Gigamon®

GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)

GigaVUE Cloud Suite

Product Version: 6.10

Document Version: 1.0

(See Change Notes for document updates.)

Trademark Attributions

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
6.10	1.0	03/07/2025	The original release of this document with 6.10.00 GA.

Contents

GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)

GigaVUE Cloud Suite for VMware provides an intelligent filtering technology that allows virtual machine (VM) traffic flows of interest to be selected, forwarded, and delivered to the monitoring infrastructure centrally attached to the Gigamon Deep Observability Pipeline, thereby eliminating any traffic blind spots in the enterprise private clouds or service provider NFV deployments.

This guide describes how to install, deploy, and operate the GigaVUE V Series Nodes in VMware.

Refer to the following topics for more detailed information:

- Overview of GigaVUE Cloud Suite for VMware
- Architecture for GigaVUE Cloud Suite for VMware ESXi
- Points to Note (VMware vCenter)
- Volume-Based License
- Supported Hypervisors for VMware
- Introduction to Supported Features for GigaVUE Cloud Suite for VMware ESXi
- Prerequisites for Integrating V Series Nodes with VMware vCenter
- Install and Upgrade GigaVUE-FM
- Deploy GigaVUE Cloud Suite for VMware (ESXi)
- Configure Monitoring Session
- Migrate Application Intelligence Session to Monitoring Session
- Monitor Cloud Health
- Configure VMware Settings
- Analytics for Virtual Resources

Overview of GigaVUE Cloud Suite for VMware

GigaVUE Cloud Suite for VMware acquires, optimizes, and distributes selected traffic to your monitoring and security tools. GigaVUE Cloud Suite for VMware provides tight integration with orchestration tools to deliver intelligent network traffic visibility for workloads running in Virtual machine in VMware. GigaVUE-FM , part of the Cloud Suite, works with VMware vCenter to automatically deploy GigaVUE V Series Node to support a growing private cloud infrastructure. GigaVUE-FM leverages dynamic service chaining and workload relocation monitoring to ensure visibility and policy integrity.

GigaVUE Cloud Suite for VMware provides the following benefits:

Flexible Traffic Acquisition: Acquires traffic through port mirroring in VMware ESXi.

Automated Visibility Provisioning: Dynamically provisions and applies traffic policies as new tenants come on board or as groups scale.

Increased Tool Efficiency: Reduces load on tools by selectively filtering, de-duplicating, and load balancing traffic sent to security and performance monitoring tools.

Application Intelligence solution: You can use Application Intelligence to identify thousands of applications and utilize over 7,000 application metadata elements.

Components for GigaVUE Cloud Suite for VMware

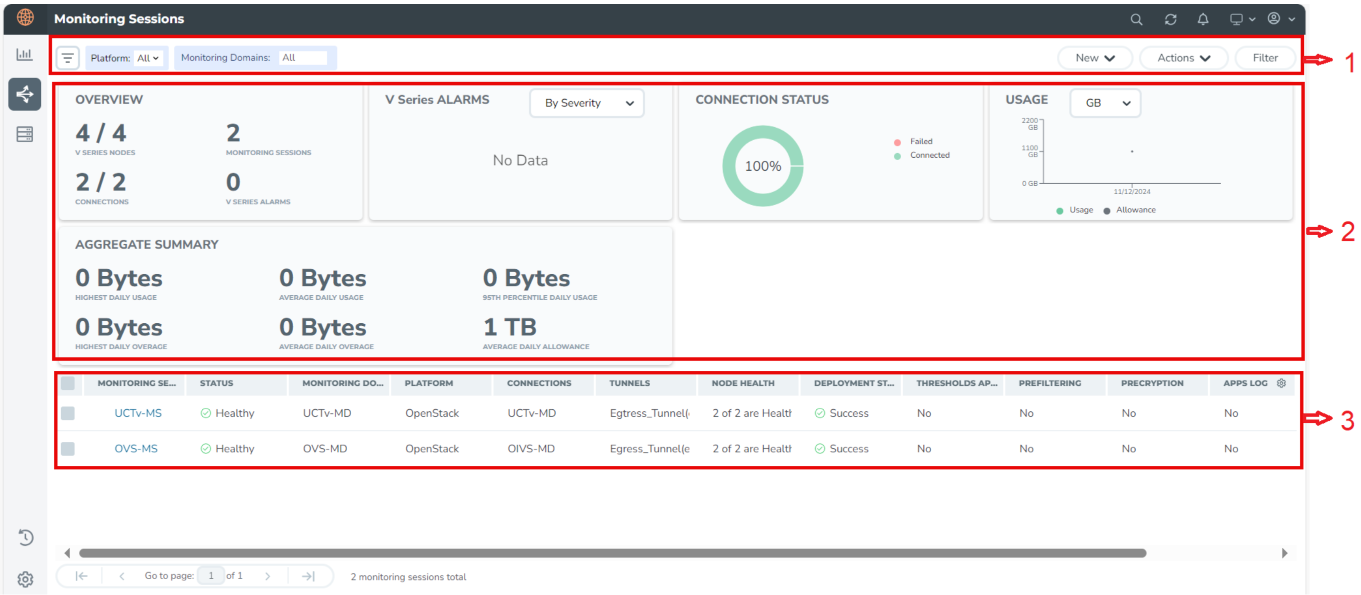
GigaVUE Cloud Suite for VMware comprises multiple elements that enable traffic acquisition, aggregation, intelligence and distribution, along with centralized, single-pane-of-glass orchestration and management. The solution consists of these components:

