



GigaVUE Cloud Suite for Nutanix - Deployment Guide

GigaVUE Cloud Suite

Product Version: 6.5

Document Version: 1.0

Last Updated: Friday, February 9, 2024

(See Change Notes for document updates.)

Copyright 2024 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
6.5.00	1.0	12/11/2023	The original release of this document with 6.5.00 GA.

Contents

GigaVUE Cloud Suite for Nutanix - Deployment Guide	1
Change Notes	3
Contents	4
GigaVUE Cloud Suite Deployment Guide - Nutanix (GigaVUE V Series)	6
Overview of GigaVUE Cloud Suite for Nutanix	6
Components of GigaVUE Cloud Suite for Nutanix	7
Cloud Overview Page	7
Overall Cloud Overview Page	7
Platform specific Cloud Overview Page	7
Top Menu	8
Viewing Charts	10
Viewing Monitoring Session Details of all Cloud Platforms	11
Viewing Monitoring Session Details of Individual Cloud Platforms	12
Get Started with GigaVUE Cloud Suite for Nutanix Deployment	12
License Information	13
Volume Based License (VBL)	13
Base Bundles	13
Add-on Packages	14
How GigaVUE-FM Tracks Volume-Based License Usage	15
Apply License	18
Install and Upgrade GigaVUE-FM	18
Configure Components in Nutanix	19
Before You Begin	19
Prerequisites	19
Minimum Compute Requirements	20
Network Firewall Requirements	20
Upload Fabric Images	22
Deploy GigaVUE Cloud Suite for Nutanix	22
Install GigaVUE-FM on Nutanix	22
Install Custom Certificate	24
Upload Custom Certificates using GigaVUE-FM	24
Upload Custom Certificate using Third Party Orchestration	25

Create a Monitoring Domain	25
Configure GigaVUE Cloud Suite Fabric Components in GigaVUE-FM	26
Nutanix Fabric Launch Configuration	26
Configure Monitoring Sessions	28
Create a Monitoring Session	28
Interface Mapping	29
Create Ingress and Egress Tunnel	30
Create a New Map	35
Add Applications to Monitoring Session	38
View Monitoring Session Statistics	40
Visualize the Network Topology	41
Cloud Health Monitoring - Configuration Health	
Monitoring	42
View Monitoring Session Configuration Health	43
Health	43
V Series Node Health	43
Target Source Health	44
View Monitoring Session Statistics	44
View Monitoring Session Diagram	45
Analytics for Virtual Resources	45
Virtual Inventory Statistics and Cloud Applications Dashboard	46
Administer GigaVUE Cloud Suite for Nutanix	51
Configure Nutanix Settings	51
Role Based Access Control	51
About Events	52
About Audit Logs	54
Additional Sources of Information	57
Documentation	57
How to Download Software and Release Notes from My Gigamon	60
Documentation Feedback	60
Contact Technical Support	61
Contact Sales	62
Premium Support	62
The VUE Community	62
Glossary	63

GigaVUE Cloud Suite Deployment Guide - Nutanix (GigaVUE V Series)

This guide describes how to install, configure, and deploy the GigaVUE Cloud Suite for Nutanix-(GigaVUE V Series) in the Prism Central environment. Use this document for instructions on configuring the GigaVUE Cloud Suite Cloud components and setting up the traffic monitoring sessions for the Nutanix.

Topics:

- [Overview of GigaVUE Cloud Suite for Nutanix](#)
- [Get Started with GigaVUE Cloud Suite for Nutanix Deployment](#)
- [Configure Components in Nutanix](#)
- [Deploy GigaVUE Cloud Suite for Nutanix](#)
- [Cloud Health Monitoring - Configuration Health Monitoring](#)
- [Analytics for Virtual Resources](#)
- [Administer GigaVUE Cloud Suite for Nutanix](#)

Overview of GigaVUE Cloud Suite for Nutanix

GigaVUE® Fabric Manager (GigaVUE-FM) is a web-based fabric management interface that provides a single pane of glass visibility and management of both the physical and virtual traffic that form the GigaVUE Cloud Suite Cloud.

GigaVUE-FM integrates with the Nutanix Platform and deploys the components of the GigaVUE Cloud Suite for Nutanix in the underlay environment.

Once the GigaVUE Cloud Suite for Nutanix instance is launched in the Nutanix Prism central, the rest of the VM instances are automatically launched from GigaVUE-FM.

Refer to the following sections for details:

- [Components of GigaVUE Cloud Suite for Nutanix](#)

Components of GigaVUE Cloud Suite for Nutanix

GigaVUE Cloud Suite for Nutanix includes the following components:

- **GigaVUE® Fabric Manager (GigaVUE-FM)** is a web-based fabric management interface that provides a single pane of glass visibility and management of both the physical and virtual traffic that forms the GigaVUE Cloud Suite Cloud for Nutanix. GigaVUE-FM manages the configuration of the **GigaVUE® V Series Node**
- **GigaVUE® V Series Node** is a visibility node that aggregates mirrored traffic. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to on premise device or tools. GigaVUE Cloud Suite for Nutanix uses the standard IP GRE or VXLAN tunnels to deliver traffic to tool endpoints.
- **GigaVUE® V Series Proxy** manages multiple GigaVUE V Series nodes and orchestrates the flow of traffic from GigaVUE V Series Nodes to the monitoring tools. GigaVUE-FM uses one or more GigaVUE V Series Proxies to communicate with the GigaVUE V Series nodes.

Cloud Overview Page

The overview page is a central location to view and monitor all the monitoring sessions in a single place. You can use this overview page to spot issues which will help in troubleshooting, or perform basic actions like view, edit, clone, and delete. This page provides a quick overview of basic statistics, V Series Alarms, Connection Status and Volume Usage vs Allowance and a table to summarize the active monitoring sessions details. You can also edit the monitoring session from this page instead of navigating to the monitoring session page in each platform.

You can view cloud overview page in the following ways:

[Overall Cloud Overview Page](#)

[Platform specific Cloud Overview Page](#)

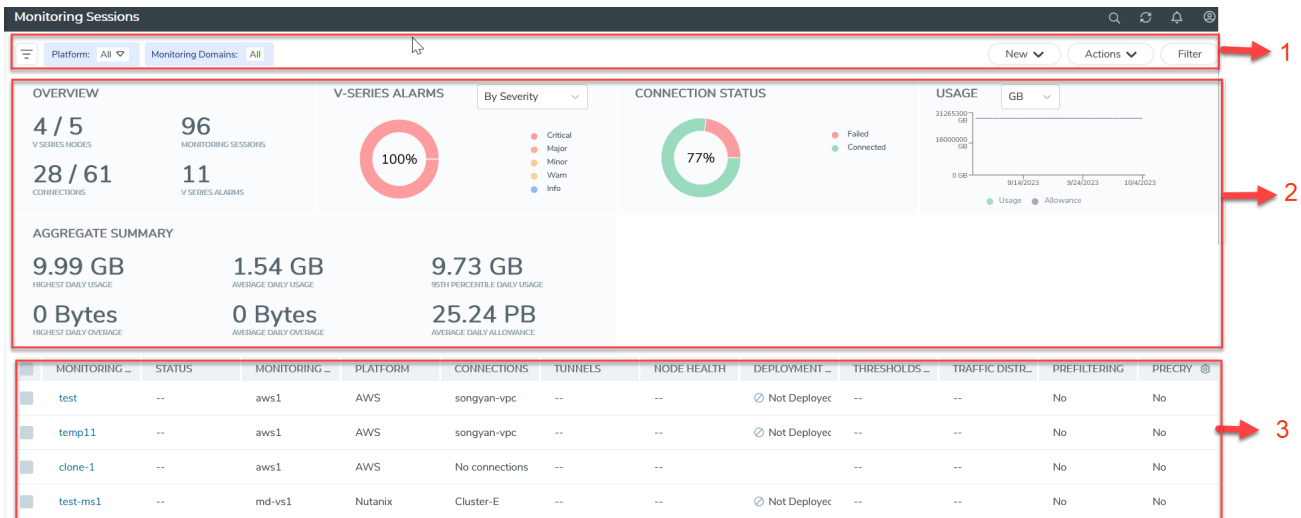
Overall Cloud Overview Page

To view the Overall Cloud Overview Page, Go to **Traffic > Virtual > Orchestrated Flows > Overview**

Platform specific Cloud Overview Page

To view Platform Specific Cloud Overview Page, Go to **Traffic > Virtual > Orchestrated Flows >** and select your cloud platform.

The **Monitoring Sessions** page appears as shown:



For easy understanding of the Monitoring Session page, the above figure is split into three major sections as described in the following table:

Number	Section	Description
1	Top Menu	Top Menu
2	Charts	Viewing Charts
3	Monitoring Session Details	<p>In Overall Cloud Overview Page, you can view the monitoring session details of all the cloud platforms.</p> <p>Refer to the section Viewing Monitoring Session Details of all Cloud Platforms</p> <p>In Platform specific Overview Page, you can view the monitoring session details of the individual cloud platforms.</p>

Top Menu

The Top menu consists of the following: options:

Options	Description
Filters	You can filter the monitoring session based on a criterion or combination of criteria such as based on the platform, monitoring session and V Series Node Id by applying filters. For more information, refer to Filters
New Drop-down list box	You create a new monitoring session and new monitoring domain. To create new monitoring session and monitoring domain refer to Create a Monitoring Session topic.

Options	Description
Action Drop-down list box	You can do the following actions through the Action Drop down list box: <ul style="list-style-type: none"> ▪ Edit - Opens the Edit page for the selected monitoring session. ▪ Delete - Deletes the selected monitoring session. ▪ Clone - Duplicates the selected monitoring session. ▪ Deploy - Deploys the selected monitoring session. ▪ Undeploy - Un-deploys the selected monitoring session. ▪ Apply Threshold - Applies the threshold template created for monitoring cloud traffic health. ▪ Apply Policy - Enables Precryption, Prefiltering, or Secure Tunnel. For more information, refer to Cloud Monitoring Session topic.

Filters

You can filter the monitoring session based on a criterion or combination of criteria such as based on the platform, monitoring session and V Series Node Id by applying filters.


You can apply the filters in two ways:

- [Filter on the left corner](#)
- [Filter on the right corner](#)

Filter on the left corner



You can view the monitoring sessions by filtering the monitoring domain based on the platform.

1. Select the required platform from the **Platform** drop- down list box.
2. Click  and select the monitoring domain.

The monitoring domain selected appears on the top menu bar.

Filter on the right corner



You can view the monitoring sessions by filtering the monitoring domain based on a criterion or by providing multiple criteria as follows:

- Monitoring Session
- Status
- Monitoring Domain
- Platform

- Connections
- Tunnel
- Deployment Status

Viewing Charts

You can view the following charts on the overview page:

- Overview
- V Series Alarms
- Connection Status
- Usage (VBL)
- Aggregate Summary

Overview

The overview dashboard displays the number of GigaVUE V Series Nodes active in GigaVUE-FM, the number of Monitoring sessions and connections configured in all the platforms, and the number of alarms triggered in V Series Nodes.

