Intelligence session with null port. You can also define the physical port, if required.

Supported Platforms

Application Intelligence is supported on the following platforms :

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

Refer to [Supported GigaSMART Operations](#) for more details on the devices that support GigaSMART operations.

Application Intelligence—Rules and Notes

Keep in mind the following rules and notes when working with the Application Intelligence solution:

- Only one Application Visualization, Application Filtering and/or Application Metadata solution can be deployed on a Gen 3 GigaSMART card or V Series node.
- Whenever you perform a backup and restore operation, you must create a backup of both the device and GigaVUE-FM, GigaVUE HC Series and then restore the backed-up data on both as well.
- Application Intelligence supports processing asymmetric (unidirectional) and symmetric (bidirectional) traffic. However, it's recommended to process symmetric traffic to get the best results.
- GigaVUE-FM can take up to 10 minutes for populating the Application Intelligence dashboards.
- When both the AMI and AFI licenses are installed on Gen 2 cards, the non-5-tuple packets will be dropped, and the packets will not pass to the AMI application for attribute extraction.
- Application Filtering Intelligence License is an optional choice for Application Metadata Intelligence, but AFI with "No-Rule-Match" pass will be enabled by default for AMI.
- The pattern matching (regex) rule and application filter rule cannot be used together in the same second-level map.
- Application Intelligence does not detect or classify ARP requests for both Gen 2 and Gen 3 devices, resulting in the dropping of packets that do not meet an APF match.
- The maximum number of user-defined applications 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.

Application Intelligence Session

Application Visualization (formerly known as Application Monitoring) collects application statistics from GigaVUE physical device and sends this information to GigaVUE-FM, GigaVUE HC Series, which acts as an application monitor. The monitoring reports are sent to GigaVUE-FM, GigaVUE HC Series on port 2056. The application statistics are displayed as a set of monitoring reports, providing easy-to-read graphical representations of application usage data. This gives you better insight over how your network is utilized and which applications consume the most resources. To enable Application Monitoring, you need to create the application intelligence session on GigaVUE HC Series devices managed by GigaVUE-FM, GigaVUE HC Series.

Application Visualization uses various classification methods to identify applications. The application statistics exported to GigaVUE-FM may take up to seven minutes to populate the following dashboards:

- Top 10 Applications
- Top 10 Applications Families
- Total Traffic
- Total Applications

Users can view the statistics based on the following metrics, Bits, Packets, and Flows. Historical data can be accessed for up to seven days. and Users can export the application visualization records using the IP interface. However, it's not recommended to use the IP interface, as disruptions to the data plane may prevent GigaVUE-FM from collecting and displaying the statistics.

Create an Application Intelligence Session in Physical Environment

To create an Application Intelligence Session:

1. On the left navigation pane, select **Traffic > Solutions > Application Intelligence**.
2. Click **Create New**. The **Create Application Intelligence Session** page appears.

NOTE: If the Create button is disabled, check whether a valid license for Application Metadata Intelligence or Application Filtering Intelligence is available.

3. In the **Basic Info** section complete the following:
 - Enter the name and description (optional).
 - Select **Physical** in the Environment field.
 - Select the node from the list of nodes.

4. In the **Configurations** section, view the following:

Option	Mandatory	Default	Notes
Monitoring	No	Enabled	AppViz is enabled by default. It can be disabled when not required. Disabling it can improve the performance.
Export Interval	Yes	300s (5 minutes)	Configures the interval of the records to be exported to GigaVUE-FM for AppViz. This is not user configurable from 6.4 onwards.
Fast Mode	No	Disabled.	<div> NOTE: It supports exporting limited HTTP attributes. GigaVUE FM automatically enables selecting only the supported attributes </div> <div> NOTE: The Fast Mode option can be enabled or disabled only when creating a new application intelligence session. </div>

5. Select a GigaSMART Group. You can also choose to create a new GigaSMART Group.

- Provide a name in the **Alias** field.
- Select a port or multiple ports from the **Port List**.
- Set Application Session Filtering Buffer Size


- Set Metadata Export Buffer Size
 - Click **Save**.
6. In the **User Defined Applications** section, select the template from the inventory where it was created. Refer [Configure User Defined Application](#) to know more about configuration steps.
 7. If you are unable to view the required port in the **Port** field, perform these steps:
 - o Click **Port Editor**. Select the **Type** as **Tool** from the drop-down list for the required **Port Id**. Select **OK**.
The selected Port appears in the list.
 - o Select the **Type** as:
 - o IPv4 - to allow the traffic in IPv4 interface.
 - o IPv6 - to allow the traffic in IPv6 interface.
 - o Provide the **IP Address, IP Mask, Gateway**, and **MTU**. Provide the IP address corresponding to the IP interface selected.
 - o Click **Save**.
 8. In the **DestinationSettings**, enter the destination IP address. The version of IP address in the Destination field should be same as the version of IP address defined in the IP-interface (applicable only when IP interface is selected). By default, the IP address of the GigaVUE-FM,GigaVUE HC Series interface is displayed.
 9. In the **Source Traffic** section, select a source port that require application monitoring in the **Source ports** field. Source port can be a single port, multiple ports, and port groups.
- NOTE:** Ports already used as source ports in the intent-based orchestrated solution will not be listed in the drop-down.
10. Click **Save**. The session created is added in the list view.
 11. In the created session, click **Edit** to perform operations related to **Application Filtering, De-duplication** and **Application Metadata**.
 12. Configure the rules for filtering the required traffic in the **L2-L4 Rules** fields. To configure a rule:
 - a. Click **Select Conditions**. Select the required parameters from the drop-down list.
 - b. Select the value for the parameters from the drop-down.
 - c. Select the required options:
 - Pass or Drop - Based on the parameter selected in the Conditions fields, the traffic that matches the conditions will either be passed or dropped.
 - Bidirectional - Allows the traffic in both directions of the flow.

NOTE: Click “+” to create multiple rules for filtering the required traffic, and click “+ New Source Traffic” to create multiple sources with filtering options.

Refer to the Map Rules section in [Inner Header and MPLS Header Filtering](#).

You can configure Inner Header qualifiers and MPLS Header qualifiers for GigaVUE-TA400 device. Refer to [Inner Header and MPLS Header Filtering](#).

The total applications participating in the network traffic are displayed in the Application Intelligence Dashboard. For more information about the dashboard, refer to the [View the Application Intelligence Dashboard](#).

If the session configuration is unsuccessful, troubleshoot the error notified (refer to [View the Health Status of a Solution](#)). Click the **Reapply all pending solutions** button  in the dashboard to redeploy the configuration.

You can also filter the traffic based on the applications. For more information, see [Create Application Filtering Intelligence for Physical Environment](#).

NOTE: Users may want to filter traffic upfront based on VLAN, subnet, and host IP address. Filtering traffic upfront can also reduce the load on the DPI engine. Application Intelligence supports configuring L2-L4-based rules to filter such traffic.

Configure User Defined Application

To configure User Defined Application signatures :

Step Number	Task	Refer the following
1	Create rules under User Defined Application Section	Create rules under User Defined Application
2	Configure Application Intelligence Session	For Physical: Application Intelligence Session
3	Monitor User Defined Application	View the Application Intelligence Dashboard

Create Rules under User Defined Application

1. Click **Inventory**.
2. Click **User Defined Applications** to create rules based on a set of **Supported Protocols and Attributes**. For information on **Supported protocols and Attributes** refer **User Defined Application** topic. This helps the physical or virtual node to classify the traffic based on the protocols and attributes selected in the created rule.

3. Click **New** in the **User Defined Applications** screen to create a new rule.

4. Enter **Application Name**.

5. Enter **Priority**. The value must be between 1 and 120.

Note: The least value will have the highest priority.

6. In the created rule:

a. Choose the **Protocol** from the list of protocols.

NOTE: The **HTTP2** protocol is not listed under the list of protocols. You need to select **HTTP** for configuring the signatures for HTTP2 applications.

b. Choose the **Attributes** from the list of attributes.

c. Choose the **Values** from the list of values.

7. Click **Apply**. The rule is now created. For information on the limitations for creating rules refer Configuration Limitations section.

8. Click the application listed under the **Applications** column.

9. Click the **Rule** tab.

10. Select a rule to view its protocol details.

For Regex examples, refer the **Supported Protocols and Attributes** section.

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	Client to	REGEXP	(.*\.)?gigamon\.com

			Name from URI or Host	Server Only		
	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 is redirected to	Server to Client Only	REGEXP	.*\football\.*
	cts-cookie	Cookie (Raw)	Raw value of the HTTP Cookie header line	Client to Server Only	REGEXP	.*tEstCoOkie.*
	content	Content	Message body	Both, Client	REGEXP	.*GIGAMON.*

			content	to Server or Server to Client		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 Hello message or the certificate		REGEXP	(.*\.)?gigamon\.com
	stc-subject_alt_name	Subject Alt Name(s)	List of host names which belong to the	Server to Client Only	REGEXP	(.*\.)?gigamon\.com

			same certificat e			
rtmp	cts- page_ url	Page URL	URL of the webpage where the audio/vid eo content is streame d	Client to Server Only	REGEXP	http://www.music.tv/recorded/1234567
tcp	stream	Payload Data	Data payload for a packet, excludin g 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 packet, excludin g the header		REGEXP	.*GIGAMON.* mindata = 100 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	REGEXP	GVUE-release 6.2.0

				to Server or Server to Client		
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 Differentiated Service (DS) Field in IP header		UINT8 as REGEXP String	33

	resolv_name	DNS Name	Server's DNS name		REGEXP	gigamon.com
ipv6	address	Server IP Address	IP address of the server		IPV6 as REGEXP String	2001:0:9d38:6ab8:307b:16a4:9c66:5f4 2001:0:9d38::9c66:5f4/64
	dscp	DSCP Value	DSCP from Differentiated 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

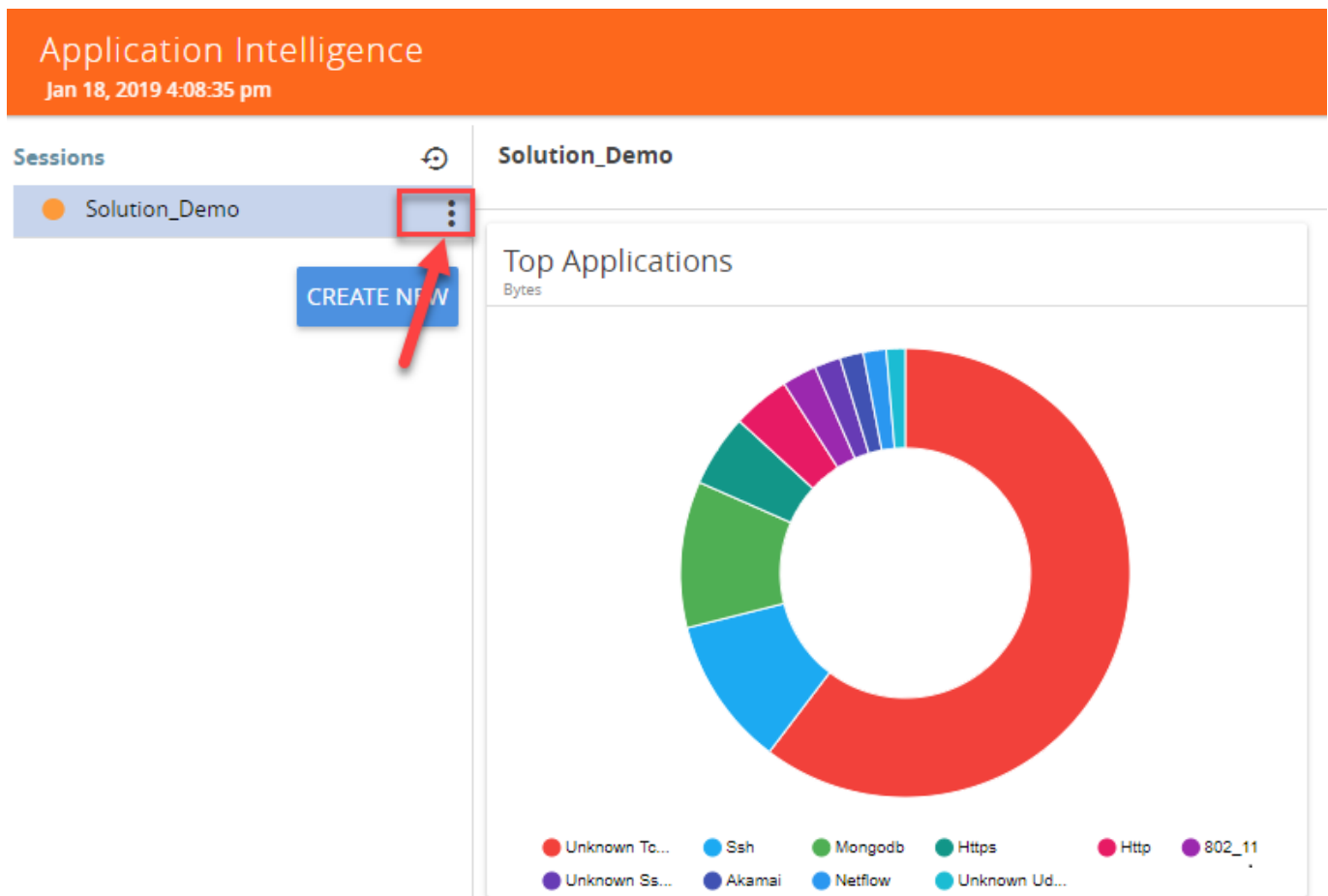
Pattern	Description
.	Matches any symbol
*	Searches for 0 or more occurrences of the symbol or character set that precedes it
+	Searches for 1 or more occurrences of the symbol or character set that precedes it
?	Searches for 0 or 1 occurrence of the symbol or character set that precedes it
()	Groups 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

View the Details of an Application Intelligence Session

To view the details and the statistics of a session, do the following steps:

1. Select the session from the **Application Intelligence Sessions** pane for which you need to view the sessions details, health status and statistics, and click the ellipsis as shown:

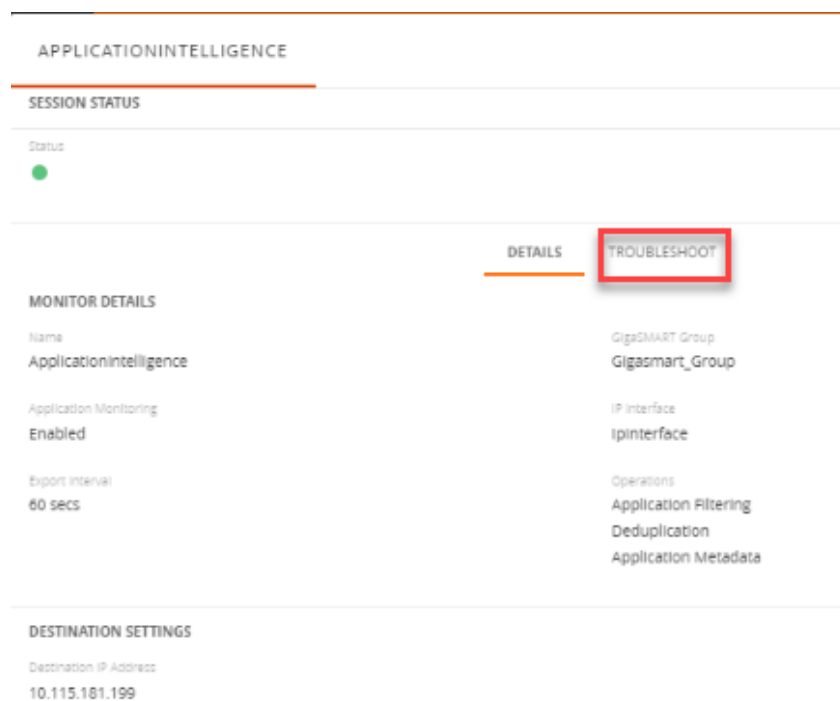


2. Select **View Details** from the drop-down list.

You can view the Monitoring Details, Destination Settings, Source Traffic, and Application Filtering-Destination Traffic, and Application Metadata-Destination Traffic in the Details page.

NOTE: You can edit the Source Traffic, Application Filtering-Destination traffic, and Application Metadata-Destination Traffic from the view details window.