Component	Description
GigaVUE-FM fabric manager (GigaVUE-FM)	GigaVUE-FM is a web-based fabric management and orchestration interface that provides a single pane of glass visibility, management, and orchestration of both the physical and virtual traffic that form the GigaVUE Cloud Suite Cloud Suite for VMware. GigaVUE-FM generates an end-to-end topology view through a single-pane-of-glass GUI, which gives you insights into which cloud instances are or are not part of the deep observability pipeline. A single instance of GigaVUE-FM can manage hundreds of visibility nodes across on-premises and multi-cloud environments. GigaVUE-FM manages the configuration of the rest of the components in your cloud platform.
GigaVUE® V Series Node	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 back haul to on premise device or tools.

Cloud Overview Page (VMware)

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.

To view the overall cloud overview page, go to **Traffic > Virtual > Overview**.



OVERVIEW

4 / 4 V SERIES NODES

2 MONITORING SESSIONS

2 / 2 CONNECTIONS

0 V SERIES ALARMS

AGGREGATE SUMMARY

0 Bytes HIGHEST DAILY USAGE

0 Bytes AVERAGE DAILY USAGE

0 Bytes 95TH PERCENTILE DAILY USAGE

0 Bytes HIGHEST DAILY OVERAGE

0 Bytes AVERAGE DAILY OVERAGE

1 TB AVERAGE DAILY ALLOWANCE

MONITORING SE...	STATUS	MONITORING DO...	PLATFORM	CONNECTIONS	TUNNELS	NODE HEALTH	DEPLOYMENT ST...	THRESHOLDS AP...	PREFILTERING	PRECRYPTION	APPS LOG
UCTv-MS	Healthy	UCTv-MD	OpenStack	UCTv-MD	Egtress_Tunnel(	2 of 2 are Healtl	Success	No	No	No	No
OVS-MS	Healthy	OVS-MD	OpenStack	OIVS-MD	Egress_Tunnel(e	2 of 2 are Healtl	Success	No	No	No	No

Go to page: 1 of 1

2 monitoring sessions total

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

Number	Section	Description
1	Top Menu	Refer to Top Menu.
2	Charts	Refer to Viewing Charts.
3	Monitoring Session Details	In the Overview page, you can view the Monitoring Session details of all the cloud platforms. Refer to Viewing Monitoring Session Details section for more details.

Top Menu

The Top menu consists of the following options:

Options	Description
New	You can create a new Monitoring Session and new Monitoring Domain.
Actions	You can do the following actions using the **Action** button: **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** - Undeploys the selected Monitoring Session. **Apply Threshold** - Applies the threshold template created for monitoring cloud traffic health. Refer to *Monitor Cloud* section for details.
Filter	You can filter the Monitoring Session details based on a criterion or combination of criteria. For more information, refer to Filters.

Filters

You can apply the filters on the Monitoring Sessions page in the below two ways:

- Filter on the left corner
- Filter on the right corner

Filter on the left corner ≡

1. Select the required platform from the **Platform** drop- down list.
2. Click ≡ and select the Monitoring Domain.

You can select one or multiple domains. You can also edit and create a new Monitoring Domain in the filter section.

Filter on the right corner Filter

You can filter Monitoring Session and Monitoring Domain details 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
- 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, 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 quickly view the V Series alarms generated. 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

You can view the following details in the overview table:

Details	Description
Monitoring Sessions	Name of the Monitoring Session. When you click the name of the session, you will be redirected to the platform specific 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 status of the GigaVUE V Series Node.
Deployment Status	Status of the deployment.

Details	Description
Threshold Applied	Specifies whether the threshold is applied or not.
Prefiltering	Specifies whether Prefiltering is configured or not.
Precryption	Specifies whether Precryption is configured or not.
APPS logging	Specifies whether APPS logging is configured or not.
Traffic Mirroring	Specifies whether Traffic Mirroring is configured or not.

NOTE: Click the settings icon ⚙ to select the required options to appear in the table.