V Series Alarms

The V Series Alarms widget presents a pie chart that helps you to view the V Series alarms generated quickly. Each type of alarm triggered is assigned a color in the graph, which is specified by the legend. Hovering the mouse over an area in the chart displays the total number of V Series alarms triggered.

Connection Status

The connection status presents a pie chart that helps you to quickly view the connection status of connections configured in the monitoring domain. The success and failed connection status is differentiated by the color in the graph, which is specified by the legend. Hovering the mouse over an area in the chart displays the total number of connections.

Usage

The Usage widget displays the traffic that flows through the GigaVUE V Series Nodes. Each bar in the graph indicates the volume usage on a particular day. Hovering the mouse over a bar in the graph displays the volume allowance and volume usage on that day.


Aggregate Summary

The aggregate summary displays the highest daily volume usage, average daily volume usage, highest daily volume over usage, average daily volume over usage, 95th percentile daily volume usage and the average daily volume allowance.

Viewing Monitoring Session Details of all Cloud Platforms

You can view the following monitoring session details:

Details	Description
Monitoring Sessions	Name of the monitoring session. When you click the name of the session, you can view the following options: <ul style="list-style-type: none"> ● View- When you click this option, you can view a split window displaying the details of the monitoring sessions such as Statistics, Connections, V Series Nodes, Source Health, Http2 Logging. For more information, refer to Viewing Monitoring Session Details of Individual Cloud Platforms ● Edit - When you click this option, you can view the Edit Monitoring Session page.
Status	Health status of the monitoring session.
Monitoring Domain	Name of the Monitoring Domain to which the monitoring session is associated.
Platform	Cloud platform in which the session is created.
Connections	Connection details of the monitoring session.
Tunnels	Tunnel details related to the monitoring session
Node Health	Health of the node.
Deployment Status	Status of the deployment
Threshold Applied	Specifies whether the threshold is applied or not
Traffic Distribute	Specifies information about traffic distribution.
Prefiltering	Specifies whether Prefiltering is configured or not
Precryption	Specifies whether Precryption is configured or not.
SBI logging	Specifies whether SBI logging is configured or not.
Traffic Mirroring	Specifies whether Traffic Mirroring is configured or not.

NOTE: Click the settings icon  to select the columns that should appear in the monitoring session.

Viewing Monitoring Session Details of Individual Cloud Platforms

For a monitoring session, you can view the following details of the monitoring session:

Details	Description
Statistics	You can view the statistics of the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. You can view the statistics for all the V Series nodes or only for the Gigamon V Series node. You can also filter the statistics based on the elements associated with the monitoring session. For more information, refer to View Monitoring Session Statistics .
Connections	You can view the connection details of the monitoring session. You can view details such as the name of the connection, deployment status, number of targets, and targets source health.
V Series Nodes	You can view the V Series nodes associated with the monitoring session. You can also view details such as name of the V Series Node, Host VPC, MD connection, Version, and Management IP.
Source Health	You can view the health of the source connected to the monitoring session.
Http2 Logging	You can view the details of the 5G SBI logging details. For more information about 5G SBI, refer to 5G-Service Based Interface Application

To view the details, click the name of the monitoring session, and then click **View**. A split window appears displaying the details.

Get Started with GigaVUE Cloud Suite for Nutanix Deployment

This chapter describe show to plan and start the GigaVUE Cloud Suite for Nutanix in Nutanix.

Refer to the following sections for details:

- [License Information](#)
- [Install and Upgrade GigaVUE-FM](#)

License Information

GigaVUE Cloud Suite for Nutanix supports Volume Based License (VBL) model.

Refer to the following sections for details:

- [Volume Based License \(VBL\)](#)
- [Apply License](#)

Volume Based License (VBL)

All the GigaVUE V Series Nodes connected to GigaVUE-FM periodically report statistics on the amount of traffic that flows through the V Series Nodes. The statistics provide information on the actual data volume that flows through the V Series Nodes. All licensed applications, when running on the node, generate usage statistics.

Licensing for Cloud Suite is volume-based. In the Volume-Based Licensing (VBL) scheme, a license entitles specific applications on your V Series Nodes to use a specified amount of total data volume over the term of the license. The distribution of the license to individual nodes becomes irrelevant for Gigamon's accounting purpose. GigaVUE-FM tracks the total amount of data processed by the various licensed applications and provides visibility on the actual amount of data, each licensed application is using on each node, and tracks the overuse, if any.

Volume-based licenses are available as monthly subscription licenses with a service period of 1 month. Service period is the period of time for which the total usage or overage is tracked. There is a grace period for each license that is encoded in the license file. The license effectively provides data allowance for this additional time after the official end time of the license.

For purchasing licenses with the Volume-Based License (VBL) option, contact our Sales. Refer to [Contact Sales](#).

Base Bundles

In volume-based licensing scheme, licenses are offered as bundles. The following three base bundle types are available:

- CoreVUE
- NetVUE
- SecureVUEPlus

The bundles are available as SKUs¹. The number in the SKU indicates the total volume allowance of the SKU for that base bundle. For example, VBL-250T-BN-CORE has a daily volume allowance of 250 terabytes for CoreVUE bundle.

Bundle Replacement Policy

Refer to the following notes:

- You can always upgrade to a higher bundle but you cannot move to a lower version.
- You cannot have two different base bundles at the same time however, you can have multiple base bundles of the same type.
- Once upgraded to a higher bundle, the existing lower bundles will be automatically deactivated.

Add-on Packages

GigaVUE-FM allows you to add additional packages called add-on packages to the base bundles. These add-on packages allow you to add additional applications to your base bundles. Add-on packages have their own start/end date and volume specifications.

Rules for add-on packages:

- Add-on packages can only to be added when there is an active base bundle available in GigaVUE-FM.
- The base bundle limits the total volume usage of the add-on package.
- If your add-on package has volume allowance less than the base bundle, then your add-on package can only handle volume allocated for add-on package.
- When the life term of an add-on package extends beyond the base bundle, then when the base bundle expires, the volume allowance of the add-on package will be reduced to zero until a new base bundle is added.

For more information about SKUs refer to the respective Data Sheets as follows:

GigaVUE Data Sheets
GigaVUE Cloud Suite for VMware Data Sheet
GigaVUE Cloud Suite for AWS Data Sheet
GigaVUE Cloud Suite for Azure Data Sheet
GigaVUE Cloud Suite for OpenStack
GigaVUE Cloud Suite for Nutanix
GigaVUE Cloud Suite for Kubernetes

¹Stock Keeping Unit. Refer to the [What is a License SKU?](#) section in the FAQs for Licenses chapter.

How GigaVUE-FM Tracks Volume-Based License Usage

GigaVUE-FM tracks the license usage for each V series node as follows:


- When you create and deploy a monitoring session, GigaVUE-FM allows you to use only those applications that are licensed at that point (applicable only for ACTIVE licenses, licenses in grace period are not included).
- When a license goes into grace period, you will be notified with an audit log.
- When a license expires (and has not been renewed yet), the monitoring sessions using the corresponding license will not be undeployed.

For releases prior to 6.4:

- The monitoring sessions using the corresponding license will be undeployed (but not deleted from the database).
- When a license is later renewed or newly imported, any undeployed monitoring sessions are redeployed.

Manage Volume-based Licenses

To manage active Volume-based License:

1. On the left navigation pane, click .
2. Go to **System > Licenses**. From the top navigation bar, select the **VBL Active** from the **FM/Cloud** drop-down.

This page lists the following information about the active Volume-based Licenses:

Field	Description
SKUs	Unique identifier associated with the license
Bundles	Bundle to which the license belongs to
Volume	Total daily allowance volume
Starts	License start date
Ends	License end date
Type	Type of license (Commercial, Trial, Lab and other license types).
Activation ID	Activation ID
Entitlement ID	Entitlement ID

NOTE: The License Type and Activation ID are displayed by default in the VBL Active page. To display the Entitlement ID field, click on the column setting configuration option to enable the Entitlement ID field.

The expired licenses are displayed in the **VBL Inactive** page, which can be found under the **FM/Cloud** drop-down in the top navigation bar. This page lists the following information about the inactive Volume-based Licenses:

Field	Description
SKUs	Unique identifier associated with the license.
Bundles	Bundle to which the license belongs to.
Ends	License end date
Grace Period	Number of days the license is in grace period
Deactivation Date	Date the license got deactivated.
Revocation Code	License revocation code.
Status	License status.

NOTE: The License Type, Activation ID and Entitlement ID fields are not displayed by default in the VBL Inactive page. To display these fields, click on the column setting configuration option and enable these fields.

Use the following buttons to manage your VBL.

Button	Description
Activate Licenses	Use this button to activate a Volume-based License. Refer to Activate Volume-based Licenses for more information.
Email Volume Usage	Use this button to send the volume usage details to the email recipients.
Filter	Use this button to narrow down the list of active Volume-based Licenses that are displayed on the VBL active page.
Export	Use this button to export the details in the VBL active page to a CSV or XLSX file.
Deactivate	Use this button to deactivate the licenses. You can only deactivate licenses that are in grace period or that have expired.


For more detailed information on dashboards and reports generation for Volume-based Licensing refer to the following table:

For details about:	Reference section	Guide
How to generate Volume-based License reports	Generate VBL Usage Reports	GigaVUE Administration Guide

Volume-based Licensed report details	Volume Based License Usage Report	GigaVUE Administration Guide
Fabric health analytics dashboards for Volume-based Licenses usage	Dashboards for Volume Based Licenses Usage	GigaVUE-FM User Guide

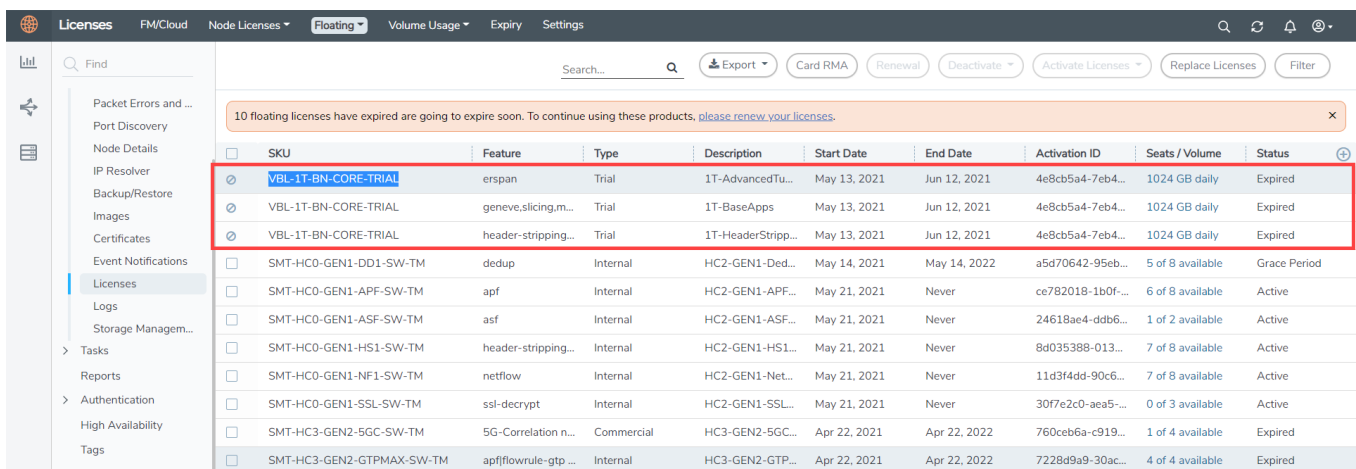
Activate Volume-based Licenses

To activate Volume-based licenses:

1. On the left navigation pane, click .
2. Go to **System > Licenses**. From the top navigation bar, select the **VBL Active** from the **FM/Cloud** drop-down.
3. Click **Activate Licenses**. The **Activate License** page appears. Perform the following steps:
 - a. Download the fabric inventory file that contains information about GigaVUE-FM. Click **Next**. Refer to the [What is a Fabric Inventory File?](#) section for more details.
 - b. Navigate to the Licensing Portal. Upload the Fabric Inventory file in the portal. Once the fabric inventory file is uploaded, select the required license and click **Activate**. A license key is provided. Record the license key or keys.
 - c. Return to GigaVUE-FM and add the additional licenses.