3. Click **Troubleshoot** to view the current statistics and health status of components associated with the solution.



The details of the components that can be viewed for a solution are shown in the following table:

Components	Details of Components
Source Traffic	<ul style="list-style-type: none"> ◦ Network Ports ◦ First Level Maps ◦ L2-L4 Rules
GigaSMART	<ul style="list-style-type: none"> ◦ GigaSMART Port ◦ GigaSMART Group ◦ Virtual Port
Application Monitoring	<ul style="list-style-type: none"> ◦ IP interface ◦ Exporter

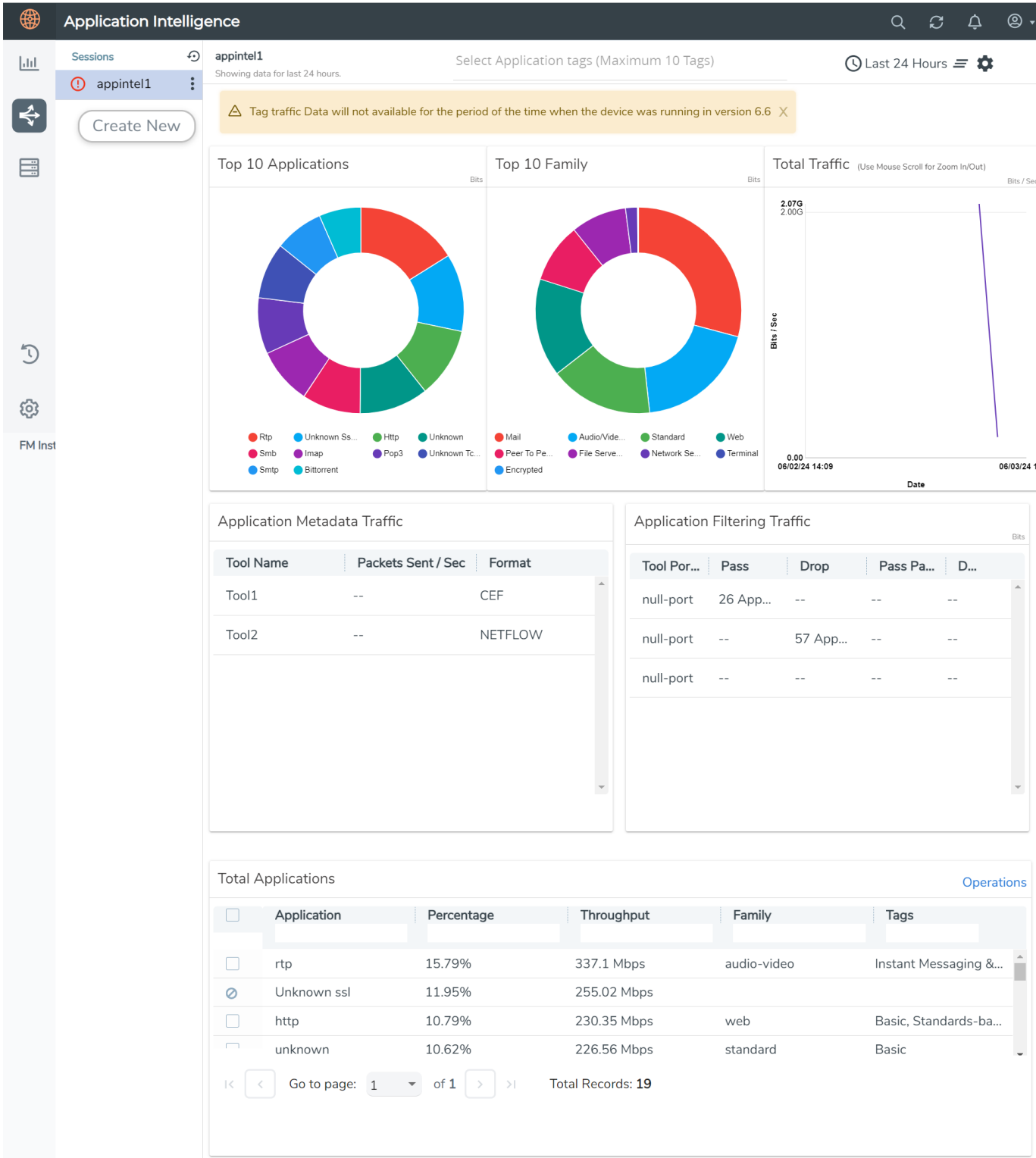
Components	Details of Components
Application Filtering - Destination Traffic	<ul style="list-style-type: none">◦ Second Level Map◦ Applications and Advanced Rules◦ Tool Ports◦ GigaSMART Operation (GSOP)
Application Filtering	<ul style="list-style-type: none">◦ Application Session Filtering
Application Metadata	<ul style="list-style-type: none">◦ IP Interface◦ Cache◦ Metadata Tools

The troubleshooting page has a flow diagram representing the components associated to the solution. You can also click on the blocks in the flow diagrams to view the details of the corresponding components.

To learn more about the color indication and the health status of a solution refer to [View the Health Status of a Solution](#).

View the Application Intelligence Dashboard

After creating the Application Intelligence Session, you can monitor the applications in the network by the reports displayed in the Dashboard as shown in the following figure:



Application Intelligence Dashboard displays the following metrics:

NOTE: The **Top 10 Application Families** metric and the **Select Application Tags** option are supported only on Gen 3 GigaSMART module and available from software release version 6.7.00 only.

- **Top 10 Applications:** 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 name in the network. The legend for the Pie-chart appears at the bottom. When you select a pie, you can view the corresponding data highlighted in the Total Applications table.
- **Top 10 Application Families:** You can view a graphical representation of top 10 application families running in the network based on the metrics. When you hover over the Pie-chart, GigaVUE-FM shows the application family name in the network.

NOTE: The **Top 10 Applications** Pie-chart may include user defined applications, but their corresponding Application Family will not be seen in the **Top 10 Application Families** Pie-chart. The user defined applications are not categorized under any family. So, if user defined applications are involved, there may be a variation in the **Top 10 Applications** and **Top 10 Application Families** Pie-charts.

- **Total Traffic:** You can view the total traffic of the network represented in the linear form of a graph.
- **Total Applications:** You can view the applications and their bandwidth in the network. You can also select the required application for filtering and exporting metadata by using the Operations field. When the following application family names are displayed in the Application list, it implies that the application could not be successfully identified:
 - unknown — unknown application name and protocol
 - unknown-TCP — unknown application name that belongs to TCP flow.
 - unknown-HTTP — unknown application name that belongs to HTTP flow.
 - unknown-UDP — unknown application name that belongs to UDP .
 - unknown-SSL — unknown application name that belongs to SSL flow.

NOTE: You can filter the applications listed under **Total Applications** using the parameters such as **Application**, **Percentage**, **Throughput**, **Family**, and **Tags**.

NOTE: You can forward the unknown application family traffic to a packet capture tool, analyze the packet capture and configure User Defined Application signatures to identify them.


- **Application Filtering Traffic:** You can view the statistics of the applications that are filtered in the tool ports in the dashboard after creating an Application Filtering Intelligence session for a device. You can view the number of applications that are dropped and passed through for the Application Filtering Traffic.
- **Application Metadata Traffic:** You can view the details of the Tool Name and the Format in which the metadata of the application is exported.

You can use the **Select Application Tags** option to filter the traffic specific to the selected application tags. On selecting the tags for filtering, the following widgets will show only the data specific to the selected tag:

- **Total Traffic**
- **Top 10 Applications**
- **Top 10 Application Families**
- **Total Applications**

GigaVUE-FM enables you to view the above metrics for a particular period by selecting the date and time from the dashboard.

GigaVUE-FM, GigaVUE HC Series 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 10 minutes to display the statistics after receiving the traffic.

You can also choose to view the graphs in the dashboard for the metrics in bytes, packets or flows. To view the metrics in bytes, packets or flows, click the gear  button in the right corner of the Application Intelligence dashboard.

NOTE: By default, you can view the metrics in the dashboard for the last one hour, if the period is not selected. From the Date Range field you can choose to view metrics from Last 1 Hour, Last 24 Hours, Last 7 days or even customize the date range by selecting the Custom option.

NOTE: The complete historical application visualization data except for the last twenty-four hours.

Application Filtering Intelligence

Application Filtering Intelligence (AFI) functionality on GigaSMART allows filtering traffic by selecting applications based on application name (such as YouTube, NetFlix, Sophos, or Facebook) or application family (such as Anti Virus, Web, ERP or Instant Messaging”) or application tag (such as Multimedia Streaming, Gaming, Cryptocurrency). Organizations use AFI to effectively filter and forward relevant route crucial applications to one or multiple tools or to a Null Port.

NOTE: Application Filtering Intelligence (AFI) and Application Metadata Intelligence (AMI) licenses are available for individual purchase or as a bundle on GigaVUE HC Series. When obtained together, all applications passed by AFI are directed to packet monitoring tools and AMI. In certain scenarios, users may prefer to export NetFlow/IPFIX or application metadata for the filtered applications instead of monitoring raw packets. In such cases, users can select Null Port (dummy tool port) as the tool destination for AFI. Traffic sent to a Null Port is internally discarded.

Some organizations may want to conserve costs associated with network forensics. Generally, payload information is bulky. In most cases it's also encrypted. Hence, organizations may choose to discard the payload as it offers little value. AFI enables such organizations to slice each flow. Organizations can configure the Packet Count to filter-in only the packet headers and discard the rest.

In diverse environments, organizations may need to monitor different types of traffic separately and block specific applications from being monitored. AFI allows configuring distinct maps to either forward or block applications to the relevant tools, and these maps are processed using logical OR operation.

You can configure up to five maps with priorities. Higher priority maps take precedence over lower ones. It's best to prioritize maps with specific rules. Advanced rules can be set within each map to optimize traffic further, using a logical AND operation for multiple rules.

Large Flows in Application Filtering Intelligence

A Large Flow data flow is a single session (TCP Session) with a relatively long-running network connection that consumes a large or disproportionate amount of bandwidth, buffers, and queues. Because of this nature, large flows can cause packet drops in other traffic and significantly increase the mean-time-to-completion (mttc) of smaller flows (mouse flows)¹.

Large flows are considered to affect the traffic in the following ways:

¹Mouse data flows are emails, web pages, data requests, or other short-lived data flow

- Disproportionately affects mouse data flows mean-time-to-completion (mttc).
- Causes significant issues to tools, detecting problems with applications and next-generation firewall (NGFW), as it causes high CPU spikes and bandwidth consumption.
- Large flows are often related to high use low inspection traffic, for example, backups, database replication, VM migrations, data migrations, etc., inside the data centers that impact network bandwidth for minutes or hours or more.

Refer to [Handle Large Flows in Application Filtering Intelligence](#) to learn more about configuration steps.

Application Session Filtering (ASF) and Buffer ASF

NOTE: The ASF license requires the APF license to be installed as a prerequisite.

Application Session Filtering (ASF) provides additional filtering on top of Adaptive Packet Filtering (APF). With APF, you can filter on any data patterns within a packet. With ASF, you apply the pattern matching and then send all the packet flows associated with the matched packet to monitoring or security tools.

ASF allows you to filter all traffic corresponding to a session. Use ASF to create a flow session and send the packets associated with the flow session to one or more tools. A flow session consists of one or more fields that you select to define the session. Either the packets for the whole session can be captured or only the packets following a pattern match.

A flow session is a session defined by protocol fields in the packet. For example, you can define a flow session with source and destination IP (two tuple), source and destination IP plus source and destination port (four tuple), or any combinations with inner or outer IP/port and protocol.

For example, use APF to filter TCP packets to capture the SYN packet. Then use ASF with GigaSMART Load Balancing to send all subsequent packets associated with the session to multiple tool ports. This example is illustrated in [Application Session Filtering \(ASF\) and Buffer ASF](#). For information on capturing a whole session by buffering packets, refer to [Application Session Filtering \(ASF\) and Buffer ASF](#).

Or use APF to create pattern-matching filters in which the pattern is a sequence of data bytes at a variable or fixed offset within a packet. Then use ASF with a specified session definition to capture subsequent packets belonging to the session. When an incoming packet matches an APF rule, a flow session is created. The subsequent incoming packets that match the value of the fields in the flow session will be forwarded to the same tool port as the matching packet.

For example, use APF to pattern match the string *www.gigamon.com*. Use the 5tuple field to identify the flow session. This creates the signature of the session. All the packets associated with the session will be forwarded to a tool port, hence APF becomes flow-aware or session-aware.

ASF provides the following session capabilities:

- filter on one, two, or both MPLS labels and/or VLAN IDs
- filter on both inner and outer IP addresses, Layer 4 ports, and protocols

Pattern matching examples are illustrated in [ASF and Buffer ASF Examples](#).

For information on load balancing, refer to stateful load balancing in the section [GigaSMART Load Balancing](#).

ASF operations can be assigned to GigaSMART groups consisting of multiple engine ports. Refer to [Groups of GigaSMART Engine Ports](#) for details.

In ASF and buffer ASF second level maps, a maximum of five (5) maps can be attached to a virtual port (vport). Each map can contain up to 25 gsrules.

Application Session Filtering (with or without buffering) is a pillar of the GigaSECURE Security Delivery Platform.

Session-Aware APF (SAPF) Renaming and Licensing Change to ASF

The GigaSMART feature named Session-Aware Adaptive Packet Filtering (SAPF) in GigaVUE-OS 4.3 was renamed to Application Session Filtering (ASF) in GigaVUE-OS 4.4. It is now encompassed within ASF as the non-buffering equivalent to Application Session Filtering with buffering.

In addition, the license has moved from the APF license to the ASF license.

Application Session Filtering with Buffering

ASF captures packets of a session after an APF rule match. When the APF match occurs in the middle of a session, packets in the session prior to the match are not captured. With some tools needing all the packets of a flow session in order to perform data analysis, GigaSMART uses buffering to ensure that all packets belonging to a flow session are captured and forwarded to the tools. This is referred to as Application Session Filtering with buffering, or buffer ASF.

Buffer ASF uses the pattern-matching and regular expression engine in APF to select packet flows based on matching criteria with one or more packets in the flow session. Buffering ensures that the entire session, from start to finish, is either dropped or forwarded to the security tools or the performance monitoring tools.

To capture all packets belonging to a flow session prior to the APF rule match, ASF needs to know the first packet of a flow session. For this, GigaSMART supports both TCP and UDP connections.

For TCP connections, the TCP SYN packet is used to indicate the start of a session. GigaSMART captures and stores (or buffers) all packets of a flow session until an APF match occurs. After that, GigaSMART will either forward or drop all stored packets belonging to that session based on the APF pass or drop rule that is configured. Subsequent packets after the APF match will be forwarded or dropped as they arrive.

For UDP connections, there is no special packet that indicates the start of a UDP flow session from a Layer 4 perspective. GigaSMART will take the first UDP packet of a session it encounters as the start of a session flow. This may result in incomplete capture at the beginning of configuration or at system boot up, but as new UDP sessions arrive, GigaSMART will capture the first packet of the flows.

ASF and Buffer ASF Session Definitions

Use the **Session Field** of the **ASF** page to define ASF and buffer ASF sessions by specifying session field attributes to add or delete. A session field is a group of one or more fields that define a flow session. (From the device view, select **GigaSMART > ASF** and click **New** to open the ASF page.)

A flow session consists of field names and attributes. Some field names include multiple attributes, which provide a quick way to define sessions.

The field names and attributes are as follows:

- gtpu-teid
- ipv4 (ipv4-src, ipv4-dst)
- ipv4-5tuple (ipv4-src, ipv4-dst, l4port-src, l4port-dst, ipv4-protocol)
- ipv4-dst
- ipv4-l4port-dst (ipv4-src, ipv4-dst, l4port-dst)
- ipv4-protocol
- ipv4-src
- ipv4-src-l4port-dst (ipv4-src, l4port-dst)
- ipv6 (ipv6-src, ipv6-dst)
- ipv6-5tuple (ipv6-src, ipv6-dst, l4port-src, l4port-dst, ipv6-protocol)
- ipv6-dst
- ipv6-l4port-dst (ipv6-src, ipv6-dst, l4port-dst)
- ipv6-protocol
- ipv6-src
- ipv6-src-l4port-dst (ipv6-src, l4port-dst)

- l4port (l4port-src, l4port-dst)
- l4port-dst
- l4port-src
- mpls-label
- vlan-id

An ASF session definition consists of combinations of the fields and attributes in the list above. In addition, for all IP and L4 port fields in the packet, each ASF session field must specify **outer** or **inner** for location. Outer specifies the first IP or L4 port in the packet. Inner specifies the second IP or L4 port in the packet (usually inside tunneling). For VLAN ID and MPLS label fields, a position (1 or 2) must be specified. Position 1 is the first occurrence of the protocol header or field in the packet. Position 2 is the second occurrence of the protocol header or field in the packet.

A buffer ASF session definition consists of combinations of the fields and attributes in the list above. **One restriction is that ipv4-src or ipv6-src needs to be defined, as a minimum.** In addition, the following restrictions apply to buffer ASF session definitions:

- the gtpu-teid field name is not supported
- the IP and L4 port fields only support location **outer**
- the VLAN ID field only supports position 1

All packets belonging to the same source and destination IP will be considered as the same flow session. This is useful if you want to capture all packets belonging to separate TCP/UDP connections that have the same IPs, such as control or data flows.

Define ASF Session

When defining an ASF session, enter the fields, attributes, and options, then save. The changes only take effect when after you save. For example, in [Figure 1An ASF Configuration](#), the settings are:

- Alias is asf2, which is name of the ASF Profile for the GigaSMART Operation
- buffer enabled
- Buffer Count before Match is 5
- ipv4-5tuple outer
- vlan-id position 1

ASF

Alias

asf2

Configuration

BI-directional

☐ Enable

Buffer

☒ Enable

Buffer Count before Match

5

Protocol

TCP Only ▼

Packet Count

☐ Enable

Timeout

15

secs

Session field

Ipv4-5tuple ✕

vlan-Id ✕

Position

☒ Outer

☐ 1

Figure 1 An ASF Configuration

Quick Session Delete for Buffer ASF

For a buffer ASF session defined with ipv4-5tuple or ipv6-5tuple, there is a quick session delete for TCP connections. The session is deleted 4 seconds after RST or both FIN packets are detected, signaling the end of the flow.

Specify Resources for Buffer ASF

A large number of sessions can consume significant memory resources on the GigaSMART line card or module. While a reload is not required the first time buffer ASF resources are allocated. However, any subsequent changes to the session count, such as increasing from 1 million to 3 million or decreasing to 2 million, will require a reload for the changes to take effect and for resources to be properly reallocated.