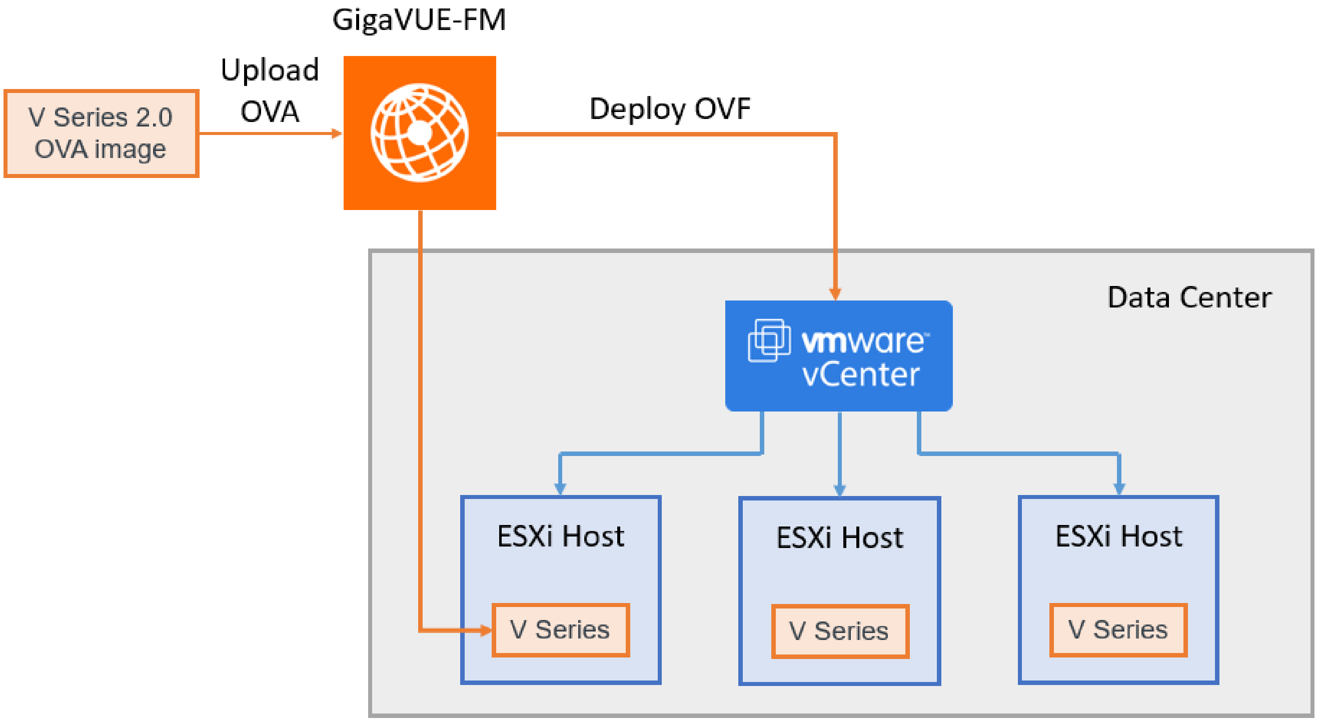
Architecture for GigaVUE Cloud Suite for VMware ESXi

This document provides an overview of the GigaVUE V Series Node deployment on the VMware ESXi platforms and describes the procedure for setting up the traffic monitoring sessions using the GigaVUE V Series Nodes. TheGigaVUE V Series Nodes support traffic visibility on the following VMware networking elements:

- vSphere standard switch
- vSphere distributed switch

GigaVUE-FM creates, updates, and deletes the GigaVUE V Series Nodes in the ESXi hosts based on the configuration information provided by the user. The VMs and GigaVUE V Series Nodes are located in the same ESXi host and the traffic mirrored from VMs is sent to GigaVUE V Series Nodes. You can deploy only one GigaVUE V Series Node on a single ESXi host. GigaVUE-FM can communicate directly with the GigaVUE V Series Nodes.

The following diagram provides a high-level overview of the deployment:



Points to Note (VMware vCenter)

1. These steps assume that VMware vCenter is installed and configured. Refer to VMware Documentation for configuration details.
2. Ensure the source Virtual Machine and the tool are connected to different Virtual Standard Switch. The traffic is looped, when the source Virtual Machine and the tool are connected in the same standard switch.
3. If NextGen Firewall (NGFW) with Deep Packet Inspection (DPI) is enabled to inspect your east-west traffic, expect an increase in latency due to mirrored traffic. To avoid increased latency, consider creating an exception rule for the tunneled traffic (mirrored traffic from the GigaVUE V Series Nodes to the tool) or configuring a private VDS that can bypass the NGFW rules for this traffic.
4. NSX Virtual Distributed Switch (N-VDS) based segments are not supported in **VMware vCenter** Monitoring Domain. N-VDS is supported only on NSX versions less or equal to 3.0. Refer to VMware Documentation for more detailed information.

Volume-Based License

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 GigaVUE 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 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 one month. Service period is the period of time for which the total usage or overage is tracked.