Default Trial Licenses

After you install GigaVUE-FM, a default free 1TB of CoreVUE trial volume-based license (VBL) is provided one-time for 30 days (from the date of installation).



SKU	Feature	Type	Description	Start Date	End Date	Activation ID	Seats / Volume	Status
VBL-1T-BN-CORE-TRIAL	erspan	Trial	1T-AdvancedTu...	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
VBL-1T-BN-CORE-TRIAL	geneve.slicing.m...	Trial	1T-BaseApps	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
VBL-1T-BN-CORE-TRIAL	header-stripping...	Trial	1T-HeaderStripp...	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
SMT-HC0-GEN1-DD1-SW-TM	dedup	Internal	HC2-GEN1-Ded...	May 14, 2021	May 14, 2022	a5d70642-95eb...	5 of 8 available	Grace Period
SMT-HC0-GEN1-APF-SW-TM	apf	Internal	HC2-GEN1-APF...	May 21, 2021	Never	ce782018-1b0f...	6 of 8 available	Active
SMT-HC0-GEN1-ASF-SW-TM	asf	Internal	HC2-GEN1-ASF...	May 21, 2021	Never	24618ae4-ddb6...	1 of 2 available	Active
SMT-HC0-GEN1-HS1-SW-TM	header-stripping...	Internal	HC2-GEN1-HS1...	May 21, 2021	Never	8d035388-013...	7 of 8 available	Active
SMT-HC0-GEN1-NF1-SW-TM	netflow	Internal	HC2-GEN1-Net...	May 21, 2021	Never	11d3f4dd-90c6...	7 of 8 available	Active
SMT-HC0-GEN1-SSL-SW-TM	ssl-decrypt	Internal	HC2-GEN1-SSL...	May 21, 2021	Never	30f7e2c0-aea5...	0 of 3 available	Active
SMT-HC3-GEN2-5GC-SW-TM	5G-Correlation n...	Commercial	HC3-GEN2-5GC...	Apr 22, 2021	Apr 22, 2022	760ceb6a-c919...	1 of 4 available	Expired
SMT-HC3-GEN2-GTPMAX-SW-TM	apfflowrule-gtp...	Internal	HC3-GEN2-GTP...	Apr 22, 2021	Apr 22, 2022	7228d9a9-30ac...	4 of 4 available	Expired

This license includes the following applications:

- ERSPAN
- Geneve
- Slicing
- Masking


- Trailer
- Tunneling
- Load Balancing
- Enhanced Load Balancing
- Flowmap
- Header-stripping
- Add header

NOTE: There is no grace period for the trial license. If you do not have any other Volume-based licenses installed, then after 30 days, on expiry of the trial license, any deployed monitoring sessions will be undeployed from the existing GigaVUE V Series Nodes.

To deactivate the trial VBL refer to [Delete Default Trial Licenses](#) section for details.

Delete Default Trial Licenses

GigaVUE-FM allows you to deactivate the default trial licenses from this page. To deactivate the license:

1. On the left navigation pane, click .
2. Go to **System > Licenses > Floating**. Click **Activated**.
3. Click **Deactivate > Default Trial VBL**.

The VBL trial licenses is deactivated and is no longer listed in the Activated page. However, you can view these deactivated licenses from the Deactivated page.

Apply License

For instructions on how to generate and apply license refer to the *GigaVUE Licensing Guide*.

Install and Upgrade GigaVUE-FM

You can install and upgrade the GigaVUE Cloud Suite® Fabric Manager (GigaVUE-FM) on cloud or on-premises.

- Cloud —To install GigaVUE-FM in Nutanix Prism Central Platform, you must upload the recent GigaVUE-FM image file to the Prism Central. For the GigaVUE-FM installation procedures, refer to [Install GigaVUE-FM on Nutanix](#).
- On-premises—To install and upgrade GigaVUE-FM in your enterprise data center, refer to *GigaVUE-FM Installation and Upgrade Guide* available in the [Gigamon Documentation Library](#).

Configure Components in Nutanix

This chapter describes how to configure GigaVUE V Series Node and GigaVUE V Series Proxy in your environment. Refer to the following sections for details:

- [Before You Begin](#)
- [Upload Fabric Images](#)
- [Install GigaVUE-FM on Nutanix](#)
- [Configure GigaVUE Cloud Suite Fabric Components in GigaVUE-FM](#)

Before You Begin

This section describes the requirements and prerequisites to configure the GigaVUE Cloud Suite for Nutanix. Refer to the following section for details.

- [Prerequisites](#)
- [Minimum Compute Requirements](#)
- [Network Firewall Requirements](#)

Prerequisites

The following are the prerequisites for configuring GigaVUE-FM and fabric images in Nutanix.

- You must upload the GigaVUE-FM image and fabric image (GigaVUE® V Series Node) files in the Prism Central repository. Do not use the Prism Element to upload the GigaVUE-FM image and fabric image files.
- Assigning a static IP for GigaVUE V Series Node, GigaVUE V Series Proxy is not supported. DHCP must be enabled for the management subnet and tunnel subnet.
- Only one GigaVUE® V Series Node can be deployed per Nutanix Node.
- For GigaVUE Cloud Suite-FM to orchestrate the solution, the minimum requirement that the Nutanix admin account must be a **Prism Central Admin** on Prism Central and a **Cluster Admin** on individual clusters. The password must set to be the same across the environment if they are locally managed. Alternatively, if the Nutanix Prism Central is configured with external authentication like AD/LDAP then you can avoid replicating the manual password creation across the environment.
- Ensure that appropriate Nutanix fabric images are uploaded.

- You must create a subnet and security group. For more information on creating a subnet, see [Configuring Network Connections](#).

Default Login Credentials

You can login to the GigaVUE V Series Node and GigaVUE V Series Proxy by using the default credentials.

Product	Login credentials
GigaVUE V Series Node	You can login to the GigaVUE V Series Node by using ssh. The default username and password is: Username: gigamon Password: Gigamon123!
GigaVUE V Series proxy	You can login to the GigaVUE V Series proxy by using ssh. The default username and password is: Username: gigamon Password: Gigamon123!

Minimum Compute Requirements

The minimum recommended computing requirements are listed in the following table.

Compute Instances	vCPU	Memory	Disk Space	Description
GigaVUE-FM	2 vCPU	16GB	2 x 40GB	GigaVUE-FM must be able to access the V Series Nodes directly or a GigaVUE V Series Proxy that will relay the commands to the GigaVUE V Series Nodes.

Network Firewall Requirements

Following are the Network Firewall Requirements for Gigamon fabrics for Nutanix deployments.

Direction	Type	Protocol	Port	CIDR	Purpose
GigaVUE-FM					
Inbound	HTTPS	TCP	443	Anywhere Any IP	Allows GigaVUE® V Series Nodes, GigaVUE V Series Proxy, and GigaVUE-FM administrators to

Direction	Type	Protocol	Port	CIDR	Purpose
					communicate with GigaVUE-FM
Inbound	SSH	TCP	22	Anywhere Any IP	Allows GigaVUE® V Series Nodes, GigaVUE V Series Proxy, and GigaVUE-FM administrators to communicate with GigaVUE-FM
Outbound (optional)	Custom TCP Rule	TCP	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Node
Outbound	Custom TCP Rule	TCP	9440	Prism Central IP, Prism Element IP	Allows GigaVUE-FM to communicate with Prism Central and Prism Element.
GigaVUE V Series Node					
Inbound	Custom TCP Rule	TCP	9903	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Proxy to communicate with GigaVUE® V Series Nodes
Inbound	UDP	UDPGRE	4754	Ingress Tunnel	Allows to UDPGRE tunnel to communicate and tunnel traffic to GigaVUE V Series Nodes
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows GigaVUE® V Series Node to communicate and tunnel traffic to the Tool
Outbound	Custom UDP Rule	<ul style="list-style-type: none"> UDP (VXLAN) IP Protocol (L2GRE) 	<ul style="list-style-type: none"> VXLAN (default 4789) L2GRE (IP 47) 	Tool IP	Allows GigaVUE® V Series Node to communicate and tunnel traffic to the Tool
Outbound (optional)	Custom ICMP Rule	ICMP	<ul style="list-style-type: none"> echo request echo reply 	Tool IP	Allows GigaVUE® V Series Node to health check the tunnel destination traffic.
GigaVUE V Series Proxy (optional)					
Inbound	Custom TCP Rule	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Node

Upload Fabric Images

The recent GigaVUE V Series Node and GigaVUE-FM image file can be downloaded from [Gigamon Customer Portal](#). After fetching the images, upload the fabric images to Prism Central. Select all the available clusters as placements while uploading fabric images.

Upload the appropriate Nutanix image file.

Once the images are uploaded, you can view the images under **Virtual Infrastructure > Images** in the Nutanix console.

Deploy GigaVUE Cloud Suite for Nutanix

This section describes how to connect, launch, and deploy fabric components of GigaVUE Cloud Suite for Nutanix.

Refer to the following sections for details:

- [Install GigaVUE-FM on Nutanix](#)
- [Create a Monitoring Domain](#)
- [Configure GigaVUE Cloud Suite Fabric Components in GigaVUE-FM](#)
- [Configure Monitoring Sessions](#)

Install GigaVUE-FM on Nutanix

To launch the GigaVUE-FM instance from the Prism Central:

1. Log in to the [Gigamon Customer Portal](#) and click on Software and Release Notes.
2. Then, search **qcow2** in the search file field.
3. Use the **Filter by** option to filter your search by Product, Release, Release Type and Release date. Select GigaVUE-FM as the product, and the enter the release version in the release field.
4. The QCOW2 file appears in the list view. Click on the latest QCOW2 file to download it.