The following table provides the range of the supported sessions for AFI on GigaVUE HC Series platform.

Platform	Gen2- Range in million	Gen3- Range in million
GigaVUE-HC1	1M	1M-2M
GigaVUE-HC3	1M-3M	1M-3M
GigaVUE-HC1-Plus	NA	Front: 1M-2M

Platform	Gen2- Range in million	Gen3- Range in million
		Rear: 1M-3M
GigaVUE-HCT	NA	1M-2M

**Notes:**

- Starting from version 6.12, the system uses the maximum range as the default value during configuration. To maintain backward compatibility, the system assigns the minimum range as the default value when the device runs an older version.
- When upgrading from a lower version to a higher version, if the existing solution range exceeds the maximum allowed value, it is limited to the maximum range.

You can reload the card from the UI, by doing the following:

- From the left navigation pane, go to **Inventory > Physical > Nodes**.
- From the left navigation pane, go to **System > Chassis**.
- Clicking the Table View button to open the Table View of the Chassis.
- Under Cards, select the card to reload.
- From the **Actions** menu, select **Shut Down**.
- Now select **Start Up** from **Actions** menu.

Alternatively, you can use the following GigaVUE-FM,GigaVUE HC Series API to reload the card:

PATCH /inventory/chassis/cards/{slotId}

For more information about the GigaVUE-FM,GigaVUE HC Series APIs, refer to the *GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide*.

You can also reload the card with the following two CLI commands:

(config) # card slot <slot ID> down

(config) # no card slot <slot ID> down

For more information about the CLI commands, refer the *GigaVUE-OS CLI Reference Guide*.

ASF and Buffer ASF Session Notes

The following are the notes related to ASF and buffer ASF:

1. A session field can only be modified or deleted if it is *not* configured in any GigaSMART operation.
2. A session field can only contain the same session attribute and position pair once.
3. A session field cannot contain overlapped session attribute and position. For example, the following is not valid: ipv4-5tuple outer and ipv4-src outer.
4. Up to a maximum of 25 flow session aliases are supported for ASF.
5. A total of 4 session tables per GigaSMART engine are supported for ASF. Each table has its own session definition.
6. Up to 2 million session entries are supported for ASF. The entries are shared by all session aliases.
7. Each session table (session alias) can only be used once within a gsgroup.
8. The number of buffer ASF sessions supported is configurable from 1 to 5 million.
9. The number of packet buffers supported for buffer ASF is from 1 to 5 million.

Buffer ASF Packet Processing Special Cases

The following are special cases of packet processing for buffer ASF:

- Non-TCP SYN packet received and no session matched—When a non-TCP SYN packet is received and there is no session matched, the packet will be considered as *no match* and will be passed to other maps. If there is no match after all maps have been processed, the packet will be forwarded to a shared collector, if one is configured.
- Out of session—When a TCP SYN packet is received and no free session is available, the packet will be considered as *no match*. Other packets belonging to this session will also be considered as *no match*, as for the special case described above.
- Out of packet storage buffer—When the buffer is full for the first packet of a session, the session will not be created and the packet will be considered as *no match*. When the buffer is full for an existing session, and the APF match has not yet occurred, a flag will be set and the current packet and all buffered packets will be considered as *no match*. Subsequent packets will also be considered as *no match*.
- Exceeded configured buffering limit—When there is no APF match after the configured number of packets have been buffered, all buffered packets and all subsequent packets belonging to this session will be considered as *no match*.

Map Statistics

Go to **Map > Statistics** to display counts of the rules that actually matched in a map. A single packet can match one or more rules. For example, if a single packet matches multiple rules in an ASF or buffer ASF map, all matching rules will have that packet counted against them and the overall map status pass counter will show 1.

Enhanced Application Session Filtering

Enhanced Application Session Filtering (ASF) allows you to filter a specific application field from the incoming traffic. Enhanced Application Session Filtering supports the following session capabilities:

- Applications SSL —Supports SNI field in a hello packet.
- HTTP—Supports HOST and User-agent field in a request packet

You can use the matching pattern in a regex profile using the regular expression format. Rules are applied based on the order in which it was created.

When a rule matches, the corresponding pass or drop action is taken on the packets. In a session, when a packet matches a pass rule, the packet and its subsequent packets belonging to the same session are forwarded to and processed by the next GS application belong to the same GSOP.

When a packet of a session matches a pass rule, the packet and the subsequent packets belonging to the same session are forwarded to and processed by the next GigaSMART application that belongs to the same GSOP. If there is no GigaSMART application in the downstream application chain in the GSOP, the packet and the subsequent packets belonging to the same session are forwarded to the tool port defined in the Map.

When a packet of a session matches a drop rule, the packet and the subsequent packets belonging to the same session are dropped.

When a packet of a session does not match a rule, it will be examined by the next rule. When a packet does not match any rules defined in the Enhanced ASF profile, the packet will be forwarded to and processed by the GSOP configured in the next Map belonging to the same VPORT.

When you create new rules, those rules are applied only to new sessions created after the rules are configured. These rules are not applied to the sessions that were already active. Any changes you make will impact only future sessions, ensuring that updates to rules do not disrupt ongoing or previously established sessions.

ASF and Buffer ASF Examples

This section provides you different use case examples for non-buffered and buffered ASF configurations.

For non-buffered ASF examples refer to the following :

- [Example 1: ASF, Forward TCP Traffic](#)

- [Example 2: ASF, Forward VNC Traffic](#)
- [Example 3: ASF, Forward Traffic Matching a Pattern](#)
- [Example 4: ASF, Forward GTP Traffic](#)

For buffered ASF examples refer to the following:

- [Example 1: Buffer ASF, Drop Netflix Traffic](#)
- [Example 2: Buffer ASF, Drop YouTube Traffic](#)
- [Example 3: Buffer ASF, Drop Windows Update Traffic](#)
- [Example 4: Buffer ASF, Forward VNC Traffic](#)
- [Example 5: Buffer ASF, Forward HTTPS Traffic on Non-Standard Port](#)

Example 1: ASF, Forward TCP Traffic

In Example 1, ASF is used with GigaSMART Load Balancing and Adaptive Packet Filtering to load balance TCP traffic among multiple tool ports. TCP SYN indicates the start of a connection. Once the TCP SYN packet is detected, subsequent packets belonging to the same TCP connection will be forwarded to a configured tool port. Packets belonging to the same connection will be sent to the same tool port, regardless of the number of connections.

NOTE: This example uses APF to filter TCP packets to capture the SYN packet. Alternatively, use buffer ASF to capture a whole session by buffering packets.

Task	Description	UI Steps
1	Create a flow session.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > ASF. 2. Click New. 3. Type asf4 in the Alias field. 4. Select ipv4-tuple from the Session field list. 5. Select outer. 6. Click Save.
2	Create a port group and specify the tool ports for load balancing.	<ol style="list-style-type: none"> 1. Select Ports > Port Groups > All Port Groups. 2. Click New. 3. Type portgrp1 in the Alias field. 4. Select Tool. 5. Select SMART Load Balancing. 6. Click in the Ports field and select the tool ports. For example, 1/1/x6, 1/1/x7, 1/2/x3, and 1/2/x4.
3	Configure a GigaSMART group and associate it with GigaSMART engine ports.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Groups > GigaSMART Groups. 2. Click New. 3. Type gsgrp1 in the Alias field. 4. Select two engine ports from the Port List field. For

Task	Description	UI Steps
		<p>example, 1/3/e1 and 1/3/e2</p> <p>5. Click Save.</p>
4	Configure the combined GigaSMART operation.	<p>1. From the device view, select GigaSMART > GigaSMART Operations (GSOP) > GigaSMART Operation and create two GigaSMART Operations.</p> <p>2. Click New.</p> <p>3. Type gsop1 in the Alias field.</p> <p>4. Select gsgroup1 from the GigaSMART Groups list.</p> <p>5. Select the operations.</p> <ul style="list-style-type: none"> o APF o ASF with asf4 for the ASF profile o Load Balancing with Stateful Type ASF, and Round Robin <p>6. Click Save.</p>

Task	Description	UI Steps
5	Create a virtual port and associate it with the GigaSMART group.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > Virtual ports. 2. Click New. 3. Enter vp1 in the Alias field. 4. Select gsg1 from the GigaSMART Groups list. 5. Click Save.
6	Create a first level map.	<ol style="list-style-type: none"> 1. Select Maps > Maps > Maps. 2. Click New. 3. Configure the map. <ol style="list-style-type: none"> a. Type map11 in the Alias field. b. Select First Level for Type. c. Select By Rule for Subtype. d. Select the network port 1/1/x1 for the Source. e. Select the virtual port vp1 for the Destination. 6. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Pass. c. Select IPv4 Version and set version to 4 4. Click Save.
7	Create a second level map. The gsrule captures the first packet of a session.	<ol style="list-style-type: none"> 1. Click New. 2. Configure the map. <ol style="list-style-type: none"> a. Type map22 in the Alias field. b. Select Second Level for Type. c. Select By Rule for Subtype. d. Select the virtual port vp1 for the Source. e. Select the port group portgrp1 for the Destination. f. Select gsop1 form the GSOP list. 7. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Pass. c. Select TCP Control. d. Enter 2 for Value. e. Enter 0 for Mask. f. Set Position to 1. 7. Click Save.

Example 2: ASF, Forward VNC Traffic

In Example 2, traffic from a Virtual Network Computing (VNC) application is forwarded from network port 1/1/x1 to tool port 1/1/x6. Packets will be matched with a VNC signature. Once a packet is matched, subsequent packets with the same IPv4 5tuple will be forwarded to the

same destination as the matching packet. By default, both the forward and the reverse traffic of the same session will be captured and forwarded.

Step	Description	Command
1	Create a flow session.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > ASF. 2. Click New. 3. Type asf1 in the Alias field. 4. Select ipv4-tuple from the Session field list. 5. Select outer. 6. Click Save.
2	Configure a GigaSMART group and associate it with GigaSMART engine ports.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Groups > GigaSMART Groups. 2. Click New. 3. Type gsgrp1 in the Alias field. 4. Select two engine ports from the Port List field. For example, 1/3/e1 and 1/3/e2 5. Click Save.
3	Configure the combined GigaSMART operation.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Operations (GSOP) > GigaSMART Operations and create two GigaSMART Operations. 2. Click New. 3. Type gsop1 in the Alias field. 4. Select gsgrp1 from the GigaSMART Groups list. 5. Select the operations. <ul style="list-style-type: none"> o APF o ASF with asf1 for the ASF profile 6. Click Save.

Step	Description	Command
4	Create a virtual port and associate it with the GigaSMART group.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > Virtual ports. 2. Click New. 3. Enter vp1 in the Alias field. 4. Select gsggrp1 from the GigaSMART Groups list. 5. Click Save.
5	Create a first level map.	<ol style="list-style-type: none"> 1. Select Maps > Maps > Maps. 2. Click New. 3. Configure the map. <ol style="list-style-type: none"> a. Type map11 in the Alias field. b. Select First Level for Type. c. Select By Rule for Subtype. d. Select the network port 1/1/x1 for the Source. e. Select the virtual port vp1 for the Destination. 6. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Pass. c. Select IPv4 Version and set Version to 4 4. Click Save.
6	Create a second level egress map. The gsrule contains the VNC signature.	<ol style="list-style-type: none"> 1. Click New. 2. Configure the map. <ol style="list-style-type: none"> a. Type map22 in the Alias field. b. Select Second Level for Type. c. Select By Rule for Subtype. d. Select the virtual port vp1 for the Source. e. Select the port group portgrp1 for the Destination. f. Select gsop1 form the GSOP list. 7. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Pass. c. Select Pattern Match. d. Select regex for Type and enter ^rfb 00[1-9]\.00[0-9]\x0a\$ e. Set Offset from 16 to 1000 6. Click Save.

Example 3: ASF, Forward Traffic Matching a Pattern

In Example 3, the traffic that matches a particular pattern (ymsg|ypns|yhoo) is forwarded from network port 1/1/x1 to tool port 1/1/x6 after adding a VLAN tag. Packets will be matched with the special signature. Once a packet is matched, subsequent packets with the same

source IP, source port, and VLAN ID will be forwarded to the same destination as the matching packet (after the VLAN header is inserted). By default, both the forward and the reverse traffic of the same session will be captured and forwarded.

Task	Description	UI Steps
1	Create a flow session and other parameters.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > ASF. 2. Click New. 3. Type asf2 in the Alias field. 4. Enable Packet Count. 5. Set Number of packets to 50. 6. Set the session field. <ul style="list-style-type: none"> o Select ipv4-src outer o Select vlan-id position 1 7. Select outer. 8. Click Save.
2	Configure a GigaSMART group and associate it with GigaSMART engine ports.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Groups > GigaSMART Groups. 2. Click New. 3. Type gsgrp1 in the Alias field. 4. Select two engine ports from the Port List field. For example, 1/3/e1 and 1/3/e2 5. Click Save.
3	Configure the GigaSMART operation.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Operations (GSOP) > GigaSMART Operation and create two GigaSMART Operations. 2. Click New. 3. Type gsop1 in the Alias field. 4. Select gsgrp1 from the GS Groups list. 5. Select the operations. <ul style="list-style-type: none"> o Adaptive Packet Filtering o Add Header and set VLAN to 1000 o ASF with asf2 for the ASF profile 6. Click Save.

Task	Description	UI Steps
4	Create a virtual port and associate it with the GigaSMART group.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > Virtual ports. 2. Click New. 3. Enter vp1 in the Alias field. 4. Select gsgrp1 from the GigaSMART Groups list. 5. Click Save.
5	Create a first level map.	<ol style="list-style-type: none"> 1. Select Maps > Maps > Maps. 2. Click New. 3. Configure the map. <ol style="list-style-type: none"> a. Type map11 in the Alias field. b. Select First Level for Type. c. Select By Rule for Subtype. d. Select the network port 1/1/x1 for the Source. e. Select the virtual port vp1 for the Destination. 6. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Pass. c. Select IPv4 Version and set Version to 4 4. Click Save.
6	Create a second level map. The gsrule contains the special signature.	<ol style="list-style-type: none"> 1. Click New. 2. Configure the map. <ol style="list-style-type: none"> a. Type map22 in the Alias field. b. Select Second Level for Type. c. Select By Rule for Subtype. d. Select the virtual port vp1 for the Source. e. Select the too port 1/1/x6 for the Destination. f. Select gsop1 form the GSOP list. 7. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Pass. c. Select Pattern Match. d. Select regex for Type and enter (ymsg ypns yhoo) e. Set Offsett from 16 to 1000 6. Click Save.

Example 4: ASF, Forward GTP Traffic

In Example 4, GTP traffic from network port 1/1/x1 is load balanced based on inner IP and tunnel ID to four tool ports: 1/1/x6, 1/1/x7, 1/2/x3, and 1/2/x4. APF filters GTP-u packets. Once a

packet is matched, subsequent packets in the same direction with the same gtpu-teid and inner IP will be forwarded to the same destination as the matching packet. In Example 4, both the outer and inner IP are IPv4.

Task	Description	UI Step
1	Create a flow session and other parameters.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > ASF. 2. Click New. 3. Type asf3 in the Alias field. 4. Set timeout to 90. 5. Set the session field. <ul style="list-style-type: none"> o Select gtpu-teid o Select Ipv4 inner 6. Select outer. 7. Click Save.
2	Create a port group and specify the tool ports for load balancing.	<ol style="list-style-type: none"> 1. Go to System > Ports > Ports > Port Groups > All Port Groups. 2. Click New. 3. Type portgrp1 in the Alias field. 4. Select Tool. 5. Select SMART Load Balancing. 6. Click in the Ports field and select the tool ports. For example, 1/1/x6, 1/1/x7, 1/2/x3, and 1/2/x4.
3	Configure a GigaSMART group and associate it with GigaSMART engine ports.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Groups > GigaSMART Groups. 2. Click New. 3. Type gsgrp1 in the Alias field. 4. Select two engine ports from the Port List field. For example, 1/3/e1 and 1/3/e2 5. Click Save.
4	Configure the combined GigaSMART operation.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Operations (GSOPS) > GigaSMART Operation and create two GigaSMART Operations. 2. Click New. 3. Type gsop1 in the Alias field. 4. Select gsgrp1 from the GigaSMART Groups list. 5. Select the operations. <ul style="list-style-type: none"> o Adaptive Packet Filtering o ASF with asf3 for the ASF profile o Load Balancing with Stateful, Type ASF, and Least Conn 6. Click Save.
5	Create a virtual port and associate it with the GigaSMART group.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > Virtual ports. 2. Click New.

Task	Description	UI Step
		<ol style="list-style-type: none"> 3. Enter vp1 in the Alias field. 4. Select gsgroup1 from the GigaSMART Groups list. 5. Click Save.
6	Create a first level map.	<ol style="list-style-type: none"> 1. Select Maps > Maps > Maps. 2. Click New. 3. Configure the map. <ol style="list-style-type: none"> a. Type map11 in the Alias field. b. Select First Level for Type. c. Select By Rule for Subtype. d. Select the network port 1/1/x1 for the Source. e. Select the virtual port vp1 for the Destination. 6. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Pass. c. Select IPv4 Protocol and set Value to UDP. d. Select Port Destination and set the port value to 2152 5. Click Save.
7	Create a second level map.	<ol style="list-style-type: none"> 1. Click New. 2. Configure the map. <ol style="list-style-type: none"> a. Type map22 in the Alias field. b. Select Second Level for Type. c. Select By Rule for Subtype. d. Select the virtual port vp1 for the Source. e. Select the port group portgroup1 for the Destination. f. Select gsgroup1 from the GSOP list. 7. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Pass. c. Select Pattern Match. d. Select IPv4 Protocol and enter the IPv4 address. Set Position to 1. e. Select Ipv4 Destination and set the port value to 2152. Set Position to 1. 6. Click Save.