For purchasing licenses with the Volume-Based License (VBL) option, contact our 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 SKUs[1]. 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 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 a volume allowance less than the base bundle, then your add-on package can only handle the volume allocated for the 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

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

GigaVUE Cloud Suite for OpenStack
GigaVUE Cloud Suite for Nutanix
GigaVUE Cloud Suite for Kubernetes

How GigaVUE-FM Tracks Volume-Based License Usage

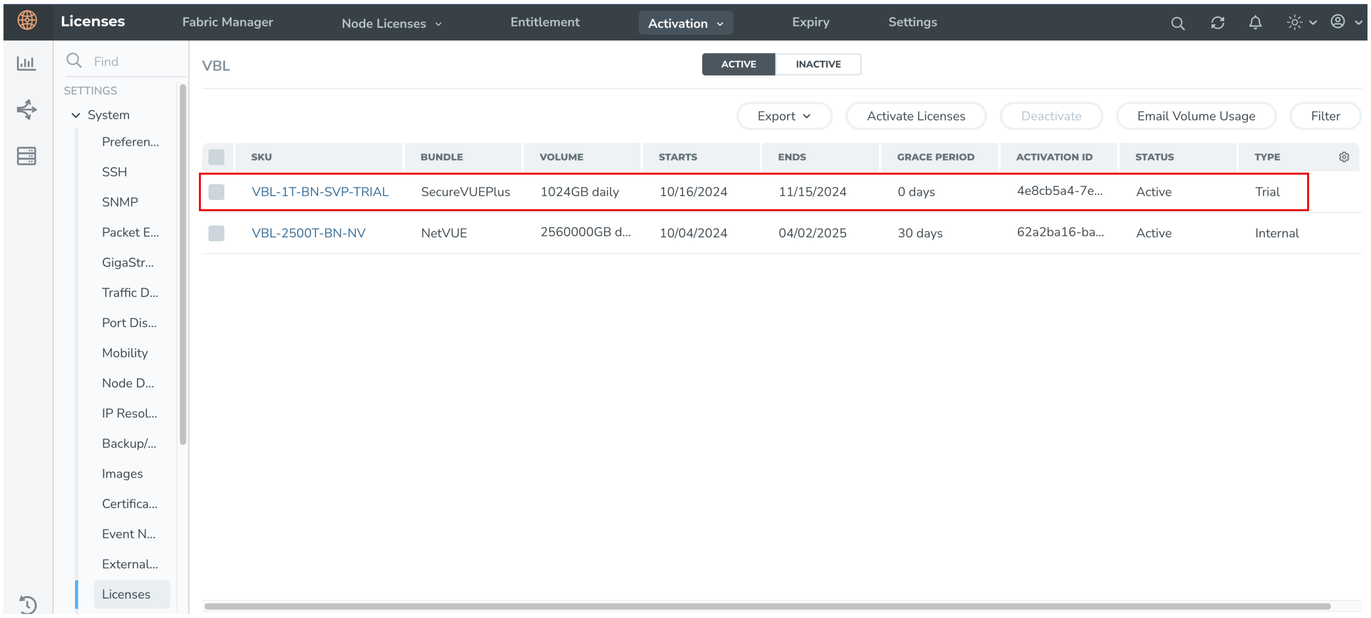
GigaVUE-FM tracks the license usage for each GigaVUE V Series Node as follows:

- 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).
- When a license expires, you will be notified with an audit log. Refer to the *About Audit Logs* section in the respective GigaVUE Cloud Suite Deployment Guide.
- 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.

> **NOTE:** When the license expires, GigaVUE-FM displays a notification on the screen.

Default Trial Licenses

After you install GigaVUE-FM, you will receive a one-time, free 1TB SecureVUE Plus trial Volume-Based License (VBL) for 30 days, starting from the installation date.



SKU	BUNDLE	VOLUME	STARTS	ENDS	GRACE PERIOD	ACTIVATION ID	STATUS	TYPE
VBL-1T-BN-SVP-TRIAL	SecureVUEPlus	1024GB daily	10/16/2024	11/15/2024	0 days	4e8cb5a4-7e...	Active	Trial
VBL-2500T-BN-NV	NetVUE	2560000GB d...	10/04/2024	04/02/2025	30 days	62a2ba16-ba...	Active	Internal

This license includes the following applications:

- ERSPAN
- GENEVE
- Slicing
- Masking
- Trailer
- Tunneling
- Load Balancing
- Enhanced Load Balancing
- Flow map
- Header Stripping
- Header Addition
- De-duplication
- NetFlow
- Application Packet Filtering
- Application Filtering Intelligence
- Application Metadata Intelligence
- Application Metadata Exporter
- Inline SSL
- SSL Decrypt
- Precryption

> **NOTE:** 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.

When you install a new Volume-Based License (VBL), the existing trial license will remain active alongside the new VBL. Once the trial license period expires, it will be automatically deactivated. After deactivation, the trial license will be moved to the **Inactive** tab in the **VBL** page.