- Log in to Prism Central.
- In Prism Central, select **Dashboard > Virtual Infrastructure > VMs**. The VMs page appears.

NOTE: You can view the uploaded images under **Virtual Infrastructure > Images**. For more detailed information on how to upload fabric images refer Upload Fabric Images topic in the *GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide*.

- On the VMs page, click **Create VM**. The **Create VM** window appears.

NOTE: If the device has more than one cluster, select the required cluster in the **Cluster Selection** window.

- Enter or select the values as described in the following table.

Field	Description
General Configuration	<ul style="list-style-type: none"> Name—Enter a name for the VM. Description—Enter description for the VM. (optional) Timezone—Select the time zone from the drop-down list.
Compute Details	<ul style="list-style-type: none"> vCPU(s)—number of vCPUs required. Minimum value is 2vCPUs. However, the recommended value is 4vCPUs. Number Of Cores Per vCPU—number of cores per vCPU. Memory—memory size of the vCPU(s). Minimum value is 16GB.
Disks	Add, edit or delete the disks. Add the GigaVUE-FM qcow2 disk image and a Container (second disk), minimum of 40GB for the VM. Select the primary image (GigaVUE-FM qcow2) as Boot Device.
Network Adapters (NIC)	Add a minimum of 1 vNIC for traffic management.
VM Host Affinity (Optional)	Set Affinity by choosing the required nodes to run GigaVUE-FM or a particular VM.

- Click **Save** and the new VM appears on the VMs list with the **Power State** as **Off**.
- Select the new VM and then select **Actions > Power On**. The new VM is now Active.
- Select the new VM and then select **Actions > Launch console**. The GigaVUE-FM console appears.
- Log in to the GigaVUE-FM console as admin with the user name as admin and default password admin123A!! and you are requested to change the password.

NOTE: You can also choose to perform the IP Networking and NTP configurations by running the **fmctl jump-start** command after you power on the GigaVUE-FM instance. Refer to Perform Network Configurations topic in the *GigaVUE-FM Installation and Upgrade Guide* for more details on how to use **fmctl jump-start** to perform the initial network configuration.

You can also log in to GigaVUE-FM by logging in to WebUI using the configured IP address using the default user name **admin** and the default password admin123A!!.

Install Custom Certificate

GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controllers have default self-signed certificates installed. The communication between GigaVUE-FM and the fabric components happens in a secure way using these default self-signed certificates, however you can also add custom certificates like SSL/TLS certificate to avoid the trust issues that occurs when the GigaVUE V Series Nodes, GigaVUE V Series Proxy, or UCT-V Controllers run through the security scanners.

You can upload the custom certificate in two ways:

- [Upload Custom Certificates using GigaVUE-FM](#)
- [Upload Custom Certificate using Third Party Orchestration](#)

Upload Custom Certificates using GigaVUE-FM

To upload the custom certificate using GigaVUE-FM follow the steps given below:

1. Go to **Inventory > Security > Custom SSL Certificate**. The **Custom Certificate Configuration** page appears.
2. On the Custom Certificate Configuration page, click **Add**. The **New Custom Certificate** page appears.
3. Enter or select the appropriate information as shown in the following table.

Field	Action
Certificate Name	Enter the custom certificate name.
Certificate	Click on the Upload Button to upload the certificate.
Private Key	Click on the Upload Button to upload the private key associated with the certificate.

4. Click **Save**.

You must also add root or the leaf CA certificate in the Trust Store. For more detailed information on how to add root CA Certificate, refer to Trust Store topic in *GigaVUE Administration Guide*.

The certificates uploaded here can be linked to the respective GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controller in the Fabric Launch Configuration Page. Refer to *Configure GigaVUE Fabric Components in GigaVUE-FM* topic in the respective cloud guides for more detailed information.

Upload Custom Certificate using Third Party Orchestration

You can also upload custom certificates to GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controller using your own cloud platform at the time of deploying the fabric components. Refer to the following topics on more detailed information on how to upload custom certificates using third party orchestration in the respective platforms:

For integrated mode:

- [Configure GigaVUE Fabric Components in AWS](#)
- [Configure GigaVUE Fabric Components in Azure](#)
- [Configure GigaVUE Fabric Components in OpenStack](#)

For generic mode:

- [Configure GigaVUE Fabric Components in AWS](#)
- [Configure GigaVUE Fabric Components in Azure](#)
- [Configure GigaVUE Fabric Components in GCP](#)
- [Configure GigaVUE Fabric Components in Nutanix](#)
- [Configure GigaVUE Fabric Components in OpenStack](#)
- [Configure GigaVUE V Series Nodes using VMware ESXi](#)

Create a Monitoring Domain

GigaVUE-FM provides you the flexibility to connect to multiple clusters.

NOTE: To configure the monitoring domain and launch the fabric components in Nutanix Prism, you must be a user with **Admin** role or a user with write access to the **Cluster Management** category.

To create a Monitoring Domain:

1. Go to **Inventory > Virtual > Nutanix** and then click **Monitoring Domain**.
2. On the Monitoring Domain page, click the **New** button. The Monitoring Domain Configuration page appears.

3. Enter or select the appropriate information as shown in the following table.

Field	Action
Monitoring Domain	Enter a monitoring domain name.
Connection Alias	An alias used to identify the monitoring domain.
Use Legacy V Series Mode	By default, V Series 2 is enabled. Enable this option, if you want to use the legacy V Series Mode
Nutanix Prism Central IP	Enter the Nutanix Prism Central IP address.
Nutanix Prism Central Username	Enter the username.
Nutanix Prism Central Password	Enter the password
Cluster	Select the cluster where the GigaVUE V Series Proxy and GigaVUE® V Series Node are to be deployed.
Traffic Acquisition tunnel MTU	Enter the Tunnel MTU size.

4. Click **Save**. The **Nutanix Fabric Launch Configuration** page appears.

Configure GigaVUE Cloud Suite Fabric Components in GigaVUE-FM

You must establish a connection between GigaVUE-FM and your Prism environment before you can perform the configuration steps for GigaVUE® V Series Node and GigaVUE V Series Proxy. After a connection is established, you can use GigaVUE-FM to specify a launch configuration for the GigaVUE® V Series Nodes.

Nutanix Fabric Launch Configuration

The fabric images (GigaVUE V Series Proxy and GigaVUE® V Series Node) are launched by GigaVUE-FM based on the configuration made in Nutanix Fabric Launch Configuration page.

GigaVUE V Series Proxy manages multiple GigaVUE® V Series Node and orchestrates the flow of traffic from GigaVUE® V Series Nodes to the monitoring tools.

To configure the Nutanix Fabric Images in GigaVUE-FM, do the following:

1. After [Nutanix Configuration](#) in GigaVUE-FM, you are navigated to **Nutanix Fabric Launch Configuration** page.
2. On the Nutanix Fabric Launch Configuration page, enter or select the following information.

Field	Description
Cluster	Select the cluster where the GigaVUE V Series Proxy and GigaVUE® V Series Node are to be deployed.
Enable Custom Certificates	Enable this option to validate the custom certificate during SSL Communication. GigaVUE-FM validates the Custom certificate with the trust store. If the certificate is not available in Trust Store, communication does not happen, and an handshake error occurs. NOTE: If the certificate expires after the successful deployment of the fabric components, then the fabric components moves to failed state.
Certificate	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For more detailed information, refer to Install Custom Certificate .
Configure a V Series Proxy (Optional)	Select this option to configure a V Series Proxy.
GigaVUE® V Series Node	<ul style="list-style-type: none"> • Hosts—Select a node or multiple nodes from the selected Cluster. • Version—Select a GigaVUE® V Series Node image file. Refer to Upload Fabric Images for more information. • Management Subnet—The subnets registered in Prism Central are listed. Select a management subnet as specified in the Prerequisites. • Data Subnets—Select the subnet(s) based on the required VMs and vNICs. Click Add Subnet to add additional Subnets. • Memory Size (GB)—Enter the memory size of the vCPU(s) • Disk Size (GB)—Enter the image size of the GigaVUE® V Series Node. • Number of vCPUs—Enter the number of vCPUs required. • Cloud-init User Data (Optional)—Enter cloud-init user data (YAML, JSON, or Shell script)

NOTE: Assigning a Static IP for GigaVUE V Series Nodes is not supported. DHCP must be enabled for the management subnet and tunnel subnet.

3. Click **Save & Configure Next Cluster** to configure next Cluster, or Click **Save & Exit** to initiate the deployment of the selected fabric images. You can view the status of the deployment on the Tasks page of Prism Central.

To view the fabric launch configuration specification of a fabric node, click on a V Series fabric node, and a quick view of the Fabric Launch Configuration appears on the Monitoring Domain page.

Configure Monitoring Sessions

GigaVUE-FM collects inventory data on all V series nodes deployed in your environment through Nutanix Prism Central. You can design your monitoring session to include or exclude the target VMs that you want to monitor. You can also choose to monitor egress, ingress, or all traffic. When a new target VM is added to your environment, GigaVUE-FM automatically detects it and based on the selection criteria, the detected target VMs are added into your monitoring session. Similarly, when a traffic monitoring target VM is removed, it updates the monitoring sessions to show the removed instance. Before deploying a monitoring session, you need to deploy a V Series node in each host where you want to monitor the traffics.

Refer to the following topics for details:

- [Create a Monitoring Session](#)
- [Create Ingress and Egress Tunnel](#)
- [Create a New Map](#)
- [Add Applications to Monitoring Session](#)
- [To deploy the monitoring session:](#)
- [View Monitoring Session Statistics](#)
- [Visualize the Network Topology](#)

Create a Monitoring Session

GigaVUE-FM automatically collects inventory data on all target instances available in your cloud environment. You can design your monitoring session to include or exclude the instances that you want to monitor. You can also choose to monitor egress, ingress, or all traffic.

When a new target instance is added to your cloud environment, GigaVUE-FM automatically detects and adds the instance into your monitoring session. Similarly, when an instance is removed, it updates the monitoring sessions to show the removed instance.

NOTE: You can have multiple monitoring sessions per monitoring domain.

You can create multiple monitoring sessions within a monitoring domain.

To create a new monitoring session:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows > Nutanix**. The **Monitoring Sessions** page appears.
2. Click **New** to open the **Create a New Monitoring Session** page.

Create A New Monitoring Session

Alias

Monitoring Domain

Cluster

3. Enter the appropriate information for the monitoring session as described in the following table.

Field	Description
Alias	The name of the monitoring session.
Monitoring Domain	The name of the monitoring domain that you want to select.
Cluster	The cluster(s) that are to be included as part of the monitoring domain. You can select the required cluster that need to be part of the monitoring domain.

4. Click **Create**. The Monitoring Session details page appears displaying the specified session information and target VMs. .

Interface Mapping

You can change the interface of individual GigaVUE V Series Nodes deployed in a monitoring session. After deploying the monitoring session, if you wish to change the interfaces mapped to an individual GigaVUE V Series Node, you can use the **Interface Mapping** button to map the interface to the respective GigaVUE V Series Nodes. To perform interface mapping:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Select a Monitoring session from the list view and click **Actions > Edit**. The Edit Monitoring session page appears.