Example 1: Buffer ASF, Drop Netflix Traffic

In Example 1, the goal is to drop all Netflix traffic. The flow session is defined by the 5tuple field and the first occurrence of VLAN ID. The Netflix traffic is expected to be identified in the first 6 packets of a session. (Configure the maximum number of packets buffered before the match to 5.) A maximum of 3 million sessions is specified.

Task	Description	UI Steps
1	Configure a GigaSMART group and associate it with GigaSMART engine ports and Define the maximum number of sessions, in millions.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Groups > GigaSMART Groups. 2. Click New. 3. Type gsgrp1 in the Alias field. 4. Select two engine ports from the Port List field. For example, 1/3/e1 and 1/3/e2 5. Under Params Resource Buffer select ASF and set the Buffer size to 3. 6. Click Save.
2	If needed, reload the GigaSMART line card or module to allocate the resources for buffer ASF.	<p>If you reset the buffer size of an ASF profile in Task 1, go to the Chassis page and select Table View. Under Cards, select the card to reload. From the Actions menu, select Shut Down and then Start Up.</p> <p>You can also issue the following CLI commands to reboot the card (the card is in slot 3 in this example):</p> <p>(config) # card slot 3 down (config) # no card slot 3 down</p>
3	Create a flow session, specify the buffer count before the match, and enable buffering. Note: The default protocol is TCP, so it does not need to be specified.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > ASF. 2. Click New or select an existing ASF profile then click Edit. 3. Type asf2 in the Alias field if this is a new ASF profile. 4. Enable Buffer. 5. Set Buffer Count before Match to 5. 6. Set the session field. <ul style="list-style-type: none"> o Select ipv4-5tuple outer o Select vlan-id position 1 7. Click Save.
4	Configure the combined GigaSMART operation.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Operations (GSOP) > GigaSMART Operation and create two GigaSMART Operations. 2. Click New. 3. Select gsgrp1 from the GigaSMART Groups list. 4. Type gsop1 in the Alias field. 5. Select the operations. <ul style="list-style-type: none"> o APF o ASF with asf2 for the ASF profile

Task	Description	UI Steps
5	Create a virtual port and associate it with the GigaSMART group.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > Virtual Ports. 2. Click New. 3. Enter vp1 in the Alias field. 4. Select gsgroup1 from the GigaSMART Groups list. 5. Click Save.
6	Create a first level map.	<ol style="list-style-type: none"> 1. Select Maps > Maps > Maps. 2. Click New. 3. Configure the map. <ol style="list-style-type: none"> a. Type map11 in the Alias field. b. Select First Level for Type. c. Select By Rule for Subtype. d. Select the network port 1/1/x1 for the Source. e. Select the virtual port vp1 for the Destination. 6. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Pass. c. Select IPv4 Protocol and set Value to UDP. d. Select Port Destination and set the port value to 2152 5. Click Save.
7	Create a second level map. The gsrule specifies the traffic to drop, using keywords. Buffered packets and all subsequent packets will be dropped.	<ol style="list-style-type: none"> 1. Click New. 2. Configure the map. <ol style="list-style-type: none"> a. Type map22 in the Alias field. b. Select Second Level for Type. c. Select By Rule for Subtype. d. Select the virtual port vp1 for the Source. e. Select the tool port 1/1/x6 for the Destination. f. Select gsop1 form the GSOP list. 7. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Drop. c. Select Pattern Match. d. Select regex and enter netflix nflxvideo nflximg Netflix nflxext. e. Set the offset from 0 to 1460 f. Set Protocol to tcp and set Position to 1. 7. Click Save.

Example 2: Buffer ASF, Drop YouTube Traffic

In Example 2, the goal is to drop all YouTube traffic. The YouTube traffic is expected to be identified in the first 7 packets of a session. (Configure the maximum number of packets buffered before the match to 6.) A maximum of 4 million sessions is specified.

Step	Description	Command
1	Configure a GigaSMART group and associate it with GigaSMART engine ports and define the maximum number of sessions, in millions	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Groups > GigaSMART Groups. 2. Click New. 3. Type gsgrp1 in the Alias field. 4. Select two engine ports from the Port List field. For example, 1/3/e1 and 1/3/e2 5. Under Params Resource Buffer, select ASF and set the Buffer Size to 4. 6. Click Save.
2	If needed, reload the GigaSMART line card or module to allocate the resources for buffer ASF.	<p>If you reset the buffer size of an ASF profile in Task 1, go to the Chassis page and select Table View. Under Cards, select the card to reload. From the Actions menu select Shut Down and then Start Up.</p> <p>You can also issue the following CLI commands to reboot the card (the card is in slot 3 in this example):</p> <pre>(config) # card slot 3 down (config) # no card slot 3 down</pre>
3	Create a flow session, specify the buffer count before the match, and enable buffering. Note: The default protocol is TCP, so it does not need to be specified.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > ASF. 2. Click New or select an existing ASF profile then click Edit. 3. Type asf2 in the Alias field if this is a new ASF profile. 4. Enable Buffer. 5. Set Buffer Count before Match to 6. 6. Set the session field to ipv4-5tuple outer 7. Click Save.
4	Configure the combined GigaSMART operation.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Operations (GSOP) > GigaSMART Operations and create two GigaSMART Operations. 2. Click New. 3. Type gsop1 in the Alias field. 4. Select gsgrp1 from the GigaSMART Groups list. 5. Select the operations. <ul style="list-style-type: none"> o Adaptive Packet Filtering o ASF with asf2 for the ASF profile 6. Click Save.
5	Create a virtual port and associate it with the GigaSMART group.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > Virtual Ports. 2. Click New.

Step	Description	Command
		<ol style="list-style-type: none"> Enter vp1 in the Alias field. Select gsgroup1 from the GigaSMART Groups list. Click Save.
6	Create a first level map.	<ol style="list-style-type: none"> Select Maps > Maps > Maps. Click New. Configure the map. <ol style="list-style-type: none"> Type map11 in the Alias field. Select First Level for Type. Select By Rule for Subtype. Select the network port 1/1/x1 for the Source. Select the virtual port vp1 for the Destination. Add a rule. <ol style="list-style-type: none"> Click Add a Rule. Select Pass. Select IPv4 Version and set Version to v4. Click Save.
7	Create a second level map. The gsrule specifies the traffic to drop, using keywords. Buffered packets and all subsequent packets will be dropped.	<ol style="list-style-type: none"> Click New. Configure the map. <ol style="list-style-type: none"> Type map22 in the Alias field. Select Second Level for Type. Select By Rule for Subtype. Select the virtual port vp1 for the Source. Select the tool port 1/1/x6 for the Destination. Select gsgroup1 from the GSOP list. Add a rule. <ol style="list-style-type: none"> Click Add a Rule. Select Drop. Select Pattern Match. Select regex and enter youtubelytimg yt3.ggpht tubeMogul tmogul. Set the offset from 0 to 1460 Set Protocol to tcp and set Position to 1. Click Save.

Example 3: Buffer ASF, Drop Windows Update Traffic

In Example 3, the goal is to drop all Windows update traffic. The Windows update traffic is expected to be identified on the HTTP request packet of a session. A maximum of 2 million sessions is specified.

Task	Description	UI Steps
1	Configure a GigaSMART group and associate it with GigaSMART engine ports and define the maximum number of sessions, in millions.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Groups > GigaSMART Groups. 2. Click New. 3. Type gsgrp1 in the Alias field. 4. Select two engine ports from the Port List field. For example, 1/3/e1 and 1/3/e2 5. Under Params Resource Buffer, select ASF and set the Buffer Size to 2. 6. Click Save.
2	If needed, reload the GigaSMART line card or module to allocate the resources for buffer ASF.	<p>If you reset the buffer size of an ASF profile in Task 1, go to the Chassis page and select Table View. Under Cards, select the card to reload. From the Actions menu select Shut Down and then Start Up.</p> <p>You can also issue the following CLI commands to reboot the card (the card is in slot 3 in this example):</p> <p>(config) # card slot 3 down (config) # no card slot 3 down</p>
3	Create a flow session, specify the buffer count before the match, and enable buffering. Note: The default protocol is TCP, so it does not need to be specified.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > ASF. 2. Click New or select an existing ASF profile then click Edit. 3. Type asf2 in the Alias field if this is a new ASF profile. 4. Enable Buffer. 5. Set Buffer Count before Match to 3. 6. Set the session field to ipv4-5tuple outer 7. Click Save.
4	Configure the combined GigaSMART operation.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Operations (GSOP) > GigaSMART Operations and create two GigaSMART Operations. 2. Click New. 3. Type gsop1 in the Alias field. 4. Select gsgrp1 from the GigaSMART Groups list. 5. Select the operations. <ul style="list-style-type: none"> o Adaptive Packet Filtering o ASF with asf2 for the ASF profile 6. Click Save.

Task	Description	UI Steps
5	Create a virtual port and associate it with the GigaSMART group.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > Virtual Ports. 2. Click New. 3. Enter vp1 in the Alias field. 4. Select gsggrp1 from the GigaSMART Groups list. 5. Click Save.
6	Create a first level map.	<ol style="list-style-type: none"> 1. Select Maps > Maps > Maps. 2. Click New. 3. Configure the map. <ol style="list-style-type: none"> a. Type map11 in the Alias field. b. Select First Level for Type. c. Select By Rule for Subtype. d. Select the network port 1/1/x1 for the Source. e. Select the virtual port vp1 for the Destination. 6. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Pass. c. Select IPv4 Version and set Version to v4. 4. Click Save.
7	Create a second level map. The gsrule specifies the traffic to drop. Buffered packets and all subsequent packets will be dropped.	<ol style="list-style-type: none"> 1. Click New. 2. Configure the map. <ol style="list-style-type: none"> a. Type map22 in the Alias field. b. Select Second Level for Type. c. Select By Rule for Subtype. d. Select the virtual port vp1 for the Source. e. Select the tool port 1/1/x6 for the Destination. f. Select gsop1 form the GSOP list. 7. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Drop. c. Select Pattern Match. d. Select regex and enter msdownload/update/software. e. Set the offset from 0 to 1460 f. Set Protocol to tcp and set Position to 1. 7. Click Save.

Example 4: Buffer ASF, Forward VNC Traffic

In Example 4, the goal is to forward VNC traffic from network port 1/1/x1 to tool port 1/1/x6. All packets belonging to the TCP connection need to be sent to the tool port. The first data packet after the TCP handshake is expected to contain the VNC pattern match. A

maximum of 2 million sessions is specified.

Task	Description	UI Steps
1	Configure a GigaSMART group and associate it with GigaSMART engine ports and define the maximum number of sessions, in millions.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Groups > GigaSMART Groups. 2. Click New. 3. Type gsgroup1 in the Alias field. 4. Select two engine ports from the Port List field. For example, 1/3/e1 and 1/3/e2 5. Under Params Resource Buffer, select ASF and set the Buffer Size to 2. 6. Click Save.
2	If needed, reload the GigaSMART line card or module to allocate the resources for buffer ASF.	<p>If you reset the buffer size of an ASF profile in Task 1, go to the Chassis page and select Table View. Under Cards, select the card to reload. From the Actions menu select Shut Down and then Start Up.</p> <p>You can also issue the following CLI commands to reboot the card (the card is in slot 3 in this example):</p> <p>(config) # card slot 3 down (config) # no card slot 3 down</p>
3	Create a flow session, specify the buffer count before the match, and enable buffering. Note: The default protocol is TCP, so it does not need to be specified.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > Application Session Filtering. 2. Click New or select an existing ASF profile then click Edit. 3. Type asf1 in the Alias field if this is a new ASF profile. 4. Enable Buffer. 5. Set Buffer Count before Match to 3. 6. Set the session field to ipv4-5tuple outer 7. Click Save.
4	Configure the combined GigaSMART operation.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Operations (GSOP) > GigaSMART Operation and create two GigaSMART Operations. 2. Click New. 3. Type gsop1 in the Alias field. 4. Select gsgroup1 from the GigaSMART Groups list. 5. Select the operations. <ul style="list-style-type: none"> o Adaptive Packet Filtering o ASF with asf1 for the ASF profile 6. Click Save.

Task	Description	UI Steps
5	Create a virtual port and associate it with the GigaSMART group.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > Virtual Ports. 2. Click New. 3. Enter vp1 in the Alias field. 4. Select gsgroup1 from the GigaSMART Groups list. 5. Click Save.
6	Create a first level map.	<ol style="list-style-type: none"> 1. Select Maps > Maps > Maps. 2. Click New. 3. Configure the map. <ol style="list-style-type: none"> a. Type map11 in the Alias field. b. Select First Level for Type. c. Select By Rule for Subtype. d. Select the network port 1/1/x1 for the Source. e. Select the virtual port vp1 for the Destination. 6. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Pass. c. Select IPv4 Version and set Version to v4. 4. Click Save.
7	Create a second level map. The gsrule specifies the traffic to pass. Buffered packets and all subsequent packets will be passed.	<ol style="list-style-type: none"> 1. Click New. 2. Configure the map. <ol style="list-style-type: none"> a. Type map22 in the Alias field. b. Select Second Level for Type. c. Select By Rule for Subtype. d. Select the virtual port vp1 for the Source. e. Select the tool port 1/1/x6 for the Destination. f. Select gsop1 from the GigaSMART Operations (GSOP) list. 7. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Pass. c. Select Pattern Match. d. Select regex and enter ^rfb 00[1-9]\.00[0-9]\x0a\$. e. Set Protocol to tcp and set Position to 1. 6. Click Save.

Example 5: Buffer ASF, Forward HTTPS Traffic on Non-Standard Port

In Example 5, the goal is to forward HTTPS traffic that uses a non-standard Layer 4 port. All packets belonging to the TCP connection need to be sent to the tool port. A maximum of 5 million sessions is specified.

Task	Description	UI Steps
1	Configure a GigaSMART group and associate it with GigaSMART engine ports and define the maximum number of sessions, in millions.	<ol style="list-style-type: none"> 1. GigaSMART > GigaSMART Groups > GigaSMART Groups. 2. Click New. 3. Type gsggrp1 in the Alias field. 4. Select two engine ports from the Port List field. For example, 1/3/e1 and 1/3/e2 5. Under Params Resource Buffer, select ASF and set the Buffer Size to 2. 6. Click Save.
2	If needed, reload the GigaSMART line card or module to allocate the resources for buffer ASF.	<p>If you reset the buffer size of an ASF profile in Task 1, go to the Chassis page and select Table View. Select the card in the table. From the Actions menu select Shut Down and then Start Up.</p> <p>You can also issue the following commands to reboot the card (the card is in slot 3 in this example):</p> <p>(config) # card slot 3 down (config) # no card slot 3 down</p>
3	<p>Create a flow session, specify the buffer count before the match, and enable buffering.</p> <div> <p>NOTE: The default protocol is TCP, so it does not need to be specified.</p> </div>	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > ASF. 2. Click New or select an existing ASF profile then click Edit. 3. Type asf2 in the Alias field if this is a new ASF profile. 4. Enable Buffer. 5. Set Buffer Count before Match to 3. 6. Set the session field to ipv4-5tuple outer 7. Click Save.
4	Configure the combined GigaSMART operation.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > GigaSMART Operations (GSOP) > GigaSMART Operations and create two GigaSMART Operations. 2. Click New. 3. Type gsop1 in the Alias field. 4. Select gsggrp1 from the GigaSMART Groups list. 5. Select the operations. <ul style="list-style-type: none"> o APF o ASF with asf2 for the ASF profile 6. Click Save.

Task	Description	UI Steps
5	Create a virtual port and associate it with the GigaSMART group.	<ol style="list-style-type: none"> 1. From the device view, select GigaSMART > Virtual Ports. 2. Click New. 3. Enter vp1 in the Alias field. 4. Select gsgroup1 from the GigaSMART Groups list. 5. Click Save.
6	Create a first level map.	<ol style="list-style-type: none"> 1. Select Maps > Maps > Maps. 2. Click New. 3. Configure the map. <ol style="list-style-type: none"> a. Type map11 in the Alias field. b. Select First Level for Type. c. Select By Rule for Subtype. d. Select the network port 1/1/x1 for the Source. e. Select the virtual port vp1 for the Destination. 6. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Pass. c. Select IPv4 Version and set Version to v4. 4. Click Save.
7	Create a second level map. The gsrule specifies the traffic to pass. The RegEx expression identifies the traffic as SSL. Buffered packets and all subsequent packets will be passed.	<ol style="list-style-type: none"> 1. Click New. 2. Configure the map. <ol style="list-style-type: none"> a. Type map22 in the Alias field. b. Select Second Level for Type. c. Select By Rule for Subtype. d. Select the virtual port vp1 for the Source. e. Select the tool port 1/1/x6 for the Destination. f. Select gsop1 from the GSOP list. 7. Add a rule. <ol style="list-style-type: none"> a. Click Add a Rule. b. Select Pass. c. Select Pattern Match. d. Select regex and enter x16\x03.{3}\x01. e. Set Protocol to tcp and set Position to 1. 6. Click Save.