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** from the **Activation** drop-down.
3. Click **Activate Licenses**. The **Activate License** page appears.
4. Select **IP Address** or **Hostname** to include this information. If you exclude the IP Address or Hostname, you will have to identify the chassis or GigaSMART card by its ID when activating.
5. Download the fabric inventory file that contains information about GigaVUE-FM. Click **Next**. Refer to the What is a Fabric Inventory File section in *GigaVUE Licensing Guide* for more details.
6. Click **Gigamon License Portal** to 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.
7. Return to GigaVUE-FM and upload the file by clicking **Choose File** button.

Manage Volume-Based Licenses

This section provides information on how to manage active and inactive Volume-Based Licenses in GigaVUE-FM.

Manage active Volume-Based License

To manage active Volume-Based License (VBL):

1. On the left navigation pane, click ⚙.
2. Go to **System > Licenses**. From the top navigation bar, select the **VBL** from the **Activation** drop-down list and click **Active**.

   This page lists the following information about the active Volume-Based Licenses.

Field	Description
SKU	Unique identifier associated with the license.
Bundle	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. Entitlement ID is the permission with which the acquired license can be activated online.
Reference ID	Reference ID.
Status	License status.

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

Manage Inactive Volume-Based License

To manage inactive Volume-Based License (VBL):

1. On the left navigation pane, click ⚙.
2. Go to **System > Licenses**. From the top navigation bar, select the **VBL** from the **Activation** drop-down and click **Inactive**.

   This page lists the following information about the inactive Volume-Based Licenses.

Field	Description
SKU	Unique identifier associated with the license.
Bundle	Bundle to which the license belongs to.
Ends	License end date.
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 Inactive tab of VBL 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. For more information, refer to the topic Manage Volume-Based Licenses of the GigaVUE Licensing Guide.
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 have expired.

> **NOTE:** If a VBL is deactivated after a bundle upgrade, you cannot create or edit Monitoring Sessions that include applications from the deactivated VBL during the grace period. You should manually deactivate the upgraded license during the grace period to move the inactive lower bundle license back to active status.

For more detailed information on dashboards and report 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 License 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

Supported Hypervisors for VMware

The following table lists the supported hypervisor versions for vCenter, VMware ESXi and VMware NSX-T.

GigaVUE V Series Node Supported Hypervisors	Tested Platforms			
		vCenter Server	ESXi	GigaVUE-FM
vSphere ESXi	v6.7	v6.7U3	v6.7U3	v5.10.02, v5.11.01, v5.12.00, v5.13.00, v5.13.01
	v7.0	v7.0	v7.0	v5.10.02, v5.11.01, v5.12.00, v5.13.00, v5.13.01, v5.14.00, v5.15.00, v5.16.00, v6.0.00, v6.1.00
	v7.0	v7.0U3	v7.0U3	v5.15.00, v5.16.00, v6.0.00,v6.1.00, v6.2.00, v6.3.00, v6.4.00, v6.5.00, v6.6.00, v6.7.00, v6.8.00, v6.9.00
	v8.0	v7.0U3	v8.0U2	v6.9.00
	v8.0	v8.0	v8.0	v6.3.00, v6.4.00, v6.5.00, v6.6.00, v6.7.00, v6.8.00, v6.9.00
	v8.0	v8.0U2, v8.0U3	v8.0U2, v8.0U3	v6.8.00, v6.9.00, 6.10.00

GigaVUE V Series Node Supported Hypervisors	Tested Platforms			
		vCenter Server	ESXi	GigaVUE-FM
vSphere NSX-T	v3.1.0	v7.0	v7.0	v5.11.01, v5.12.00
	v3.1.2	v7.0	v6.7U3, v7.0U1	v5.12.00, v5.13.00, v5.13.01
	v3.1.3	v7.0	v6.7U3, v7.0U1	v5.13.01, v5.14.00, v6.0.00
	v3.2.0	v7.0, v7.0U3	v6.7U3, v7.0U1, v7.0U3	v5.14.01, v5.15.00, v5.16.00, v6.0.00
	v3.2.1	v7.0U3	v6.7U3, v7.0U1, v7.0U3	v6.0.00, v6.1.00, v6.2.00
	v3.2.2	v7.0U3	v7.0U3	v6.3.00, v6.4.00
	v3.2.3	v7.0U3	v7.0U3	v6.5.00, v6.6.00, v6.7.00, v6.8.00, v6.9.00, v6.10.00
	v4.0.0	v7.0U3	v7.0U3	v6.0.00, v6.1.00, v6.2.00, v6.3.00
	v4.1.0	v7.0U3	v7.0U3	v6.3.00, v6.4.00, v6.5.00
		v8.0U2	v8.0U2	v6.5.00, v6.6.00, v6.7.00
	v4.1.2	v8.0U2, v8.0U3	v8.0U2, v8.0U3	v6.8.00, v6.9.00
	v4.2	v8.0U2	v8.0U2, v8.0U3	v6.9.00, 6.10.00