3. In the Edit Monitoring session canvas page, click on the **Interface Mapping** button.
4. The **Select nodes to deploy the Monitoring Session dialog box** appears. Select the GigaVUE V Series Nodes for which you wish to map the interface.
5. After selecting the GigaVUE V Series Node, select the interfaces for each of the REPs and the TEPs deployed in the monitoring session from the drop-down menu for the selected individual GigaVUE V Series Nodes. Then, click **Deploy**.

Create Ingress and Egress Tunnel

Traffic from the GigaVUE V Series Node is distributed to tunnel endpoints in a monitoring session. A tunnel endpoint can be created using a standard L2GRE, VXLAN, or ERSPAN tunnel.

To create a new tunnel endpoint:

1. After creating a new monitoring session, or click **Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select **New > New Tunnel**, drag and drop a new tunnel template to the

workspace. The **Add Tunnel Spec** quick view appears.

3. On the New Tunnel quick view, enter or select the required information as described in the following table.

Field	Description	
Alias	The name of the tunnel endpoint. NOTE: Do not enter spaces in the alias name.	
Description	The description of the tunnel endpoint.	
Type	The type of the tunnel. Select ERSPAN, or L2GRE, or VXLAN, or UDPGRE to create a tunnel.	
VXLAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose In (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
Out	Choose Out (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint.	
	Remote Tunnel IP	For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled

Field	Description	
		with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
L2GRE		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose In (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value between 0 and 4294967295.
Out	Choose Out (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint.	
	Remote Tunnel IP	For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.

Field	Description	
	DSCP	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value between 0 and 4294967295.
ERSPAN		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		
In	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	Flow ID	The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023.
TLS-PCAPNG		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		

Field	Description	
In	IP Version	The version of the Internet Protocol. only IPv4 is supported.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6.
Delay Acknowledgments	Enable to receive the acknowledgments when there is a delay.	

4. Click **Save**.

To delete a tunnel, select the required tunnel and click **Delete**.

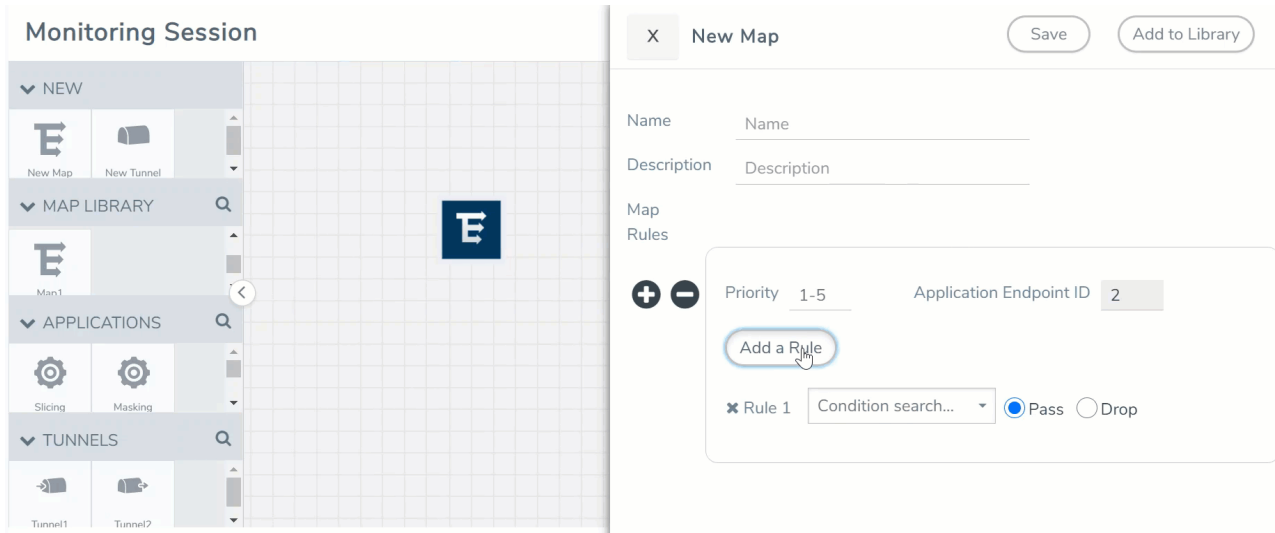
Create a New Map

You must have the flow map license to deploy a map in monitoring session.


For new users, the free trial bundle will expire after 30 days and the GigaVUE-FM prompts you to buy a new license. For detailed information on GigaVUE-FM licenses, refer to "Licenses" section in the *GigaVUE Administration Guide*.


To create a new map:

1. After creating a new monitoring session, or click **Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select **New > New Map**, drag and drop a new map template to the workspace. The New Map quick view appears.



3. On the New Map quick view, enter or select the required information as described in the following table.

Field	Description
Name	Name of the new map
Comments	Description of the map
Map Rules	<p>The rules for filtering the traffic in the map. Through the map, packets can be dropped or passed based on the highest to lowest rule priority. You can add multiple rule sets on a map. Use the + and - buttons to add or remove a rule set in the map. A rule set can have only 5 rules per map and 25 conditions per map. To add ATS rules for an Inclusion/Exclusion map, you must select atleast one rule condition.</p> <p>To add a map rule:</p> <ol style="list-style-type: none"> Enter a Priority value from 1 to 5 for the rule with 5 being the highest and 1 is the lowest priority. Click Add a Rule. The new rule field appear for the Application Endpoint. Select a required condition from the drop-down list. Select the rule to Pass or Drop through the map. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> If two rules with same condition are configured as pass and drop,</p> <ul style="list-style-type: none"> on a same tunnel endpoint, the traffic filtering precedence will be based on the priority value. on two different tunnel endpoints, the traffic will be passed or dropped to the respective tunnel endpoints. <p>For detailed information on filtering fragmented and unfragmented packets, refer to "GigaSMART Adaptive Packet Filtering (APF)" section on the <i>GigaVUE Fabric Management Guide</i>.</p> </div>

-  • Pass and Drop rule selection with Automatic Target Selection (ATS) differ with the Map type as follows:

 - Traffic Map—Only Pass rules for ATS
 - Inclusion Map—Only Pass rules for ATS
 - Exclusion Map—Only Drop rules for ATS

4. To reuse the map, click **Add to Library**. Save the map using one of the following ways:
- Select an existing group from the **Select Group** list or create a **New Group** with a name.
 - Enter a description in the **Description** field, and click **Save**.
5. Click **Save**.

NOTE: If a packet is fragmented then all the fragments will be destined to the same application end point. You can find the stats of mapped fragmented traffic in GigaVUE-FM. Refer to "Map Statistics" section in *GigaVUE Fabric Management Guide* for detailed information.

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

Add Applications to Monitoring Session

GigaVUE Cloud Suite with GigaVUE V Series Node supports the following GigaSMART applications in the GigaVUE-FM canvas:

- Application Visualization
- Application Filtering Intelligence
- Application Metadata Intelligence
- NetFlow
- Slicing
- Masking
- De-duplication
- Load Balancing
- Header Stripping
- SSL Decrypt

For more detailed information on how to configure these application, refer to *GigaVUE V Series Applications Guide*.

To deploy the monitoring session:

1. Drag and drop the following items to the canvas as required:
 - Maps from the **MAP LIBRARY** section
 - Inclusion and Exclusion maps from the Map Library to their respective section at the bottom of the workspace.
 - GigaSMART apps from the **APPLICATIONS** section
 - Egress tunnels from the **TUNNELS** section

- After placing the required items in the canvas, hover your mouse on the map, click the red dot, and drag the arrow over to another item (map, application, or tunnel).

NOTE: You can drag multiple arrows from a single map and connect them to different maps.

- Click **Show Targets** to view details about the subnets and monitored instances. The instances and the subnets that are being monitored are highlighted in orange.
- Click **Deploy** to deploy the monitoring session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on all the V Series nodes. Click on the status link in the Status column on the Monitoring Session page to view the Monitoring Session Deployment Report. When you click on the Status link, the Deployment Report is displayed. If the monitoring session is not deployed properly, then one of the following errors is displayed in the Status column.
 - Partial Success—The session is not deployed on one or more instances due to V Series node failure.
 - Failure—The session is not deployed on any of the V Series nodes. The **Monitoring Session Deployment Report** displays the errors that appeared during deployment.

The Monitoring Session page also has the following buttons:

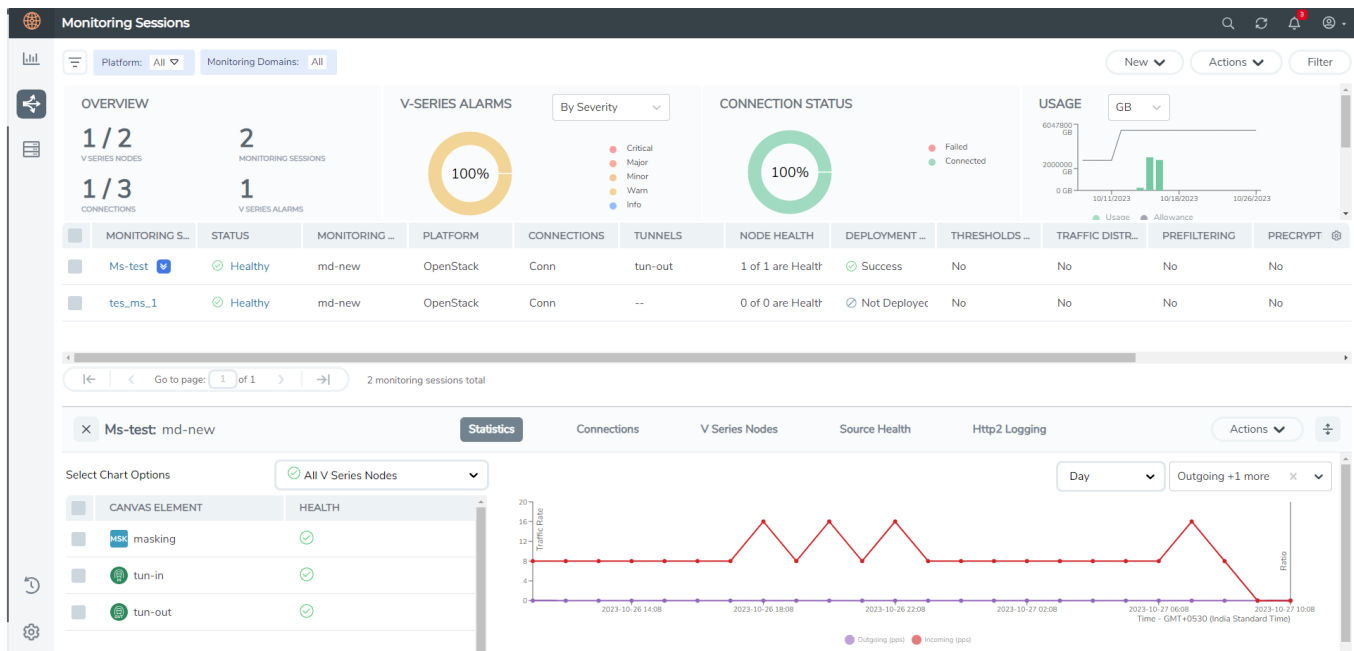
Button	Description
Undeploy	Undeploys the selected monitoring session.
Clone	Duplicates the selected monitoring session.