Display ASF Statistics

To display ASF statistics on the GigaSMART operation, select **GigaSMART > Statistics**.

Refer to [ASF Statistics Definitions](#) for descriptions of these statistics as well as to [GigaSMART Operations Statistics Definitions](#).

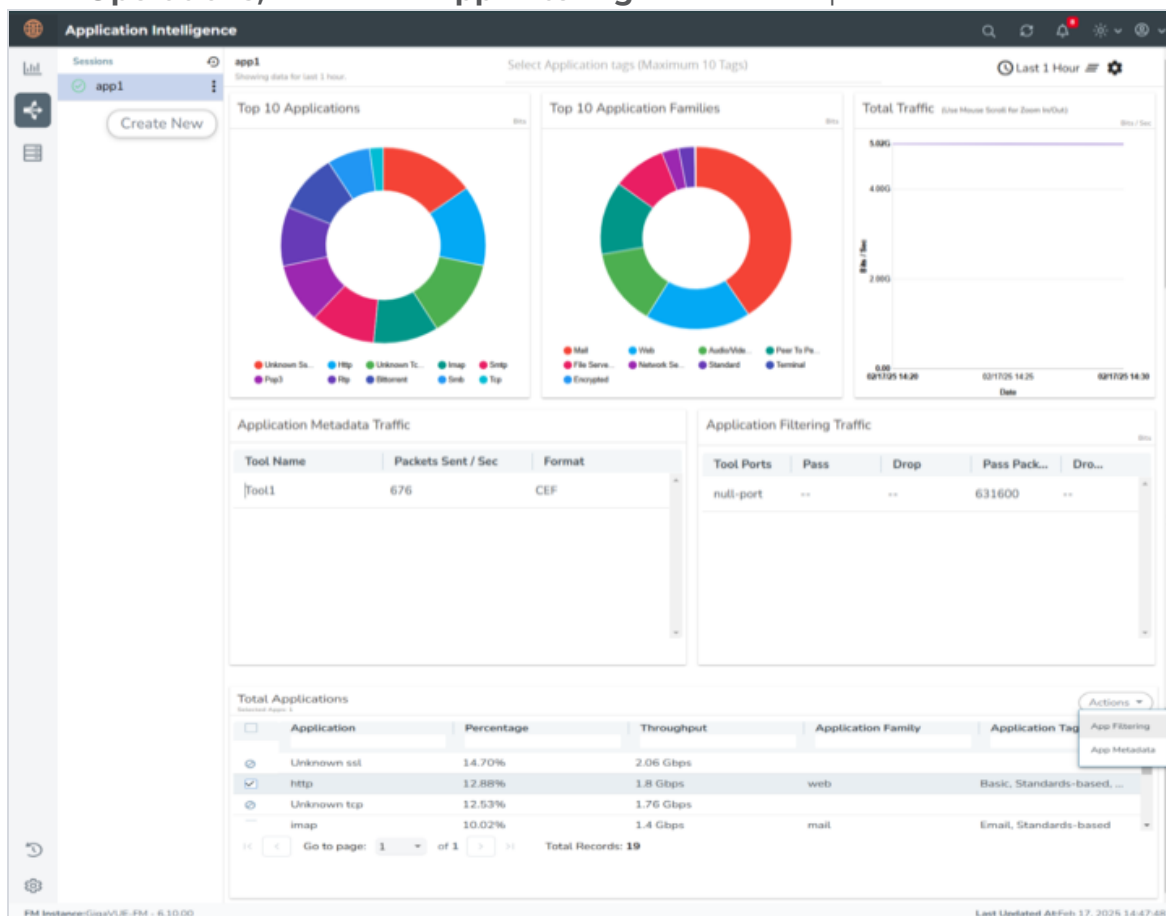
Create Application Filtering Intelligence for Physical Environment

GigaVUE-FM allows you to create Application Filtering Intelligence by selecting the applications available from the **Total Applications** displayed on the Application Intelligence (AFI) dashboard. To create Application Filtering Intelligence, follow these steps:

1. On the left navigation pane, go to **Traffic**  **> Solutions>App Intelligence**.

NOTE: If you are creating Application Filtering Intelligence immediately after creating Application Monitoring, then you can proceed from Step 2.

2. Select the required application from the **Total Applications** in the right pane of the Application Intelligence dashboard. You can also select multiple applications for creating the Application Filtering Intelligence.
3. Click **Operations**, and select **App Filtering** from the drop-down list.




You can view the list of applications selected in the **Selected Applications** section.

4. Select either the **Pass** or **Drop** check box for an application to allow it to either pass through or get dropped off in the tool port present in the **Destination Traffic Priority**. You can also perform a search operation to filter the required application from the list of applications.
5. Use the **Destination Traffic Priority** section, to either choose the available tool port or add a new port for creating a traffic priority. In the **Select ports...** field, select the tool ports for sending the filtered applications traffic to the external tool. If you are unable to view the required port in the **Port** field, perform these steps:
 - o Click **Port Editor**. Select the **Type** as **Tool** from the drop-down list for the required **Port Id**. Select **OK**.
The selected Port appears in the list.
 - o Click **Save**.
6. In the **Priority** section, you can perform the following actions:
 - o Enable the **Pass All** check box to pass all the applications when there are no matching rules.
 - o Click **Advanced Rules > Add a rule** to add new rules to perform advanced filtering on the application. For more details on adding a rule, refer to [Adding Rules](#) section.

NOTE: To view the statistics of packets that are sent due to no rule match pass, view the Map Rule Counters. Refer [Review Map Statistics with Map Rule Counters](#).

7. In the **Destination Traffic Priority** section, click **+Add New** to create additional **Destination Traffic Priority** (second level maps). In Application Filtering Intelligence, you can create a maximum of five Destination Traffic Priorities.

NOTE: You can click and drag the icon  to reorder the map priority when there are multiple priorities.

8. Click **Filter to** button for the corresponding **Priority** in a **Destination Traffic Priority** section for passing and dropping the applications to the required tool ports.

NOTE: You cannot filter the traffic using applications when you select pattern match in the rules configuration.

In the **Application Filtering Intelligence Settings**, you can edit the following options while creating the Application Filtering Intelligence:

Field	Mandatory	Default	Notes
Bidirectional	No	Enabled	Configures the direction of traffic to be filtered.
Timeout	Yes	15s	Range: 10-120s

Field	Mandatory	Default	Notes
			Configures the timeout interval for flushing the flows that remain silent.
Buffer	No	20	<p>Range: 3-20</p> <p>The DPI engine identifies applications based on the first few packets. This setting allows AFI to buffer the packets before applying the filtering rules.</p> <p>Decreasing the buffer size can result in premature packet drops. It's not recommended to change the setting. Please seek an expert's advice from Gigamon if you want to change it.</p>
Protocol	Yes	TCP-UDP	<p>Options: TCP only, UDP only, TCP-UDP, TCP UDP and SCTP, SCTP only.</p> <p>Application Intelligence maintains sessions based on the 5tuples. This option determines the protocol type for maintaining the sessions. The traffic that does not match the protocol type will be dropped. You can configure first-level shared collector map to monitor the traffic as needed.</p>
Packet Count	No	Disabled	<p>Range: 20-100 Configures the no. of packets to be passed per flow. This option can help to monitor the first few packets as in, for example, TLS handshake.</p>
Session Fields	Yes	5tuple	<p>Configures the protocol fields to be used for uniquely identifying flows. By default, inner header fields (Source and Destination IP address, Source and Destination Port Numbers, and Protocol) are used for identifying flows.</p> <p>(Optional) VLAN can be included along with the 5tuples.</p>

9. Click **Save**.

You can view the **Application Filtering Intelligence** Statistics from the Application Intelligence Dashboard page.

Adding Rules

You can use **Advanced Rules** option to add more rules in Application Filtering. To add rules, do the following:

1. Go to **Priority>Advanced Rules >Add a Rule**
2. Click the field **Select Options** in **Rule 1**. and select any of the following options:
 - DSCP
 - ERSPAN ID
 - EtherType
 - GRE Key
 - GTP-U TEID
 - IP Fragmentation

- IP Version
 - IPv4 Destination
 - IPv4 Source
 - IPv4 protocol
 - IPv4 TOS
 - IPv4 TTL
 - IPv6 Destination
 - IPv6 Flow Label
 - IPv6 Next Header
 - IPv6 Source
 - MAC Source
 - MAC Destination
 - MPLS Label
 - Pattern Match — You can select the pattern type as either as follows and provide the respective values.
 - **String**
 - **Regex**- For example, you can use it if you want to filter HTTP sessions that include JSON and API traffic.
 - Port Destination
 - Port Source
 - TCP Control
 - VLAN
 - VN-Tag Destination VIF ID
 - VN-Tag Source VIF ID
 - VN-Tag VIF List ID
 - VXLAN ID
3. Click **Pass** or **Drop** check box to allow it to either pass through or get dropped off in the tool port present in the **DestinationTrafficPriority**.
 4. Click **Save**.

Application Filtering Intelligence can also be configured for virtual environment, refer to Application Filtering Intelligence section in *GigaVUE V Series Applications Guide* for more detailed information.

Handle Large Flows in Application Filtering Intelligence


Application Filtering Intelligence detects and handles the large flows in the traffic. This feature helps to optimize the performance of the following GigaSMART cards when large flows are present in the traffic:

- HC1-X12G4

- SMT-HC3-C05

In tunneled traffic, this feature detects the large flows , but it doesn't involve in optimizing the performance of the GigaSMART engine.

To detect the large flows (elephant flows) in the traffic, do the following in the GigaVUE-FM:

1. On the left navigation pane, go to  , go to **Physical > Nodes**.
2. Click on the required Cluster ID.
3. From the device view, go to **System > GigaSMART > GigaSMART Groups**.
4. Click **New** to create a new GigaSMART Group for detecting the traffic with elephant flow.
 - a. Enter the name of the group in the **Alias** field.
 - b. Select the ports in the **Port List**.

You can also include the detection of elephant flow in a existing GigaSMART group.

5. In the **GigaSMART Parameters > Eflow** section, enable the **Eflow** checkbox to enable the detection of elephant flow.
6. Enable the **Log** check box to print the parameters of the large flows (elephant flows) including the 5-tuple information into the GigaSMART logs.

NOTE: It is recommended to disable the check box after collecting the required parameters.

7. Enter the following parameters to identify the large flows :
 - a. **Interval** — The interval within which packet-count and packet-ratio for a traffic flow are examined. The interval should be specified in seconds. The range lies between 0 to 3600. Specify the interval as 0 to ignore this parameter. The default value is **2 secs**.
 - b. **Packet Count**— Enter the maximum number of packets to be received by the flow within the given interval to categorize the flow as an elephant flow. The default value is **10,000**.
 - c. **Packet Ratio** — Enter the packet ratio, which is the percentage concentration of the packets in the flow to the packets seen overall by the gsgroup. Specify 0 to ignore this parameter. The default value is **0**.
8. You can modify the Resource Buffer settings to scale the internal packet buffers in the GigaSMART engine, which helps reduce ingress drops caused by large flows From the device view, go to **System > GigaSMART > GigaSMART Groups> GigaSMART Parameters > Resource Buffer** section, select the **Enable Resource Buffer Packet**

check box and provide packet buffer scale in the **Resource Packet Buffer scale** field from 1-2 scale. The default value is 1. By default for scale 1, the default buffers are allocated for each platform.

NOTE: A packet buffer scale of 2 is only applicable to the GigaVUE-HC3 Gen 2 device. When set to 2, twice the number of buffers are allocated. Make sure to reboot the card after applying any configurations.

Refer to [gsgroup](#) command in GigaVUE-OS CLI Reference Guide to configure through GigaVUE-OS CLI

You can handle the large flows in Application Filtering Intelligence Solution by using the *gsgroup* created to detect the flow.

Refer to the *GigaVUE-OS CLI Reference Guide* to learn about the commands that must be configured to detect and handle the large flow of traffic.

Configure Application Filtering Intelligence with Slicing and Masking

Application Filtering Intelligence (AFI) with Slicing and Masking is an advanced virtual solution designed to optimize network traffic management. By allowing users to filter, slice, and mask traffic based on specific applications or application families, this tool enhances the efficiency and security of data flow.

To configure AFI with slicing follow the below steps:

1. Create **GigaSMART group** for GigaSMART Engine.
2. Enable **Application Session Filtering**.
3. Set the **Buffer Size** to 2.
4. Create **GigaSMART Operation**.
5. Select **GigaSMART Group**.
6. Select **ASF**, **APF** and **Slicing** for **GigaSMART Operations (GSOP)**.
7. For Slicing, select protocol and desired offset.
8. Create **Application Session Filtering** profile from GigaVUE-FM using the following steps:
 - a. Click **GigaSMART**.
 - b. Click **App Identification**.
 - c. Click **Application Session Filtering**.
 - d. Enable **Bidirectional**

- e. Enable **Buffer**.
 - f. Set the **Buffer Count Before Match** to 20.
 - g. Select **TCP-UDP** for **PROTOCOL**.
 - h. Select **5tuple** for **Session Fields**.
9. Create **New Virtual Port**.
10. Select the GigaSMART groups and **ASF Profile** created in the previous steps.
11. Create **First Level** Map using the following steps:
- a. Click **Traffic**.
 - b. Click **Maps**.
 - c. Click **New**.
 - d. Select **Type** as **First Level**.
 - e. Select **Source** as Network Ports and **Destination** as Vport.
12. Create **Second Level** Map using the following steps:
- a. Click **Traffic**.
 - b. Click **Maps**.
 - c. Click **New**.
 - d. Select **Type** as **Second Level**.
 - e. Select **Source** as **Vport** and To Port as **Tool Port**
13. Attach the GSOP.
14. Create the Application profile using the following steps:
- a. Click Create New Application Profile drop down in the PASS/DROP application profile option.
 - b. Search and select applications for Pass/Drop.
15. **Save** the map. The solution is deployed

To verify the configuration , you can utilize the following commands:

- o show map stats
- o show vport stats
- o show gsop stats
- o show gsgroup stats and port stats of Source port, GS engine and Tool port

NOTE: The same procedure can be used for Masking and Advanced Flow Slicing GSOPs by selecting Masking or Advanced Flow Slicing instead of Slicing in the 6th step.

Application Metadata Intelligence

Application Metadata Intelligence can export up to 6000 attributes for over 4000 applications without impacting the users, devices, applications, or the network appliances. The feature identifies applications even when the traffic is encrypted.

NOTE: The DPI attributes of certain applications will be extracted and exported only if the traffic is decrypted. Please refer to the list of such applications under "Decrypted Traffic Support" in the GigaVUE-FM Application Protobook.

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.

NOTE: Work with your Gigamon representative to get the latest IPFIX elements.

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

Application Metadata Intelligence Capabilities

NetFlow/IPFIX Generation

AMI supports generating only unsampled (i.e., 1:1) NetFlow/IPFIX records. Records can be generated in the following formats: NetFlow v5/v9, IPFIX, or CEF. Only standard information elements can be exported (i.e., no application metadata).

Users can select the NetFlow v5 tool template for exporting NetFlow v5 records or configure the collect fields for exporting NetFlow v9 and IPFIX records.

Flow Behavior

The flow behavior determines the number of records generated for each direction of the (monitored) traffic flows. Exporters can be configured with either Unidirectional or Bidirectional Flow Behavior. Unidirectional Flow Behavior exports one record for each direction, whereas Bidirectional Flow Behavior exports one record for both directions. The Flow Behavior is user configurable under Application metadata Settings. The following table lists the export formats supported for each flow behavior.

More than one exporter (max 5) can be configured to export records to multiple tools. When more than one exporter exists, all the exporters must support the same Flow Behavior.

Export Formats*	Unidirectional Flow Behavior	Bidirectional Flow Behavior
NetFlow v5/v9	Supported	Not Supported
IPFIX	Supported	Supported
CEF	Supported	Supported

*Application metadata can be exported in IPFIX or CEF format and it supports only bidirectional flow behavior.

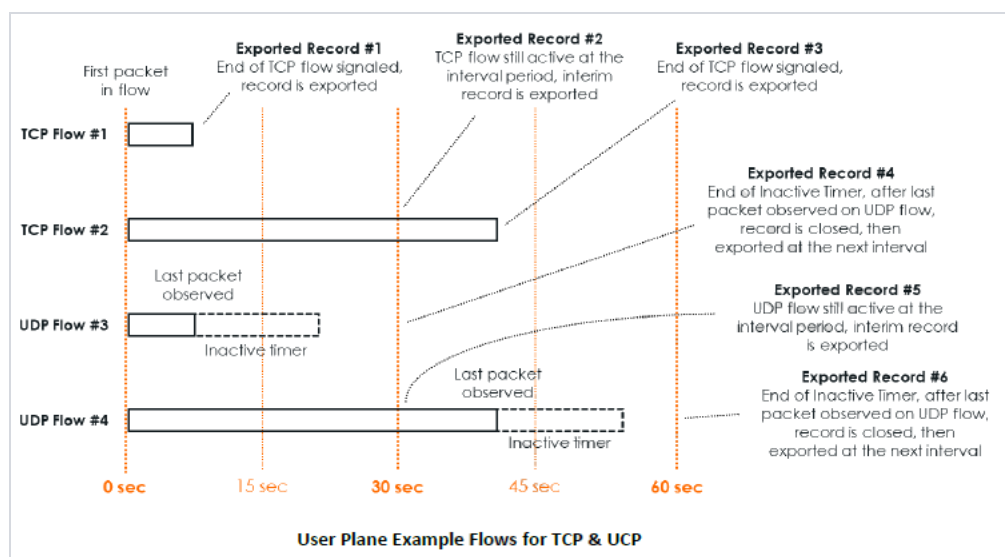
Record Types

AMI can generate separate records (Segregated) for network and application metadata. Tools that rely on flow correlation will prefer to receive network and application metadata in a single record. In which case, AMI can be configured to generate consolidated (Cohesive) records for each flow.