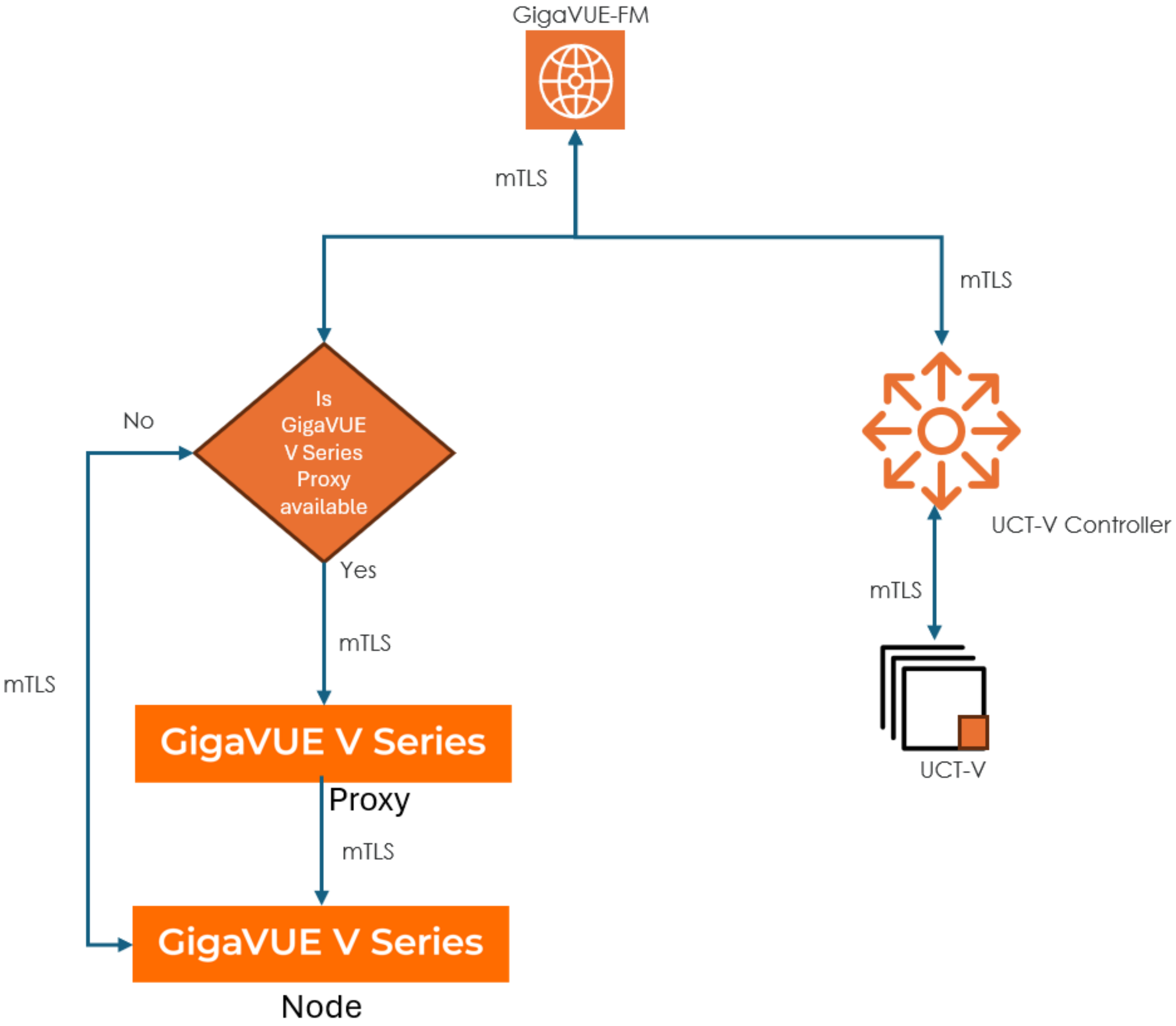
Introduction to Supported Features for GigaVUE Cloud Suite for VMware ESXi

GigaVUE Cloud Suite for VMware (ESXi) supports the following features:

- Rediscover
- Analytics for Virtual Resources
- Sharing the Same Host across Different Monitoring Domains
- Cloud Health Monitoring
- Selective Source Selection

Secure Communication between GigaVUE Fabric Components

The Secure Communication feature in GigaVUE-FM enhances security by enabling mutual Transport Layer Security (mTLS)-based authentication across GigaVUE Fabric Components. With this feature, each fabric component is assigned a properly signed certificate from a Certificate Authority (CA), ensuring authenticated, encrypted communication without relying on static credentials.



In the above diagram, GigaVUE-FM establishes an mTLS connection and checks for GigaVUE V Series Proxy availability. If GigaVUE V Series Proxy is unavailable, it directly connects to the GigaVUE V Series Node through mTLS. If a GigaVUE V Series Proxy is available, then

GigaVUE-FM first connects to the GigaVUE V Series Proxy, which then establishes an mTLS connection with the GigaVUE V Series Node. Separately, GigaVUE-FM also initiates an mTLS connection to the UCT-V Controller, which then establishes an mTLS connection with UCT-V. This structured flow ensures secure communication using mTLS-based authentication across all the fabric components.