Button	Description
Edit	Opens the Edit page for the selected monitoring session. NOTE: In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again.
Delete	Deletes the selected monitoring session.

View Monitoring Session Statistics

The Monitoring Session Statistics page lets you analyze the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis.

On the Monitoring Sessions page, click the name of the monitoring session, and then click **View**. A split window appears displaying the **Statistics, Connections, V Series Nodes, Source Health** and **Http2 Logging** of the monitoring session as shown:



To know more about the statistics of the session, click **Statistics**.

You can view the statistics by applying different filters as per the requirements of analysing the data. GigaVUE-FM allows you to perform the following actions on the Monitoring Session Statistics page:

- You can view the **Statistics** in full screen. To view in full screen, click the **Actions** drop-down list at the right corner of the window, and select **Full Screen. Statistics** appear in full screen.
- You can view the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. You can select the options from the drop-down list box.
- You can filter the traffic and view the statistics based on factors such as **Incoming, Outgoing, Ratio (Out/In), Incoming Packets, Outgoing Packets, Ratio (Out/In) Packets**. You can select the options from the drop-down list box.
- You can also view the statistics of the monitoring session deployed in the individual V Series Nodes. To view the statistics of the individual V Series Node, select the name of the **V Series Node** from the drop-down list for which you want to view the statistics from the V Series node drop-down menu on the top left corner of the Monitoring Session Statistics page.
- You can view the statistics of the elements involved in the monitoring session. To view the statistics, click on the **Select Chart Options** page and select the elements associated with the session.
- Directly on the graph, you can click on **Incoming(Mbps), Outgoing (Mbps), or Ratio (Out/In) (Mbps)** to view the statistics individually.



Raw EndPoint (REP) is a part of the monitoring session but can also receive the bypassed traffic that is not filtered by the map, so it is recording more packets than expected. For example, if the map has a rule as IPv4, but the REP can receive the bypassed (non-ipv4) traffic. The recorded number of packets from the V Series node can be more than expected.

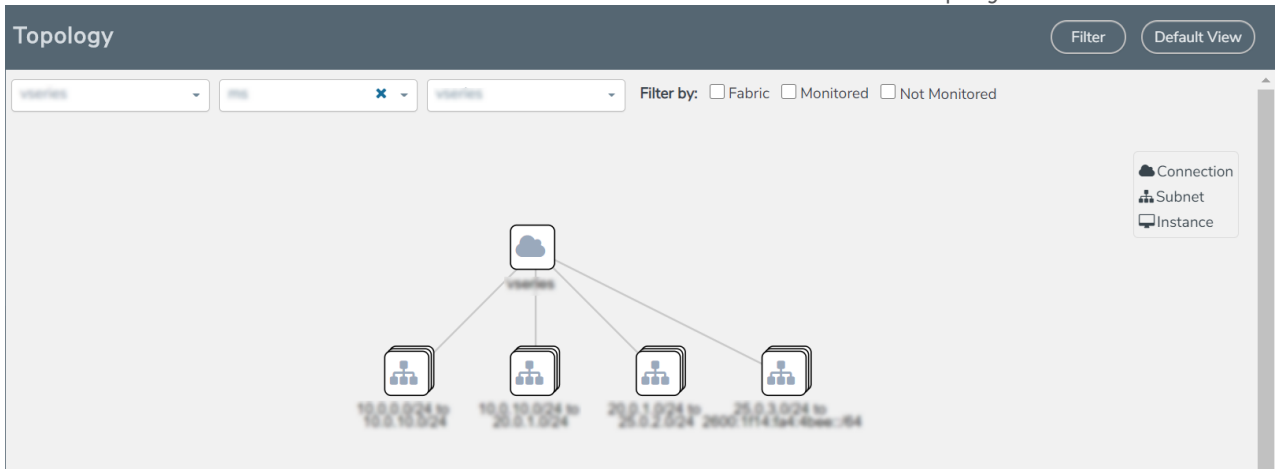
Visualize the Network Topology

You can have multiple connections in GigaVUE-FM. Each connection can have multiple monitoring sessions configured within them. You can select the connection and the monitoring session to view the selected subnets and instances in the topology view.

To view the topology diagram in GigaVUE-FM:

1. On the Monitoring Session page, select **Topology** tab. The Topology page appears.
2. Select a monitoring domain from the **Select monitoring domain...** list.
3. Select a connection from the **Select monitoring session...**list.

- Select a monitoring session from the **Select connection...** list. The topology view of the monitored subnets and instances in the selected session are displayed.



- (Optional) Hover over or click the subnet or VM Group icons to view the subnets or instances present within the group.

In the topology page, you can also do the following:

- Use the **Filter** button to filter the instances based on the VM name, VM IP, Subnet ID, or Subnet IP, and view the topology based on the search results.
- Use the **Default View** button to view the topology diagram based on the source interfaces of the monitoring instances.
- Use the arrows at the right-bottom corner to move the topology page up, down, left, or right. Click the **Fit-to-Width** icon to fit the topology diagram according to the width of the page.
- Use **+** or **-** icons to zoom in and zoom out the topology view.

Cloud Health Monitoring - Configuration Health Monitoring

GigaVUE-FM allows you to monitor the configuration health status of the entire monitoring session and also the individual fabric components for which monitoring session is configured. This feature provides detailed information about the configuration and deployment status of the deployed monitoring session.

This feature is supported for the following fabric components and features on the respective cloud platforms:

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware
- Nutanix

For UCT-Vs:

- AWS
- Azure
- OpenStack

For VPC Mirroring:

- AWS

For OVS Mirroring and VLAN Trunk Port:

- OpenStack

View Monitoring Session Configuration Health

You can view the configuration status of the monitoring session and the components deployed, in the monitoring session page. This section provides information about the configuration health status of the various fabric components deployed in the monitoring session.

The following columns in the monitoring session page are used to convey the configuration health status:

Health

This column displays the configuration health status of the entire monitoring session.

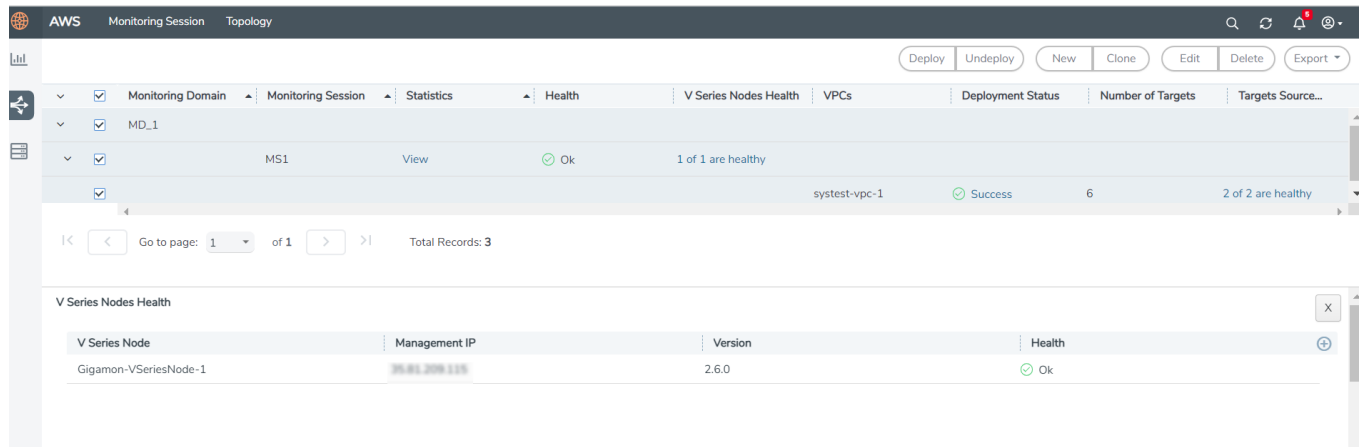
The error message associated with monitoring session configuration appears when you hover over the health column. You can use the error message to help you troubleshoot and identify the components that are in conflict or mis-configured.

V Series Node Health

This column displays the configuration health status of the monitoring session deployed in V Series Nodes. This column provides information on the number of monitoring sessions successfully deployed on a particular V Series Node to the total number of monitoring session deployed on that particular V Series Node.

You can view the health status of the individual V Series Nodes and also the error message associated with them, by clicking on the V Series Node Health column.

NOTE: V Series node health only displays the configuration health status therefore even if the V Series Node is down it will not be reflected in the monitoring session page.



Target Source Health

This column displays the configuration health status of the monitoring session deployed in targets. This column provides information on the number of monitoring sessions successfully deployed on a particular target to the total number of monitoring session deployed on that particular target.

You can view the health status of the individual targets and also the error message associated with them, by clicking on the Target Source Health column.

View Monitoring Session Statistics

You can now view the statistics of the monitoring session deployed in the individual V Series Nodes. To view the statistics of the individual V Series Node, select the name of the V Series Node for which you want to view the statistics from the V Series Node drop-down menu on the top left-corner of the Monitoring Session Statistics page.

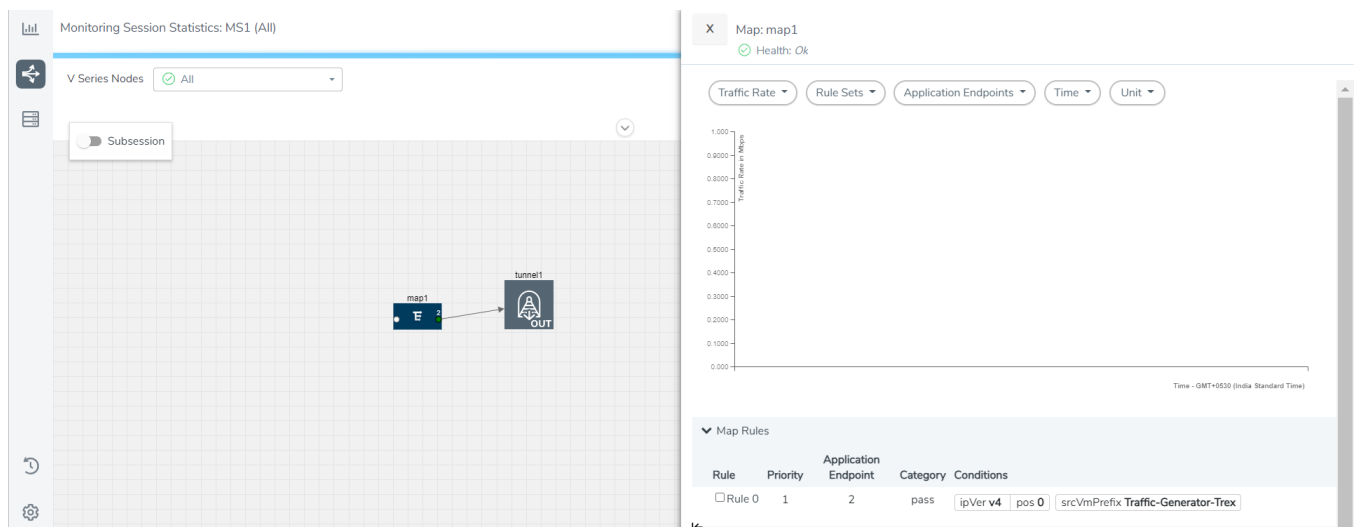
Hover over the V Series Node drop-down to view the number of the applications, end points, and other application environments configured for a particular V Series Node. It also displays the error message related to configuration for the particular V Series Node.