Records Export

AMI keeps track of all sessions using the 5-tuple information, including flows exchanged over reliable transport protocols like TCP and connectionless transport protocols like UDP. Records are exported based on the Active Timeout and Inactive Timeout, with the following exceptions:

- For connection-oriented applications (ex., TCP-based applications), records are exported as soon as the corresponding connections are closed.
- For connectionless applications (ex., UDP-based applications), the corresponding flows are determined to be completed after the expiration of the inactive timeout. The default value for the inactive timeout is 15 seconds (user configurable). Records for the corresponding flows are exported thereafter.



In the diagram above, there are 4 flows, but 6 records are generated. Two flows (#2 & #4) lasted longer than the configured Active Timeout (30 seconds). Therefore, interim records were generated at every 30 seconds. If the flows had lasted longer than 60 seconds, additional interim records would have been generated at 90 seconds, 120 seconds, and so on.

Tool Templates

Tool template in Application Metadata Intelligence predefines a list of applications and its attributes, which you can choose as per your requirements while configuring Application Metadata Intelligence solution.

A template once created can be used by multiple exporters to export the attributes in the specified format to the destination tools.

You can use the tool templates while creating an Application Metadata Intelligence session. By default, you can find the following tool templates:

- BroMetadata Template
- Netflow V5 Template
- SplunkMetadata Template

Starting from software version 6.2.00, the following tool templates are supported:

- SecurityPosture
- RogueActivity
- SuspiciousActivities
- AnomalousTraffic
- Troubleshooting
- M2131Logging

- UnmanagedAssets

The following table provides the purpose of each of the tool templates when used in Application Metadata Intelligence :

Tool Template	Purpose
BroMetadata Template	For selecting applications and attributes that can be detected by Bro sensor
Netflow V5 Template	For emulating NetFlow V5 behavior
SplunkMetadata Template	For providing a quick insight into the network traffic generated by various applications and protocols
SecurityPosture	For detecting flaws in securing the applications in the network
RogueActivity	For detecting unsanctioned applications that can pose challenges to network security
SuspiciousActivities	For detecting issues related to unmanaged devices, suspicious connections, and traffic outside normal limits in the network
AnomalousTraffic	For detecting challenges with HTTP, HTTPS, and DNS traffic in the network
Troubleshooting	For detecting latency, connectivity, and protocol errors in the network
M2131Logging	For U.S. Office of Management and Budget M-21-31 logging requirements
UnmanagedAssets	For providing visibility into unmanaged hosts and devices in the network

NOTE: You cannot edit the above templates. Hover over the Description column to view the description of the default tool templates.

You can create new tool templates according to your requirements. You can also edit and clone the templates. Refer to [Application Metadata Intelligence Capabilities](#) for more information.

DPI Packet limit

DPI Packet Limit 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 to improve the AMI performance.

Aggregate Round-trip Time

Aggregate Round-trip Time allows to export the minimum, maximum, and mean of RTT values , and also the aggregate of TCP Lost byte values collected per export time interval.

RTT Attribute in AMI

The RTT attribute supported in AMI export is in the struct timeval format. The size of the attribute is 16 bytes. The RTT attribute when exported in IPFIX format the first 8 bytes represent the value in seconds and the next 8 bytes represent the value in microseconds.

The values are exported in the network byte order.

In the following example:

- The PEN id 3365 has a RTT value of 0 seconds and 0x05d9 microseconds
- The PEN id 3384 has a RTT value of 0 seconds and 0x3131 microseconds

Flow 1

```
Enterprise Private entry: (Gigamon Systems LLC) Type 3365: Value (hex bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05 d9
Enterprise Private entry: (Gigamon Systems LLC) Type 3384: Value (hex bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 31 31
Enterprise Private entry: (Gigamon Systems LLC) Type 3385: Value (hex bytes): 00 00 00 00
Enterprise Private entry: (Gigamon Systems LLC) Type 3397: Value (hex bytes): 00 00 00 00
Classification Engine ID: PANA-L7-PEN (20)
```

The RTT attribute when exported in CEF format will be converted in seconds like shown below

CEF:

```
Wed Mar 20 14:19:14 2024 SOL-HC3-SP CEF:0|Gigamon|metadata|6.6.00|4|metadata
generation|6|GigamonMdata_tcp_rtt=0.001497 GigamonMdata_tcp_rtt_app=0.012593
GigamonApplicationID=68 GigamonMdataTcpFlags=19 src=192.168.12.5
dst=192.168.12.14 proto=6 spt=39408 dpt=443 GigamonInitiatorOctets=2046
GigamonResponderOctets=5020 GigamonInitiatorPackets=20
GigamonResponderPackets=20 GigamonApplicationName=https
GigamonFlowID=5677081841385865217 GigamonMdataSeqNum=0
```

Import and Export Tool Templates

You can export and import tool templates. The following are the advantages of exporting and importing tool templates:

- Retrieve a tool template that was deleted unintentionally.
- Deploy the template in another device.
- Re-deploy the template in the device after GigaVUE-FM, GigaVUE HC Series is upgraded to a new version (in case of issues in the existing solution).

To export a tool template:

1. In the Tool Templates page, select a template that must be exported.
2. Click the ellipsis and select **Export**.
3. Save the file to the required location.

To import a tool template:

1. Click **Import**.
2. Select the required file from the local folder.
3. Click **Deploy** to deploy the template.

Create Custom Tool Templates

To create a customized Tool Template, do the following:




1. On the left navigation pane, Go to **Resources > Tool Templates**.
You can view two system defined templates by default.
2. Click **Create**. The **New Tool Template** page appears.
 - a. Enter the **Template Name**.
 - b. Select the **GS Version**.
 - c. Enable the **Application Family** or **Application Tag** option. Only if you choose the **GS Version** as **1.680.0.24**, the **Application Family** and **Application Tag** options appear.
 - d. Enable the **fastmode** check box. When the **fastmode** option is enabled, only the **fastmode** supported attributes will be listed. Only if you choose the **GS Version** as **1.680.0-20** or **1.680.0.24**, the **fastmode** option appears.
 - e. Enter the **Description**.
3. Click the **App Editor** button. The **App Editor** page appears.
4. Click the **Application Family** field and select an Application Family such as antivirus, webmail that needs to be filtered from the traffic. You can also select multiple application families.
5. If you choose to add or delete all the applications in a family, click **Add All Application in Families** or **Delete All Application in Families**.

NOTE: You can select the required applications without selecting the application family.

6. Click the **Application Tags** field and select an **Application Tags** that needs to be filtered from the traffic. You can also select multiple application tags. If you choose to add or delete all the applications in **Application Tags**, click **Add All Application in Tags** or **Delete All application in Tags**.
7. Select the format (CEF/NetFlow) in which the application details need to be exported to the tool.
8. Select the record or 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.
9. Enter the **Active timeout** and **Inactive timeout** in seconds.

NOTE: Select the Version and the Template Refresh Interval for the Netflow format.

10. In the **AdvancedSettings > Collects** section, you can view and configure the following collect types:

- **Counter** - Select the Bytes and Packets.
- **IPv4** - Select and enter the required information in the fields such as Source Address, Destination Address, Fragmentation, and Header Size and Payload Size.
- **IPv6** - Select and enter the required information in the fields such as Source Address, Destination Address, Fragmentation, and Header Size and Payload Size.
- **Transport** - Select and enter the required information in the fields such as Source Address, Destination Address, and Header Size, Payload Size, MSS, Aggregate Window Size, Zero Window etc. Refer to [Attributes for GigaVUE Enriched Metadata for Mobile Networks](#).
- By default, the above collect types are displayed. Click  to add the following collect types:
 - **Data Link** - Select any one of the parameters such as Source Mac, Destination Mac and VLAN.
 - **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.
 - **Interface** - These options are supported only in standalone deployments (GigaVUE-HC1, GigaVUE-HC3, GigaVUE-HCT, and GigaVUE-HC1P) and legacy cluster deployments. Select any one of the following parameters:
 - **Input Physical** - Select the **Input Physical** checkbox to export the ingress interface as one of the fields sent in the NetFlow record. It also allows exporting the interface index in the NetFlow record. Under Input Physical Width, choose 2 bytes or 4 bytes. A width of 4 bytes is recommended for both v9 and IPFIX protocols, while v5 supports only 2 bytes. CEF supports exporting the Input interface index with a width of 2B (default) or 4B.
 - **Output Physical** - Select the **Output Physical** checkbox to export the egress interface as one of the fields sent in the NetFlow record. It also allows exporting the interface index in the NetFlow record. Under Output Physical Width, choose 2 bytes or 4 bytes. A width of 4 bytes is recommended for both v9 and IPFIX protocols, while v5 supports only 2 bytes. CEF supports exporting the Output interface index with a width of 2B (default) or 4B.
 - **Input Name** - Select the **Input Name** checkbox to export the interface name. In the Input Name Width field, specify a value between 1 and 32 bytes. The default value is 16 bytes. The total character limit for the interface name is 128 characters. Refer [Create NetFlow Session for Physical Environment](#) to know more details on the Collects fields.

NOTE: When Input/Output Physical interface width is set to 2B, only the lower order bytes of the interface index are exported.

11. Click **Save**. The new tool template is added to the list view.
12. Select a tool template and click the ellipsis to perform the following:
 - **View Details** - To view the details in the template.
 - **Edit** - To edit the parameters and fields in the template.

- **Delete** - To delete the template from the list.
- **Duplicate** - To duplicate the template in the list.
- **Export** - To export a tool template.

NOTE: When a solution is **fastmode** enabled, you can only select the tool templates that has all the attributes supported in the **fastmode**. The other tool templates that are listed will be greyed out. Refer "Create an Application Intelligence Session" topic for information on **fastmode**.

NOTE: You can edit an existing template and the attributes associated with it as required, and save the updates as a new template while creating an Application Metadata Intelligence session. Refer to [Application Metadata Intelligence](#) for details.

Create Application Metadata Intelligence for Physical Environment

Create an Application Metadata Intelligence session in GigaVUE-FM by selecting the applications available from the Total Applications displayed on the Application Intelligence (AMI) dashboard.

To create an Application Metadata Intelligence session, follow these steps:

1. From the left navigation pane, go to **Traffic > Solutions > App Intelligence**.
2. In the **Application Intelligence Session**, click **Application Metadata**.

You must configure Application Intelligence session, to monitor the application on the network and to display them on the **Total Applications**. To create Application Intelligence session refer to [Application Intelligence Session](#).

3. From the navigation pane, click **App Intelligence**. Select the applications from the **Total Applications** in the right pane of the Application Intelligence dashboard.
4. Click **Operations** and select **App Metadata** from the drop-down list.

You can view the list of applications selected in the **Selected Applications** section.

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

5. Expand the application and select the attributes to be extracted.

NOTE: Each exporter can be assigned up to 8 application profiles, with each profile containing multiple attributes from various protocols. In total, an exporter can be configured to include attributes from a maximum of 32 applications, and for each application, up to 64 attributes can be configured. The total number of Exporters that can be configured are five.

NOTE: The attributes IP source and IP destination cannot be configured to be extracted from the **App Editor** section. To export, them utilize the **Advanced Settings > Collects** section. The total number multi-collects for both IPFIX and CEF are up to five.

6. In the **DestinationTraffic** section, you can attach five exporters to a GigaSMART group. You can only create a maximum of 5 exporters. Enter the following details:

Option	Mandatory	Default	Description
Tool Name	Yes		Configures the alias name for the tool.
IP Interface	Yes		Configures the IP interface on the Gigamon device that connects to the tool.
Tool IP Address	Yes		Configures the destination IP address for exporting the records.
Template	No		Configures pre-defined tool templates for exporting metadata. Tool templates are user configurable. Ex. SplunkMetadataTemplate, SecurityPostureTemplate etc.
L4 Source Port	Yes		Configures the Source Port of the IP interface on the Gigamon device.
L4 Destination Port	Yes		Configures the destination port on the tools side.
SNMP	No	Disabled	<p>Enables or disables the processing of SNMP packets on the exporter interface. When enabled, the interface will accept and forward SNMP packets (UDP port 161) to the system for processing.</p> <p>Note:</p> <p>1) Prior to enabling SNMP on a exporter, ensure it is enabled and configured globally. Refer to Use SNMP.</p> <p>2) If more than one exporter is configured using the same IP interface, all the exporters must have the SNMP configuration either enabled or disabled.</p> <p>3) SNMP packets can be monitored via IP interface RX and TX counters.</p>
Application ID	No	Disabled	<p>Configures exporting Application Name for all applications identified by the DPI engine.</p> <p>Note: Requires AMI/SVP/ZTA license.</p>
Application List	No		Each exporter can be customized to export metadata for certain applications/ protocols.
Format	Yes		<p>Options: NetFlow, CEF</p> <p>Configures the format for exporting the records.</p>
Version	Yes	IPFIX	Options: v5, v9 and IPFIX.

Option	Mandatory	Default	Description
			Configures the version of NetFlow for exporting the records.
Template Refresh Interval	Yes	60s	<p>Range: 1-216000s</p> <p>Configures the interval at which the template record is exported while exporting the IPFIX records. Changing the refresh interval can impact ingesting the records on the tools side. Please seek guidance from your tool's vendor before changing the default.</p>
Record Type	Yes	Cohesive/ Segregated	<p>Default depends on the Flow Behavior configuration.</p> <ul style="list-style-type: none"> • Segregated: Default when the Flow Behavior is set to Unidirectional. Separate records are exported for network and application metadata. • Cohesive: Default when the Flow Behavior is set to Bidirectional. Generates consolidated record comprising of network and application metadata. <p>If record size exceeds the IP interface MTU, the records will be exported as fragments.</p>
Active Timeout	Yes	60s	<p>Range: 1-604800s</p> <p>. This option configures the timeout interval for exporting interim records for such flows.</p> <p>Shorter timeouts increase the no. of records and longer timeouts result in fewer records. Longer timeouts can also increase the record size. Please seek expert guidance from Gigamon and tool vendor before changing the default.</p>
Inactive Timeout	Yes	15s	<p>Range: 1-604800s</p> <p>Configures the timeout interval for marking flows as inactive and exporting their records soon after.</p> <p>Inactive timeout constitutes idle time after receiving the last packet. Shorter timeouts can prematurely deem a flow as inactive and subsequent packets would be considered as a new flow that can skew the analytics on the tools side.</p> <p>Please seek expert guidance from Gigamon and tool vendor before changing the default.</p>


7. When editing the exporter template, if you change any of the non-editable fields (Format, Record Type, NetFlow Version), the solution fails.

NOTE: When you create a session with flow-behaviour as bi-directional, GigaVUE-FM allows you to select Netflow v5 and v9 templates. When you edit the same session, you cannot select the Netflow v5, and v9 templates.

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.

NOTE: The format and the record/template type get selected automatically, after selecting the Tool Template.

8. In the **Advanced Settings > Collects** section, you can select the following packet attributes:
 - **Counter** - Select the Bytes, and Packets.
 - **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.

By default, the above collect types are displayed. Click  to add the following collect types:

- **Data Link** - Select any one of the parameters such as Source Mac, Destination Mac and VLAN.
- **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.
- **Interface** - These options are supported only in standalone deployments (GigaVUE-HC1, GigaVUE-HC3, GigaVUE-HCT, and GigaVUE-HC1P) and legacy cluster deployments. Select any one of the following parameters.

NOTE: When Input/Output Physical interface width is set to 2B, only the lower order bytes of the interface index are exported.

- **Input Physical** - Select the **Input Physical** checkbox to export the ingress interface as one of the fields sent in the NetFlow record. It also allows exporting the interface index in the NetFlow record. Under Input Physical Width, choose 2 bytes or 4 bytes. A width of 4 bytes is recommended for both v9 and IPFIX protocols, while v5 supports only 2 bytes. CEF supports exporting the Input interface index with a width of 2B (default) or 4B.
- **Output Physical** - Select the **Output Physical** checkbox to export the egress interface as one of the fields sent in the NetFlow record. It also allows exporting the interface index in the NetFlow record. Under Output Physical Width, choose 2 bytes or 4 bytes. A width of 4 bytes is recommended for both v9 and IPFIX protocols, while v5 supports only 2 bytes. CEF supports exporting the Output interface index with a width of 2B (default) or 4B.
- **Input Name** - Select the **Input Name** checkbox to export the interface name. In the Input Name Width field, specify a value between 1 and 32 bytes. The default value is 16 bytes. The total character limit for the interface name is 128 characters.

Refer [Create NetFlow Session for Physical Environment](#) to know more details on the Collects fields.