GigaVUE-FM manages certificates by acting as the Public Key Infrastructure (PKI), ensuring a centralized and secure approach to certificate management.

GigaVUE-FM acts as the PKI

GigaVUE-FM acts as a private PKI, automatically issuing and managing certificates for all fabric components. GigaVUE-FM uses Step-CA to handle certificate issuance and renewal using the Automatic Certificate Management Environment (ACME) protocol in this method. This eliminates the need for external dependencies while ensuring secure, automated certificate management.

Bring Your Own CA

Organizations with existing PKI infrastructure can import externally issued certificates into GigaVUE-FM. This method supports enterprise CA solutions while allowing seamless integration with Gigamon’s secure communication framework.

For more details on how to integrate your PKI infrastructure with GigaVUE-FM, refer to Integrate Private CA

Supported Platforms

- AWS
- Azure
- OpenStack
- Nutanix
- Third Party Orchestration
- VMware ESXi
- VMware NSX-T

Supported Components

- GigaVUE V Series Node
- GigaVUE V Series Proxy
- UCT-V
- UCT-V Controller

Rules and Notes

- For public cloud platforms, if the public IP is revoked, you can issue a new certificate from GigaVUE-FM to remove the public IP from the certificate.

  NOTE: This is an optional configuration.
- When GigaVUE-FM and GigaVUE Fabric Components are deployed on different hosts, ensure that the hosts are time-synchronized with NTP configured and running.
- When applying the certificates, the GigaVUE Fabric Components may move to a Down state and automatically recover.

Rediscover

When modifying the configurations of the GigaVUE V Series Node deployed in VMware vCenter, it may lead to configuration mismatch between the GigaVUE V Series Node and the virtual machine configuration present in GigaVUE-FM. You can use the Rediscover button in GigaVUE-FM to overcome this. The following GigaVUE V Series Node configuration can be rediscovered from GigaVUE-FM:

- GigaVUE V Series Node name
- Datastore
- Management IP address
- Tunnel IP address
- Network name for Management Interface
- Network name for Tunnel Interface

NOTE: GigaVUE-FM performs an auto-rediscovery every 24 hours. Every 24 hours GigaVUE-FM checks for the above-mentioned things and updates the GigaVUE V Series Node configuration.

You can select an individual or multiple GigaVUE V Series Node in the Monitoring Domain page and follow the instructions given below:

1. Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. On the **Monitoring Domain** page, click **Actions > Rediscover**.

NOTE: You can only rediscover GigaVUE V Series Nodes that are in **OK** state.

Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics 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 for Virtual Resources for more detailed information.

Sharing the Same Host across Different Monitoring Domains

GigaVUE-FM has the ability to share a host between VMware ESXi and VMware NSX-T monitoring domain. You can deploy multiple V Series nodes from VMware NSX-T monitoring domain and one V Series Node from VMware ESXi monitoring domain on the same host. This way the workload virtual machines connected to NSX segments can be monitored using the V Series nodes deployed in NSX-T monitoring domain and workload virtual machines connected to regular VSS / VDS networks can be monitored using the V Series node deployed in the ESXi monitoring domain.

NOTE: If a Virtual Machine has NICs attached to both VMware NSX-T segments and ESXi VDS or VSS port groups then GigaVUE-FM cannot provide visibility to those virtual machines in ESXi platform.

Cloud Health Monitoring

GigaVUE-FM allows you to monitor the traffic and configuration health status of the monitoring session and its individual components. This section provides detailed information on how to view the traffic and configuration health status of the monitoring session and its individual components.

For more information on how to configure cloud health monitoring, refer to the topic Monitor Cloud Health.

Selective Source Selection

Using this feature, you can select an individual Network adapter of a virtual machine as a target when creating maps. Refer to Create a New Map (VMware ESXi) topic for more detailed information.

Customer Orchestrated Source - Use Case

Customer Orchestrated Source is a traffic acquisition method that allows to tunnel traffic directly to the GigaVUE V Series Nodes. In cases where UCT-V or VPC Mirroring cannot be configured due to firewall or other restrictions, you can use this method and tunnel the traffic to GigaVUE V Series Node, where the traffic is processed.

When using Customer Orchestrated Source, you can directly configure tunnels or raw endpoints in the monitoring session, where you can use other applications like Slicing, Masking, Application Metadata, Application Filtering, etc., to process the tunneled traffic. Refer to Create Ingress and Egress Tunnel (VMware vCenter) and Create Raw Endpoint for more detailed information on how to configure Tunnels and Raw End Points in the Monitoring Session.

You can configure an Ingress tunnel in the Monitoring Session with the GigaVUE V Series Node IP address as the destination IP address, then the traffic is directly tunneled to that GigaVUE V Series Node.