View Monitoring Session Diagram

The Monitoring Session diagram page displays the applications and end points deployed in a particular monitoring session in pictorial form. To view the statistics of a particular application or an endpoint, click on the application icon for which you want to view the statistics. You can also view the statistics of a particular application for an individual V Series Node by selecting the name of the V Series Node for which you want to view the statistics from the V Series Node drop-down menu on the top left-corner of the Monitoring Session page.

When you select a V Series Node from the V Series Node drop-down, the application icon displays the name of that particular application as configured in the V Series Node.

The subsession toggle button available in the top-left corner of the canvas allows you to view the statistics of individual paths in the monitoring session.



Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics¹ you can create visual elements such as charts that are embedded as visualizations. The visualizations are grouped together in dashboards. You can also create search objects using Analytics. Dashboards, Visualizations and Search Objects are called Analytics objects. Refer to [Analytics](#) topic in *GigaVUE Fabric Management Guide* for more detailed information on Analytics.

Rules and Notes:


¹Analytics uses the OpenSearch front-end application to visualize and analyze the data in the OpenSearch database of GigaVUE-FM.

- You cannot edit or delete these default dashboards. However, you can clone the dashboards and visualizations. Refer to the [Clone Dashboard](#) section for more details.
- Use the Time Filter option to select the required time interval for which you need to view the visualization.

Virtual Inventory Statistics and Cloud Applications Dashboard

Analytics dashboards allow users to monitor the physical and virtual environment and detect anomalous behavior and plan accordingly. Refer to the [Analytics](#) section in *GigaVUE Fabric Management Guide* for details on how to create a new dashboard, clone a dashboard, create a new visualization, and other information about the Discover page and Reports page.

To access the dashboards:

1. Go to  -> **Analytics -> Dashboards**.
2. Click on the required dashboard to view the visualizations.

The following table lists the various virtual dashboards:

Dashboard	Displays	Visualizations	Displays
Inventory Status (Virtual)	Statistical details of the virtual inventory based on the platform and the health status. You can view the following metric details at the top of the dashboard: <ul style="list-style-type: none"> • Number of Monitoring Sessions • Number of V Series Nodes • Number of Connections • Number of GCB Nodes You can filter the visualizations based on the following control filters: <ul style="list-style-type: none"> • Platform • Health Status 	<i>V Series Node Status by Platform</i>	Number of healthy and unhealthy V Series Nodes for each of the supported cloud platforms.
		<i>Monitoring Session Status by Platform</i>	Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms
		<i>Connection Status by Platform</i>	Number of healthy and unhealthy connections for each of the supported cloud platforms
		<i>GCB Node Status by Platform</i>	Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms
V Series Node Statistics	Displays the Statistics of the V Series node such as the CPU usage, trend of the	<i>V Series Node Maximum CPU Usage Trend</i>	Line chart that displays maximum CPU usage trend of

Dashboard	Displays	Visualizations	Displays
	<p>receiving and transmitting packets of the V Series node.</p> <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> • Platform • Connection • V Series Node 		<p>the V Series node in 5 minutes interval, for the past one hour.</p> <div data-bbox="1170 401 1468 709" style="border: 1px solid #ccc; padding: 5px;"> <p>NOTE: The maximum CPU Usage trend refers to the CPU usage for service cores only. Small form factor V-series nodes do not have service cores, therefore the CPU usage is reported as 0.</p> </div>
		<p><i>V Series Node with Most CPU Usage For Past 5 minutes</i></p>	<p>Line chart that displays Maximum CPU usage of the V Series node for the past 5 minutes.</p> <div data-bbox="1170 940 1468 1087" style="border: 1px solid #ccc; padding: 5px;"> <p>NOTE: You cannot use the time based filter options to filter and visualize the data.</p> </div>
		<p><i>V Series Node Rx Trend</i></p>	<p>Receiving trend of the V Series node in 5 minutes interval, for the past one hour.</p>
		<p><i>V Series Network Interfaces with Most Rx for Past 5 mins</i></p>	<p>Total packets received by each of the V Series network interface for the past 5 minutes.</p> <div data-bbox="1170 1507 1468 1654" style="border: 1px solid #ccc; padding: 5px;"> <p>NOTE: You cannot use the time based filter options to filter and visualize the data.</p> </div>
		<p><i>V Series Node Tunnel Rx Packets/Errors</i></p>	<p>Displays the reception of packet at the Tunnel RX. This is the input to V Series Node, Grouping</p>

Dashboard	Displays	Visualizations	Displays
			by tunnel identifier comprising {monDomain, conn, VSN, tunnelName}, before aggregation.
		<i>V Series Node Tunnel Tx Packets/Errors</i>	TX is for output tunnels from VSN. V Series Node Tunnel Tx Packets/Errors
Dedup	<p>Displays visualizations related to Dedup application.</p> <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> • Platform • Connection • VSeries Node 	<i>Dedup Packets Detected/Dedup Packets Overload</i>	Statistics of the total dedup packets received (ipV4Dup, ipV6Dup and nonIPDup) against the dedup application overload.
		<i>Dedup Packets Detected/Dedup Packets Overload Percentage</i>	Percentage of the dedup packets received against the dedup application overload.
		<i>Total Traffic In/Out Dedup</i>	Total incoming traffic against total outgoing traffic
Tunnel (Virtual)	<p>Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets.</p> <p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> • Monitoring session: Select the required monitoring session. The cloud platform, monitoring domain and connection within the monitoring domain that is used by the V-series node are shown in square brackets, comma-separated, after the name, to distinguish the whole path to it. • V series node: Management IP of the V Series node. Choose the required V-series node from the drop-down. 	<i>Tunnel Bytes</i>	<p>Displays received tunnel traffic vs transmitted tunnel traffic, in bytes.</p> <ul style="list-style-type: none"> • For input tunnel, transmitted traffic is displayed as zero. • For output tunnel, received traffic is displayed as zero.

Dashboard	Displays	Visualizations	Displays
	<ul style="list-style-type: none"> • Tunnel: Select any of the tunnels shown in the Tunnel drop-down. The direction for each tunnel is shown with the prefix in or out. <p>The following statistics are displayed for the tunnel:</p> <ul style="list-style-type: none"> • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets • Received Dropped Packets • Transmitted Errored Packets • Transmitted Dropped Packets 		
		<i>Tunnel Packets</i>	Displays packet-level statistics for input and output tunnels that are part of a monitoring session.
App (Virtual)	<p>Displays Byte and packet level statistics for the applications for the chosen monitoring session on the selected V series node.</p> <p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> • Monitoring session • V series node • Application: Select the required application. By default, the visualizations displayed includes all the applications. <p>By default, the following statistics are displayed:</p> <ul style="list-style-type: none"> • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Errored Packets • Dropped Packets 	<i>App Bytes</i>	Displays received traffic vs transmitted traffic, in Bytes.

Dashboard	Displays	Visualizations	Displays
		<i>App Packets</i>	Displays received traffic vs transmitted traffic, as the number of packets.
End Point (Virtual)	<p>Displays Byte and packet level statistics for the un-tunneled traffic deployed on the V-series nodes.</p> <p>The following statistics that are shown for Endpoint (Virtual):</p> <ul style="list-style-type: none"> • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets • Received Dropped Packets • Transmitted Errored Packets • Transmitted Dropped Packets <p>The endpoint drop-down shows <i><V-series Node Management IP address : Network Interface></i> for each endpoint.</p> <p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> • Monitoring session • V Series node • Endpoint: Management IP of the V Series node followed by the Network Interface (NIC) 	<i>Endpoint Bytes</i>	Displays received traffic vs transmitted traffic, in Bytes.
		<i>Endpoint Packets</i>	Displays received traffic vs transmitted traffic, as the number of packets.

NOTE: The Tunnel (Virtual), App (Virtual) and Endpoint (Virtual) dashboards do not show data from the previous releases if the *Monitoring Session [Platform : Domain : Connection]* dashboard filter is applied. This is because, this filter relies on the new attributes in the OpenSearch database, which are available only from software version 5.14.00 and beyond.

Administer GigaVUE Cloud Suite for Nutanix

You can perform the following administrative tasks in GigaVUE-FM for GigaVUE Cloud Suite for Nutanix:

- [Configure Nutanix Settings](#)
- [Role Based Access Control](#)
- [About Events](#)
- [About Audit Logs](#)

Configure Nutanix Settings

To configure the Nutanix Settings:

1. Go to **Inventory > VIRTUAL > Nutanix** and then click **Settings**. The Settings page appears.
2. Click **Advanced** tab on the Settings page, click **Edit** to edit the Settings fields. Refer to the following table for descriptions of the Settings fields:

Settings	Description
Maximum number of connections allowed	Specifies the maximum number of connections you can establish in GigaVUE-FM.
Refresh interval for VM target selection inventory (secs)	Specifies the frequency for updating the state of target VMs in Nutanix.
Traffic distribution tunnel range start	Specifies the start range value of the tunnel ID.
Traffic distribution tunnel range end	Specifies the closing range value of the tunnel ID.

Role Based Access Control

The Role Based Access Control (RBAC) feature controls the access privileges of users and restricts users from either modifying or viewing unauthorized data. Access privileges in GigaVUE Cloud Suite works on the same principles of access privileges in GigaVUE-FM in which the access rights of a user depends on the following:

- **User role:** A user role defines permission for users to perform any task or operation
- **User group:** A user group consists of a set of roles and set of tags associated with that group. When a user is created they can be associated with one or more groups.

To access the resources and to perform a specific operation in GigaVUE Cloud Suite you must be a user with **fm_super_admin** role or a user with write access to the following resource category depending on the task you need to perform.

Resource Category	Cloud Configuration Task
<p>Physical Device Infrastructure Management: This includes the following cloud infrastructure resources:</p> <ul style="list-style-type: none"> • Cloud Connections • Cloud Fabric Deployment • Cloud Configurations • Sys Dump • Syslog • Cloud licenses • Cloud Inventory 	<ul style="list-style-type: none"> • Configure GigaVUE Cloud Components • Create Monitoring Domain and Launch Visibility Fabric
<p>Traffic Control Management: This includes the following traffic control resources:</p> <ul style="list-style-type: none"> • Monitoring session • Stats • Map library • Tunnel library • Tools library • Inclusion/exclusion Maps 	<ul style="list-style-type: none"> • Create, Clone, and Deploy Monitoring Session • Add Applications to Monitoring Session • Create Maps • View Statistics • Create Tunnel End Points

NOTE: Cloud APIs are also RBAC enabled.