9. In the **Application Metadata Settings** section:

O p t i o n	M a n d a t o r y	D e f a u l t	N e t F l o w	Description
Eve nts	Yes	Tra n s a c t i o n e n d	N/A	Options: None and Transaction End Transaction End allows exporting records of TCP traffic soon after the connections terminate. Else, the records will be exported after the Inactive Timeout
Flo w Dire	Yes		Sup por ted	Options: Unidirectional, Bidirectional. Enables record to be exported for each direction (Unidirection) of the traffic flow or a single record to be exported for

Option	Mandatory	Default	Net Flow	Description															
ction/ Behavior				both directions (Bidirection) of the traffic flow.															
Timeout	Yes	300s	Supported	Range: 1 to 604800s Configures the duration for which flows can be cached. Upon timeout, the flows are flushed. New flows are created as and when new packets are received.															
Cache Size	Yes	1: Gen 2 2: Gen 3	Supported	<div>Supported range:<table><tr><th>Platform</th><th>Gen2- Range in million</th><th>Gen3- Range in million</th></tr><tr><td>GigaVUE-HC1</td><td>1M</td><td>1M-2M</td></tr><tr><td>GigaVUE-HC3</td><td>1M-5M</td><td>1M-10M</td></tr><tr><td>GigaVUE-HC1-Plus</td><td>NA</td><td>Front: 1M-2M Rear: 1M-10M</td></tr><tr><td>GigaVUE-HCT</td><td>NA</td><td>1M-2M</td></tr></table></div> <div>Note: Starting from version 6.12, the maximum range is set as the default value for the AMI. To maintain backward compatibility, the system assigns the minimum range as the default value when the device is running on an older version.</div> <div>Note: If you upgrade your solution from 6.5 to any of the LTS versions your cache size will be shown lesser.</div> <div>This option is supported only on GigaVUE HC Series (refer to the No. of Flows for GigaVUE V Series). It configures the session table size for maintaining the max no. of concurrent flows. The default value is set to support all combinations of the apps i.e. AppViz+AFI+AMI+De-dup. It can be changed from GigaVUE-OS CLI under an expert's guidance.</div>	Platform	Gen2- Range in million	Gen3- Range in million	GigaVUE-HC1	1M	1M-2M	GigaVUE-HC3	1M-5M	1M-10M	GigaVUE-HC1-Plus	NA	Front: 1M-2M Rear: 1M-10M	GigaVUE-HCT	NA	1M-2M
Platform	Gen2- Range in million	Gen3- Range in million																	
GigaVUE-HC1	1M	1M-2M																	
GigaVUE-HC3	1M-5M	1M-10M																	
GigaVUE-HC1-Plus	NA	Front: 1M-2M Rear: 1M-10M																	
GigaVUE-HCT	NA	1M-2M																	
Multi-Collect	No	Disabled	N/A	<div>By default, only one value is exported per attribute. Some attributes can have multiple values. Ex. DNS host address. When multi- collect is allowed, it enables exporting more than one value per attribute.</div> <div>By default, multi-collect is supported for the following protocols, DNS, GTP and GTPV2.</div> <div>IPFIX can support up to 5 multi-collects per attribute. CEF has no such limit.</div>															

Option	Mandatory	Default	NetFlow	Description										
Data Link	No	Disabled	N/A	Can be enabled to export Source and Destination MAC and ingress VLAN ID. Note: When the Data link is enabled flows with identical 5-tuples but different VLAN IDs are treated as the same.										
Observation Domain ID	No	0	Supported	Range: 0-255 When multiple application intelligence sessions are configured, customers can assign different IDs for creating additional level of abstraction for analysis on the tools side. For example: If you enter 5 in this field, then the observation domain ID is calculated as follows: <table><tr><th colspan="2">Observation Domain ID (4-Bytes)</th></tr><tr><td>Byte 1</td><td>0</td></tr><tr><td>Byte 2</td><td>1</td></tr><tr><td>Byte 3</td><td>GS engine slot (for e.g. 2 if 1/2/e1)</td></tr><tr><td>Byte 4</td><td>User defined (for e.g. 5). Default : 0.</td></tr></table> The calculated value of Observation Domain Id in Hexadecimal is 00 01 02 05 , and in Decimal is 66053 .	Observation Domain ID (4-Bytes)		Byte 1	0	Byte 2	1	Byte 3	GS engine slot (for e.g. 2 if 1/2/e1)	Byte 4	User defined (for e.g. 5). Default : 0.
Observation Domain ID (4-Bytes)														
Byte 1	0													
Byte 2	1													
Byte 3	GS engine slot (for e.g. 2 if 1/2/e1)													
Byte 4	User defined (for e.g. 5). Default : 0.													

Option	Mandatory	Default	NetFlow	Description																				
DPI Packet limit	No	Disabled	N/A	The value must range between 20 - 50 as the first 20 to 50 packets contains the most significant attributes.																				
Aggregate Round-Trip Time	No	Disabled	N/A	<p>On GigaVUE HC Series, it's supported only in the Gen3 GS module.</p> <p>This option enables multi-collect for the following protocols, TCP, HTTP, SSH, TELNET, ICMP, ICMP6 and WSP.</p> <p>By default, RTT and TCP Loss bytes are exported only at the beginning of a flow. These attributes can change over the lifetime of a flow. Aggregate mode can be enabled to closely monitor the flows. When enabled, the attributes are exported at each export interval as follows for the duration of the flow.</p> <p>RTT: Exports minimum, Maximum, and Mean values for protocols such as TCP, HTTP, SSH, ICMP etc.</p> <p>TCP Loss Count: Exports the consecutive missing bytes per flow.</p> <table><thead><tr><th>Protocol Name</th><th>Attribute</th></tr></thead><tbody><tr><td>http</td><td>rtt</td></tr><tr><td>icmp</td><td>rtt</td></tr><tr><td>icmp6</td><td>rtt</td></tr><tr><td>ssh</td><td>rtt</td></tr><tr><td>tcp</td><td>rtt</td></tr><tr><td>tcp</td><td>rtt_app</td></tr><tr><td>telnet</td><td>rtt</td></tr><tr><td>wsp</td><td>connect_rtt</td></tr><tr><td>wsp</td><td>query_rtt</td></tr></tbody></table>	Protocol Name	Attribute	http	rtt	icmp	rtt	icmp6	rtt	ssh	rtt	tcp	rtt	tcp	rtt_app	telnet	rtt	wsp	connect_rtt	wsp	query_rtt
Protocol Name	Attribute																							
http	rtt																							
icmp	rtt																							
icmp6	rtt																							
ssh	rtt																							
tcp	rtt																							
tcp	rtt_app																							
telnet	rtt																							
wsp	connect_rtt																							
wsp	query_rtt																							

10. In the **SelectedApplications** section, select **Export** and click **Export To** for the applications that needs to be exported to the destination tool.
11. Click **Save**.

Enable De-duplication in Application Filtering Intelligence or Application Metadata Intelligence

Required License: De-duplication

Duplicate packets are common in network analysis environments where both the ingress and egress data paths are sent to a single output (for example, as a result of a SPAN operation on a switch). They can also appear when packets are gathered from multiple collection points along a path. GigaSMART de-duplication lets you eliminate these packets, only forwarding a packet once and thus reducing the processing load on your tools. For more information, refer to the [GigaSMART De-Duplication](#).

To enable De-duplication in the Application Filtering Intelligence or Application Metadata Intelligence, click **De-duplication**.

Requirements and guidelines:

- You must install licenses for De-duplication and Application Filtering Intelligence on your GigaSMART Modules to enable the features in GigaVUE-FM.
- Application Filtering Intelligence and De-duplication can be combined on the same GigaSMART engine.
- When combining Application Filtering Intelligence (AFI) and De-duplication, AFI has the higher priority and it is executed before De-duplication.

Create NetFlow Session for Physical Environment

Note: This configuration is applicable only when using NetFlow License.

1. On the left navigation pane, select **Traffic > Solutions > Application Intelligence**.
2. Click **Create New**. The **Create Application Intelligence Session** page appears.

NOTE: If the Create button is disabled, check whether a valid license for Application Metadata Intelligence or Application Filtering Intelligence is available.

3. In the **Basic Info** section complete the following:
 - Enter the name and description (optional).
 - Select **Physical** in the Environment field.
 - Select the node from the list of nodes.
 4. In the **Configurations** section, view the following:
 - a. Select a GigaSMART Group. You can also choose to create a new GigaSMART Group.
 - Provide a name in the **Alias** field.
 - Select a port or multiple ports from the **Port List**.
 - Click **Save**.
 5. If you are unable to view the required port in the **Port** field, perform these steps:
 - Click **Port Editor**. Select the **Type** as **Tool** from the drop-down list for the required **Port Id**. Select **OK**.

The selected Port appears in the list.
 - Select the **Type** as:
 - IPv4 - to allow the traffic in IPv4 interface.
 - IPv6 - to allow the traffic in IPv6 interface.
 - Provide the **IP Address, IP Mask, Gateway**, and **MTU**. Provide the IP address corresponding to the IP interface selected.
 - Click **Save**.
 6. In the **Source Traffic** section, select a source port that require application monitoring in the **Source ports** field. Source port can be a single port, multiple ports, and port groups.
- NOTE:** Ports already used as source ports in the intent-based orchestrated solution will not be listed in the drop-down.
7. Configure the rules for filtering the required traffic in the **L2-L4 Rules** fields. To configure a rule:
 - a. Click **Select Conditions**. Select the required parameters from the drop-down list.

- b. Select the value for the parameters from the drop-down.
- c. Select the required options:
 - Pass or Drop - Based on the parameter selected in the Conditions fields, the traffic that matches the conditions will either be passed or dropped.
 - Bidirectional - Allows the traffic in both directions of the flow.

NOTE: Click “+” to create multiple rules for filtering the required traffic, and click “+ New Source Traffic” to create multiple sources with filtering options.

8. Click on the **Application Metadata** tab.
9. In the **Destination Traffic** section, click **+ Add New** to create an exporter to receive application-specific traffic. You can only create a maximum of 5 exporters. Enter the following details:

Option	Mandatory	Default	Description
Tool Name	Yes		Configures the alias name for the tool.
IP Interface	Yes		Configures the IP interface on the Gigamon device that connects to the tool.
Tool IP Address	Yes		Configures the destination IP address for exporting the records.
Template	No		Configures pre-defined tool templates for exporting metadata. Tool templates are user configurable. Ex. SplunkMetadataTemplate, SecurityPostureTemplate etc.
L4 Source Port	Yes		Configures the Source Port of the IP interface on the Gigamon device.
L4 Destination Port	Yes		Configures the destination port on the tools side.
Application ID	No	Disabled	Configures exporting Application Name for all applications identified by the DPI engine. Note: Requires AMI/SVP/ZTA license.
Application List	No		Each exporter can be customized to export metadata for certain applications/ protocols.
Format	Yes		Options: NetFlow, CEF Configures the format for exporting the records.
Version	Yes	IPFIX	Options: v5, v9 and IPFIX. Configures the version of NetFlow for exporting the records.
Template Refresh	Yes	60s	Range: 1-216000s Configures the interval at which the

Option	Mandatory	Default	Description
Interval			<p>template record is exported while exporting the IPFIX records.</p> <p>Changing the refresh interval can impact ingesting the records on the tools side. Please seek guidance from your tool's vendor before changing the default.</p>
Record Type	Yes	Cohesive/ Segregated	<p>Default depends on the Flow Behavior configuration.</p> <ul style="list-style-type: none"> • Segregated: Default when the Flow Behavior is set to Unidirectional. Separate records are exported for network and application metadata. • Cohesive: Default when the Flow Behavior is set to Bidirectional. Generates consolidated record comprising of network and application metadata. <p>If record size exceeds the IP interface MTU, the records will be exported as fragments.</p>
Active Timeout	Yes	60s	<p>Range: 1-604800s</p> <p>. This option configures the timeout interval for exporting interim records for such flows. Shorter timeouts increase the no. of records and longer timeouts result in fewer records. Longer timeouts can also increase the record size. Please seek expert guidance from Gigamon and tool vendor before changing the default.</p>
Inactive Timeout	Yes	15s	<p>Range: 1-604800s</p> <p>Configures the timeout interval for marking flows as inactive and exporting their records soon after.</p> <p>Inactive timeout constitutes idle time after receiving the last packet. Shorter timeouts can prematurely deem a flow as inactive and subsequent packets would be considered as a new flow that can skew the analytics on the tools side.</p> <p>Please seek expert guidance from Gigamon and tool vendor before changing the default.</p>

10. In the **Advanced Settings > Collects** section, the following details are already configured.

NOTE: When the template is NetFlow v5 or when the format is NetFlow and the version as V5 you cannot modify the **Collects**.

NOTE: The GTP -U collects are disabled if the template is the Netflow v9 .

Collect Fields	Attributes	Default Export	Notes
Data Link	Source MAC	No	
	Destination MAC	No	
	VLAN	No	
Interface	Input Interface	No	Supported values: 2B, 4B The default value is 2B for NetFlow v5 and 4B for NetFlow v9, IPFIX, and CEF. CEF supports exporting the Input interface index with a width of 2B (default) or 4B.
	Output Interface	No	Supported values: 2B, 4B The default value is 2B for NetFlow v5 and 4B for NetFlow v9, IPFIX, and CEF. CEF supports exporting the Output interface index with a width of 2B (default) or 4B.
	Input Name Width	No	Range: 1B to 32B The Default value is 16B.
IPv4			
	Source Address	Yes	
	Destination Address	Yes	
	TOS	No	
	DSCP	No	
	Protocol	Yes	
	Header Length	No	
	Payload Length	No	
	Total Length	No	
	Precedence	No	
	TTL	No	
	Option Map	No	
	Fragmentation ID	No	
	Fragmentation Offset	No	
	Fragmentation Flags	No	

Collect Fields	Attributes	Default Export	Notes
IPv6	Source Address	Yes	
	Destination Address	Yes	
	Extension Map	No	
	Next Header	Yes	
	Flow Label	No	
	Precedence	No	
	Traffic Class	No	
	DSCP	No	
	Hop Limit	No	
	Fragmentation ID	No	
	Fragmentation Offset	No	
	Fragmentation Flags	No	
	Header Length	No	
	Total Length	No	
	Payload Length	No	

Collect Fields	Attributes	Default Export	Notes
Transport	Source Port	Yes	Corresponds to both TCP and UDP.

Collect Fields	Attributes	Default Export	Notes
	Destination Port	Yes	Corresponds to both TCP and UDP.

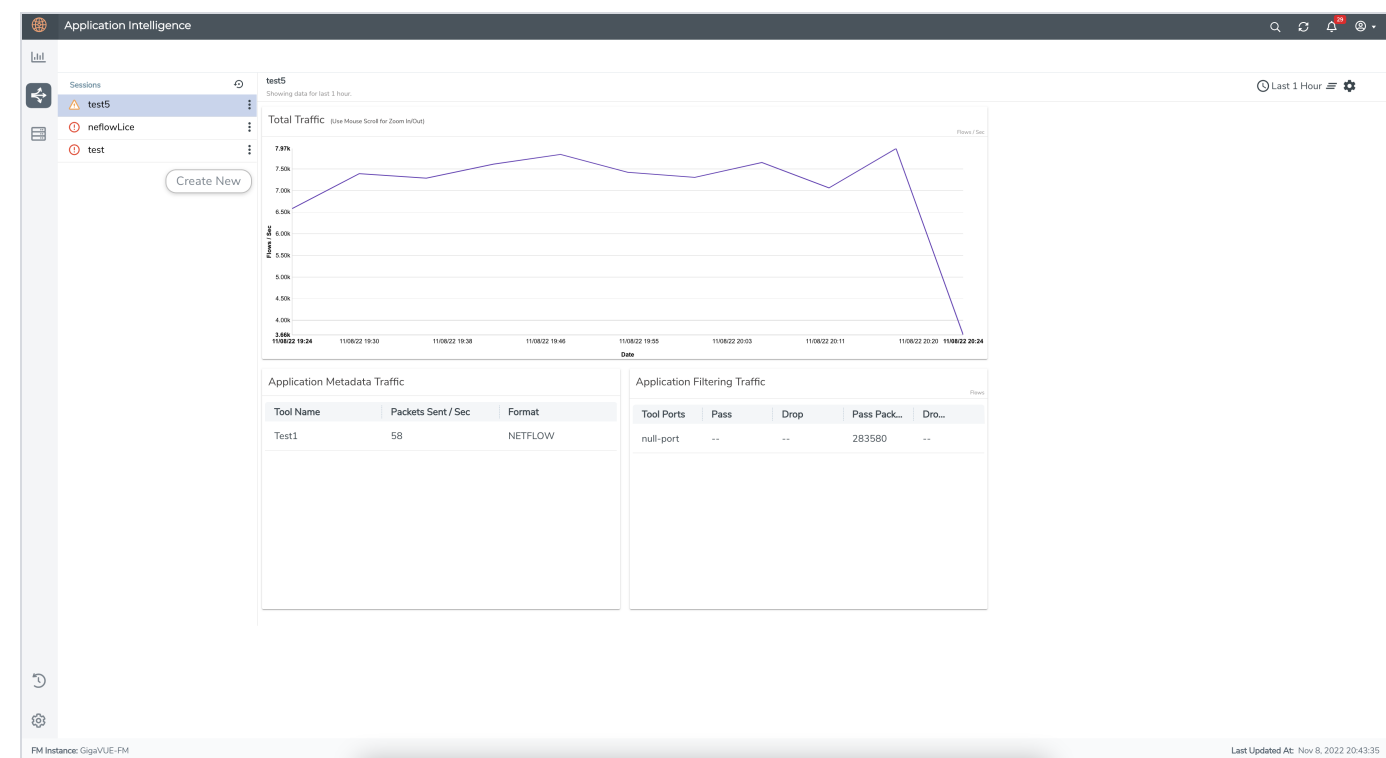
Collect Fields	Attributes	Default Export	Notes
	TCP ACK Number	No	
	TCP Header Length	No	
	TCP Sequence Number	No	
	TCP Urgent Pointer	No	
	TCP Flags	No	Following flags are supported in Gen 2 nodes : SYN, SYNACK, RST and FIN. For Gen 3 nodes all TCP flags are supported.
	TCP Window Size	No	
	UDP Message Length	No	
	MSS	No	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. This is supported only in Gen 3 GigaSMART cards and GigaVUE V Series.
	Aggregate Window Size	No	The actual minimum, mean, and maximum TCP window size values, calculated separately for both sender and receiver packets for a given flow per export interval. Its exported only when bidirectional flows are configured. This is supported only in Gen 3 GigaSMART cards and GigaVUE V Series.
	Zero Window	No	This captures TCP zero window event statistics (zero window, zero window probe and zero window acknowledgment) for both sender and receiver, indicating when the TCP receive buffer is full and data transmission is temporarily paused due to flow control for a given flow per export interval. Its exported only when bidirectional flows are configured. This is supported only in

Collect Fields	Attributes	Default Export	Notes
			Gen 3 GigaSMART cards and GigaVUE V Series.
ICMP	ICMP Code	No	Corresponds to types IPv4 and IPv6.
	ICMP Type	No	Corresponds to types IPv4 and IPv6.
Counter	Bytes	Yes	Options: 32, 64 (default) Determines the length of the counters, 32B or 64B. NetFlow v5 supports only 32B.
	Packets	Yes	Options: 32, 64 (default)
Timestamp	System Uptime First	Yes	Difference between the flow start time and the GigaSMART® uptime in milliseconds.
	System Uptime Last	Yes	Difference between the flow end time and the GigaSMART® uptime in milliseconds.
	Flow Start	Yes (msec)	
	Flow End	Yes (msec)	
Flow	End Reason	Yes	Inner flow end reason – TCP ack, reset, inactive, etc.

11. Click **Save**.

NetFlow Dashboard

In Appviz, only the traffic statistics are displayed as applications cannot be configured and used in the NetFlow configuration.



GigaVUE Enriched Metadata for Mobile Networks

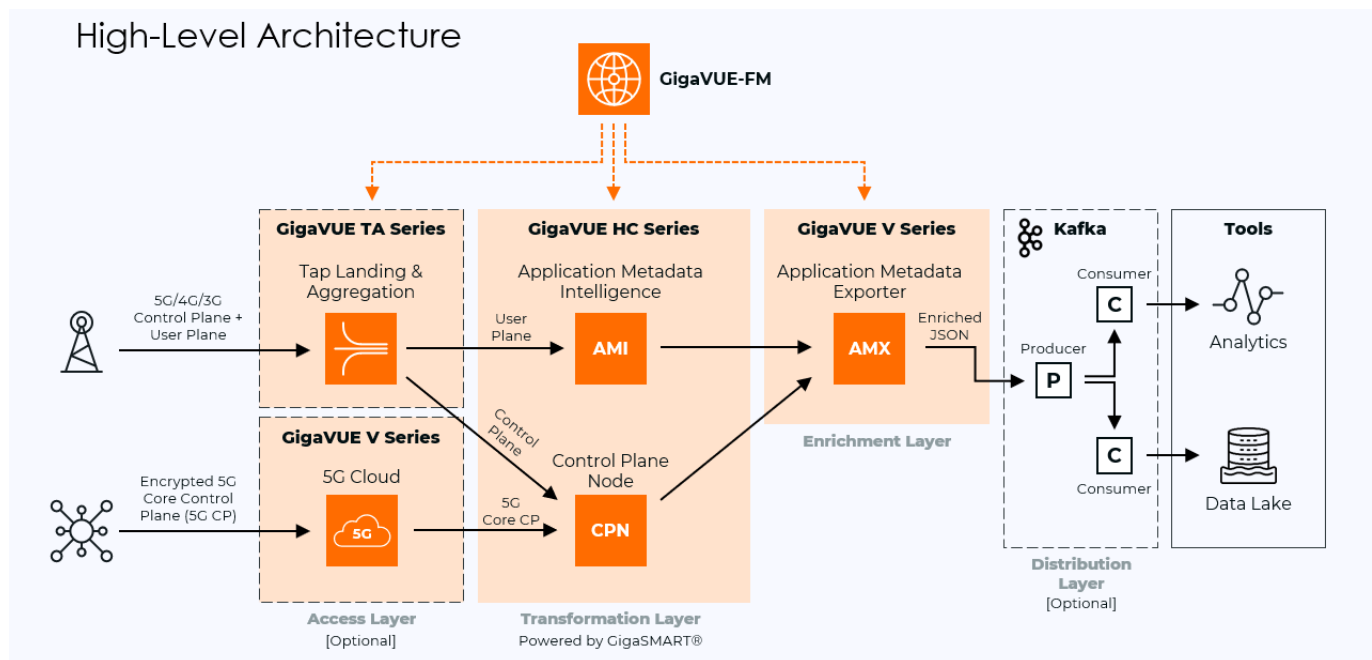
The metadata enrichment enhances service provider analytics by generating metadata on 5G/4G/3G network traffic. The AMX correlates the user plane metadata produced by AMI with the control plane metadata produced by the GTP/5G correlation mobility application to produce an enriched metadata feed for the mobile networks. This data feed helps the customers 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 stamp.
- Application Protocol
- Core Network Information
- User Tunnel Information

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

For information on AMX, refer to [Configure Application Metadata Exporter Application](#).

The architecture of GigaVUE Enriched Metadata for Mobile Networks is as follows:



AMI Configurations

The following CLI commands show the configurations to be done before the attributes are exported:

```
gsgroup alias GSG_S1U_AMI_01 port-list 1/2/e2 hash advanced
apps metadata app-profile alias AMI_APP_PROFILE
application add id
counter add bytes size 4
counter add inner-bytes size 4
counter add packets size 4
flow add end-reason
ipv4 add destination prefix minimum-mask /32
ipv4 add protocol
ipv4 add source prefix minimum-mask /32
ipv6 add destination prefix minimum-mask /128
ipv6 add next-header
ipv6 add source prefix minimum-mask /128
timestamp add flow-end-msec
timestamp add flow-start-msec
transport add destination-port
transport add source-port
type export
exit
```

The following CLI commands show how frequently the attributes are exported and to which destination (destination IP address, destination port number) they are exported:

```
apps metadata exporter alias AMI_METADATA_EXPORTER
app-profile attach alias AMI_APP_PROFILE
cef timeout active 30
cef timeout inactive 15
destination dscp 0
destination ip ver4 172.31.251.1
destination l4 protocol udp
l4 port dest 30100
l4 port src 35100
max-packet-size disable
monitor timeout 60
netflow template-refresh-interval 60
netflow timeout active 60
netflow timeout inactive 15
netflow version ipfix
record-type cohesive
source ip-interface attach HC3-TO-AMX-ETH0
```



```
ttl 64
type cef
exit
```

The following CLI commands explain about the cache details and the flow behavior of AMI Metadata Exporter:

```
apps metadata cache alias AMI_APP_CACHE
advance-hash disable
aggregate-mode disable
dpi-inject-limit disable
events enable transaction-end
exporter attach alias AMI_METADATA_EXPORTER
flow-behaviour bi-direction
match ipv4 add destination prefix minimum-mask /32
match ipv4 add protocol
match ipv4 add source prefix minimum-mask /32
match ipv6 add destination prefix minimum-mask /128
match ipv6 add next-header
match ipv6 add source prefix minimum-mask /128
match transport add destination-port
match transport add source-port
multi-collect disable
observ-domain-id 0
size flow 10
timeout idle 300
exit

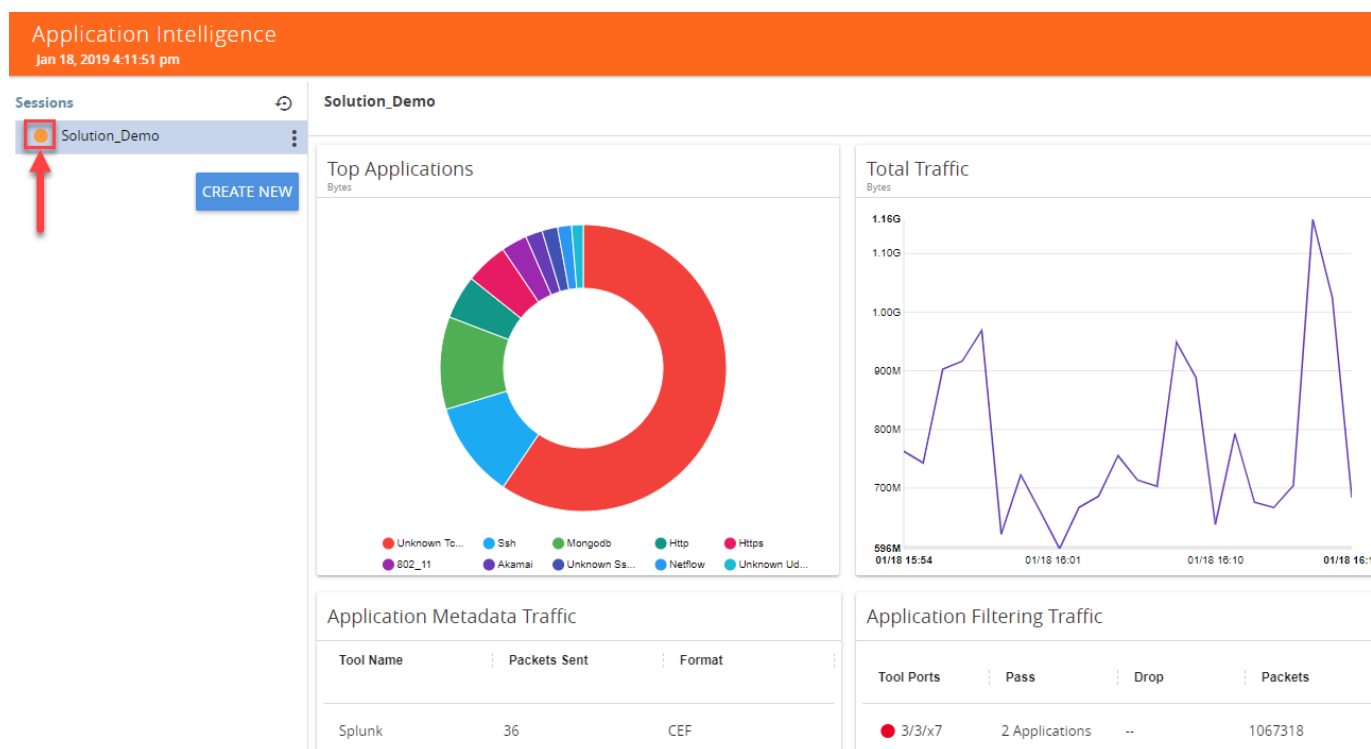
gsparams gsgroup GSG_S1U_AMI_01
resource metadata 10
metadata fastMode enable
exit
```

View the Health Status of a Solution

The health of an Application Intelligence solution is determined by the health status of the following components, and the configuration status during deployment of the solution in a device:

- IP interface
- Source Port
- Destination Port
- GigaSMART Engine


You can view the health status of the solution by a color indication next to the name of the solution as shown in the following figure:



The health status of a solution is indicated by the following colors:

Color	Health Status of a Solution
Green	Healthy - All the components in a solution are functioning properly.
Red	Unhealthy - Any of the components in a solution is not functioning properly.
Amber	Partially Healthy

You can also view the reason for a failover when you hover your mouse over the color indicator next to the name of the solution. To avoid this scenario:

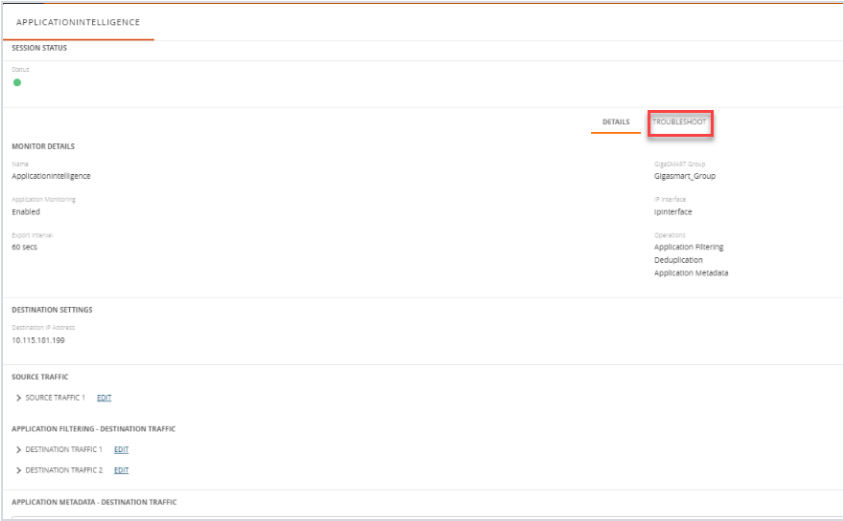
1. On the right side of the top navigation bar, click .
2. On the left navigation pane, select **System > Thresholds**.
3. Set the threshold value of GigaSMART engine port packet drops to zero.

The following table provides the health state of the Application Intelligence solution corresponding to the health state of its associated components:

Table 1: Health status of Solution Vs Health status of Associated Components

Health Status of a Solution	GSGroup	IP Interface	Network Port and Tool Port	Metadata Exporter	Configuration Deployment Status
Red	Unhealthy	Healthy	Healthy	Healthy	Success
Amber	Partially Healthy	Healthy	Healthy	Healthy	Success
Red	Healthy	Unhealthy	Healthy	Healthy	Success
Amber	Healthy	Partially Healthy	Healthy	Healthy	Success
Amber	Healthy	Healthy	Some Maps are Unhealthy/Partially Healthy	Healthy	Success
Red	Healthy	Healthy	All Maps are Unhealthy	Healthy	Success
Red	Healthy	Healthy	Healthy	All Metadata Exporters are Unhealthy	Success
Amber	Healthy	Healthy	Partially Unhealthy	Healthy	Success
Amber	Healthy	Healthy	Healthy	Some metadata exporters are Unhealthy	Success
Red	Healthy	Healthy	Healthy	Healthy	Failed
Amber	Healthy	Healthy	Healthy	Healthy	Partial Success
Red	Healthy	Healthy	Healthy	Healthy	Failed
Green	Healthy	Healthy	Healthy	Healthy	Success

To view the details of a solution, click **View Details > Troubleshoot**. For more details, refer to [View the Details of an Application Intelligence Session](#).



The solution page provides you the details of the health status of its associated components.

Upgrading the Protocol Signature

You can upgrade the protocol signature by upgrading the image file on the GigaSMART card, and by uploading the GigaSMART card image to GigaVUE-FM from the Internal Server or External Server. To select the image, follow the steps:

- Internal Server—Upload the GigaSMART card image to GigaVUE-FM from the internal server and select the image that you need to upgrade from the selected GigaSMART card.
- External Server—Provide the location of the image in the external server that you need to upgrade from the GigaSMART card.

For more information on upgrading the image, refer to the following topics in the GigaVUE-OS Upgrade guide:

- [Upgrade using image in External Image Server](#)
- [Upgrade using image in Internal server](#)

Disable Application Visibility in Application Intelligence Session

To disable Application Visibility, do the following:

1. Edit the Application Intelligence Session.
2. Disable the checkbox next to **Monitoring Enabled**.
3. Select **Save**.

After disabling the monitoring session, the Application Intelligence dashboard does not receive the updates and a message " **Monitoring has been disabled. Please enable monitoring to get latest data** " is shown in red at the top of the dashboard.

Application Intelligence Feature Compatibility

The table below shows the compatibility between Application Intelligence features and devices.

Application Intelligence Features	GigaVUE-HC1		GigaVUE-HC3		GigaVUE-HC1 Plus		GigaVUE-HCT
	Gen 2 On-board	Gen 3 SMT-HC1-S	Gen 2 (C05)	Gen 3 (C08)	Rear Gen3 SMT-HC1A-R	Front Gen 3 SMT-HC1-S	Gen 3 SMT-HC1-S
User Defined Application Signatures	X	√	X	√	√	√	√
Fast Mode	X	√	X	√	√	√	√
Aggregate Mode	X	√	X	√	√	√	√
Application Family and Tags	X	√	X	√	√	√	√
Max Packet Size	X	√	X	√	√	√	√
DPI Packet Limit	X	√	X	√	√	√	√
AMI Cache Monitoring	X	√	X	√	√	√	√

AdditionalInfoAppx

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 VÜE Community](#)

Documentation

This table lists all the guides provided for GigaVUE-FM,GigaVUE HC Series 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-FM,GigaVUE HC Series 6.12 Hardware and Software Guides	
<p>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.</p>	
Hardware	
how to unpack, assemble, rackmount, connect, and initially configure ports the respective GigaVUE-FM,GigaVUE HC Series devices; reference information and specifications for the respective GigaVUE-FM,GigaVUE HC Series 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-FM,GigaVUE HC Series 6.12 Hardware and Software Guides	
GigaVUE-TA100 Hardware Installation Guide	
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,GigaVUE HC Series 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 HC Series
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	
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-FM,GigaVUE HC Series 6.12 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,GigaVUE HC Series 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 HC Series, 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,GigaVUE HC Series 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,GigaVUE HC Series" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM,GigaVUE HC Series 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)