Refer to the *GigaVUE Administration Guide* for detailed information about Roles, Tags, User Groups.

About Events

The Events page displays all the events occurring in the virtual fabric node, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

- Cloud provider License Expiry
- UCT-V Inventory Update Completed

- Cloud provider Connection Status Changed

An Alarm is a response to one or more related events. If an event is considered of high severity, then GigaVUE-FM raises an alarm. An example of alarm could be your cloud provider license expiry.

The alarms and events broadly fall into the following categories: Critical, Major, Minor, or info.

Navigate to **Dashboard > SYSTEM > Events**. The Event page appears.

Source	Time	Event Type	Severity	Affected Entity T...	Affected Entity	Alias	Device IP	Host Name	Scope	Description	Tags
FM	2022-08-10 0...	Licenses Expir...	Info	Floating License					FM	4 Floating	
FM	2022-08-09 0...	Licenses Expir...	Info	Floating License					FM	4 Floating	
FM	2022-08-08 0...	Licenses Expir...	Info	Floating License					FM	4 Floating	
FM	2022-08-07 0...	Licenses Expir...	Info	Floating License					FM	4 Floating	
FM	2022-08-06 0...	Licenses Expir...	Info	Floating License					FM	4 Floating	
FM	2022-08-05 1...	FM Applicatio...	Info	fm application ...				fmha1	fmService	CMS service f...	
FM	2022-08-04 1...	FM Applicatio...	Info	fm application ...				fmha1	fmService	CMS service f...	
FM	2022-08-04 1...	Alarm Delete ...	Critical	VSeries Node	vc-obc-pod2.u...				Alarm	Node Down. P...	

The following table describes the parameters recording for each alarm or event. You can also use filters to narrow down the results.

Controls/ Parameters	Description
Source	The source from where the events are generated. The criteria can be as follows: <ul style="list-style-type: none"> ▪ FM - indicates the event was flagged by the Fabric Manager. ▪ IP address - is the address of the GigaVUE HC Series node that detected the event. For a node to be able to send notifications to the Fabric Manager, the SNMP_TRAP must be configured with the Fabric Manager's IP address specified as a host. Refer to the GigaVUE Administration Guide for instructions on adding a destination for SNMP traps. ▪ VMM - indicates the event was flagged by the Virtual Machine Manager. ▪ FM Health - indicates the event was flagged due to the health status change of GigaVUE-FM.
Time	The timestamp when the event occurred. IMPORTANT: Timestamps are shown in the time zone of the client browser's computer and not the time zone of the node reporting the event. The timestamp is based on the correctly configured clock on the GigaVUE-FM server and converted from UTC to the client computer's configured time zone.
Event Type	The type of event that generated the events. The type of events can be CPU utilization high, cluster updated, device discovery failed, fan tray changed, netflow statistics, and so on.
Severity	The severity is one of Critical, Major, Minor, or Info. Info is informational messages. For example, when power status change

Controls/ Parameters	Description
	notification is displayed, then the message is displayed as Info.
Affected Entity Type	The resource type associated with the event. For example, when low disk space notification is generated, 'Chassis' is displayed as the affected entity type.
Affected Entity	The resource ID of the affected entity type. For example, when low disk space notification is generated, the IP address of the node with the low disk space is displayed as the affected entity.
Alias	Event Alias
Device IP	The IP address of the device.
Host Name	The host name of the device.
Scope	The category to which the events belong. Events can belong to the following category: Domain, Node, Card, Port, Stack, Cluster, Chassis, GigaVUE-FM, GigaVUE-VM, and so on. For example, if there is a notification generated for port utilization low threshold, the scope is displayed as Physical Node.

To filter the alarms and event:

1. Click **Filter**. The Filter quick view is displayed.
2. Select the filtering criteria, then click **Apply Filter**. The results are displayed in the Events page.

About Audit Logs

Audit logs track the changes and activities that occur in the virtual nodes due to user actions. The logs can be filtered to view specific information.

Navigate to **Dashboard > SYSTEM > Audit Logs**. The **All Audit Logs** page appears.

All Audit Logs Filter Manage

Filter : none

Time	User	Operation Type	Entity Type	Source	Device IP	Hostname	Status	Description	Tags
2020-1...	admin	login fmUser ad...	User	fm			SUCCESS		
2020-1...	admin	logout fmUser a...	User	fm			SUCCESS		
2020-1...	admin	login fmUser ad...	User	fm			SUCCESS		
2020-1...	admin	update monitor...	Monitor...				SUCCESS		

⏪ ⏩ Go to page: of 16 ⏪ ⏩ Total Records: 106

The Audit Logs have the following parameters:

Parameters	Description
Time	Provides the timestamp on the log entries.
User	Provides the logged user information.
Operation Type	Provides specific entries that are logged by the system such as: <ul style="list-style-type: none"> Log in and Log out based on users. Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.
Source	Provides details on whether the user was in FM or on the node when the event occurred.
Status	Success or Failure of the event.
Description	In the case of a failure, provides a brief update on the reason for the failure.

NOTE: Ensure that the GigaVUE-FM time is set correctly to ensure accuracy of the trending data that is captured.

Filtering the audit logs allows you to display specific type of logs. You can filter based on any of the following:

- **When:** display logs that occurred within a specified time range.
- **Who:** display logs related a specific user or users.
- **What:** display logs for one or more operations, such as Create, Read, Update, and so on.
- **Where:** display logs for GigaVUE-FM or devices.
- **Result:** display logs for success or failure.

To filter the audit logs, do the following:

1. Click **Filter**. The quick view for Audit Log Filters displays.
2. Specify any or all of the following:
 - **Start Date** and **End Date** to display logs within a specific time range.
 - **Who** limits the scope of what displays on the Audit Logs page to a specific user or users.
 - **What** narrows the logs to the types of operation that the log is related to. You can select multiple operations. Select **All Operations** to apply all operation types as part of the filter criteria.
 - **Where** narrows the logs to particular of system that the log is related to, either FM or device. Select **All Systems** apply both FM and device to the filter criteria.
 - **Result** narrows the logs related to failures or successes. Select All Results to apply both success and failure to the filter criteria.

3. Click **OK** to apply the selected filters to the Audit Logs page.

Additional Sources of Information

This appendix provides additional sources of information. Refer to the following sections for details:

- [Documentation](#)
- [Documentation Feedback](#)
- [Contact Technical Support](#)
- [Contact Sales](#)
- [The VUE Community](#)

Documentation

This table lists all the guides provided for GigaVUE Cloud Suite software and hardware. The first row provides an All-Documents Zip file that contains all the guides in the set for the release.

NOTE: In the online documentation, view [What's New](#) to access quick links to topics for each of the new features in this Release; view [Documentation Downloads](#) to download all PDFs.

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.5 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>
<p>Hardware</p> <p>how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices</p>
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 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 Cloud Suite 6.5 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-OS Installation Guide for DELL S4112F-ON	
G-TAP A Series 2 Installation Guide	
GigaVUE M Series Hardware Installation Guide	
GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW	
Software Installation and Upgrade Guides	
GigaVUE-FM Installation, Migration, and Upgrade Guide	
GigaVUE-OS Upgrade Guide	
GigaVUE V Series Migration Guide	
Fabric Management and Administration Guides	
GigaVUE Administration Guide	covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide	how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
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 V Series Quick Start Guide	
GigaVUE Cloud Suite Deployment Guide - AWS	
GigaVUE Cloud Suite Deployment Guide - Azure	
GigaVUE Cloud Suite Deployment Guide - OpenStack	
GigaVUE Cloud Suite Deployment Guide - Nutanix	
GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)	
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)	
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration	

GigaVUE Cloud Suite 6.5 Hardware and Software Guides

Universal Cloud Tap - Container Deployment Guide

Gigamon Containerized Broker Deployment Guide

GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide

GigaVUE Cloud Suite Deployment Guide - AWS 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 TA Series devices

GigaVUE-OS Security Hardening Guide

GigaVUE Firewall and Security Guide

GigaVUE Licensing Guide

GigaVUE-OS Cabling Quick Reference Guide

guidelines for the different types of cables used to connect Gigamon devices

GigaVUE-OS Compatibility and Interoperability Matrix

compatibility information and interoperability requirements for Gigamon devices

GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide

samples uses of the GigaVUE-FM Application Program Interfaces (APIs)

Release Notes

GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes

new features, resolved issues, and known issues in this release ;
important notes regarding installing and upgrading to this release

NOTE: Release Notes are not included in the online documentation.

NOTE: Registered Customers can log in to [My Gigamon](#) to download the Software and Release Notes from the Software & Docs page on to [My Gigamon](#). Refer to [How to Download Software and Release Notes from My Gigamon](#).

In-Product Help

GigaVUE-FM Online Help

how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Release Notes** page on to [My Gigamon](#). Use the My Gigamon Software & Docs page to download:

- Gigamon Software installation and upgrade images,
- Release Notes for Gigamon Software, or
- Older versions of PDFs (pre-v5.7).

To download release-specific software, release notes, or older PDFs:

1. Log in to [My Gigamon](#)
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.6.xx.

NOTE: My Gigamon is available to registered customers only. Newer documentation PDFs, with the exception of release notes, are all available through the publicly available online documentation.

Documentation Feedback

We are continuously improving our documentation to make it more accessible while maintaining accuracy and ease of use. Your feedback helps us to improve. To provide feedback and report issues in our documentation, send an email to:

documentationfeedback@gigamon.com

Please provide the following information in the email to help us identify and resolve the issue. Copy and paste this form into your email, complete it as able, and send. We will respond as soon as possible.

Documentation Feedback Form		
About You	Your Name	
	Your Role	
	Your Company	

For Online Topics	Online doc link	<i>(URL for where the issue is)</i>
	Topic Heading	<i>(if it's a long topic, please provide the heading of the section where the issue is)</i>
For PDF Topics	Document Title	<i>(shown on the cover page or in page header)</i>
	Product Version	<i>(shown on the cover page)</i>
	Document Version	<i>(shown on the cover page)</i>
	Chapter Heading	<i>(shown in footer)</i>
	PDF page #	<i>(shown in footer)</i>
How can we improve?	Describe the issue	<i>Describe the error or issue in the documentation. (If it helps, attach an image to show the issue.)</i>
	How can we improve the content? Be as specific as possible.	
	Any other comments?	

Contact Technical Support

For information about Technical Support: Go to **Settings**  **> Support > Contact Support** in GigaVUE-FM.

You can also refer to <https://www.gigamon.com/support-and-services/contact-support> for Technical Support hours and contact information.

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to contact Gigamon channel partner or Gigamon sales representatives:

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

Email Gigamon at inside.sales@gigamon.com for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

The VÜE Community

The **VÜE Community** is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the VÜE 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)