Prerequisites for Integrating V Series Nodes with VMware vCenter

- Refer to Supported Hypervisors for VMware for supported VMware vCenter, VMware ESXi and VMware NSX-T versions.
- ESXi hosts must have the minimum vCPU and memory resources for hosting the GigaVUE V Series Nodes. Refer toRecommended Form Factor for VMware vCenter (Instance Types) for more information.
- To support internationalized characters in the VMware vCenter environment, ensure that the vCenter character encoding is set to UTF-8.
- GigaVUE V Series Node device OVA image file. The GigaVUE V Series Node OVA image files can be downloaded from Gigamon Customer Portal.
- All the target VMs must have VMware guest tools or Open VM tools if you use IP based filtering.
- Port 8889 must be available for GigaVUE-FM to access GigaVUE V Series Nodes.
- TCP Port 443 must be open between the GigaVUE-FM instance and the ESXi host to upload the OVA files. Refer to Network Firewall Requirements for more detailed information on ports that must be opened for configuring GigaVUE Cloud Suite for VMware vCenter.

- If you wish to enable **VMware EVC** in VMware vCenter, a minimum of **Intel Sandy Bridge** CPU compatibility is required to ensure proper operation and optimal performance. While **Skylake** and above is the recommended option.

Refer to the following topics for more detailed information:

- Recommended Form Factor for VMware vCenter (Instance Types)
- Network Firewall Requirements
- Required VMware Virtual Center Privileges
- Default Login Credentials

Recommended Form Factor for VMware vCenter (Instance Types)

The form factor (instance) size of the GigaVUE V Series Node is configured on the OVF file and packaged as part of the OVA image file. The following table lists the available form factors (instance types) and sizes based on memory and the number of vCPUs for a single GigaVUE V Series Node. Instances sizes can be different for GigaVUE V Series Nodes in different ESXi hosts and the default size is Small.

Type	Memory	vCPU	Disk space	vNIC
Small	4GB	2 vCPU	8GB	1 Management interface, 1 Tunnel interface, and 8 vTAP interfaces
Medium	8GB	4 vCPU		
Large	16GB	8 vCPU		

NOTE: For any queries on which form factor to use, reach out to your account manager or contact Gigamon Technical Support

Minimum Virtual Computing Requirements

There is a minimum required number of ports for port groups of a Virtual Distributed Switch (VDS) used by GigaVUE V Series Node deployments:

- In a single GigaVUE V Series Node deployment, 1 or 2 port groups can be used. The number of ports required is calculated based on the number of port groups used.
- If you are using a single port group, then each GigaVUE V Series Node uses 10 ports from the port group. Therefore, the port group must support at least the number of GigaVUE V Series Nodes deployed in that port group multiplied by 10.
- If you are using two-port groups in a single GigaVUE V Series Node deployment, the minimum number of required ports changes for Management and Tunnel port groups as follows:
    - Minimum ports for Management port group = # GigaVUE V Series Nodes

  - Minimum ports for Tunnel port group = # GigaVUE V Series Nodes multiplied by 9

Network Firewall Requirements

Following are the Network Firewall Requirements for GigaVUE V Series Node deployment.

Source	Destination	Source Port	Destination Port	Protocol	Service	Purpose
GigaVUE-FM	ESXi hosts	Any (1024-65535)	443	TCP	https	Allows GigaVUE-FM to communicate with vCenter and all ESXi hosts to import the V Series OVA files. OVA files require access to the host IP/URL for bulk deployment
	vCenter					
GigaVUE-FM	GigaVUE V Series Nodes	Any (1024-65535)	8889	TCP	Custom API	Allows GigaVUE-FM to communicate with GigaVUE V Series Node
GigaVUE-FM	GigaVUE V Series Nodes	Any (1024-65535)	5671	TCP	Custom TCP	Allows GigaVUE-FM to receive the traffic health updates with GigaVUE V Series Node
GigaVUE-FM	GigaVUE V Series Nodes	Any (1024-65535)	80	TCP	Custom TCP	Allows GigaVUE-FM to send ACME challenge requests to GigaVUE V Series Node.
Administrator	GigaVUE-FM	Any (1024-65535)	443	TCP	https	Management connection to GigaVUE-FM
			22		ssh	
Administrator	GigaVUE V Series Nodes	Not Applicable	22		ssh	Troubleshooting GigaVUE V Series Nodes.

Remote Source	GigaVUE V Series Nodes	Custom Port (VXLAN and UDPGRE),N/A for GRE	4789	UDP	VXLAN	Allows to UDPGRE Tunnel to communicate and tunnel traffic to GigaVUE V Series Nodes (Applicable for Tunnel Ingress option only)
			N/A	IP 47	GRE	
			4754	UDP	UDPGRE	
GigaVUE V Series Nodes	Tool/ GiagVUE HC Series instance	Custom Port (VXLAN),N/A for GRE	4789	UDP	VXLAN	Allows GigaVUE V Series Node to communicate and tunnel traffic to the Tool
			Not Applicable	IP 47	GRE	
GigaVUE V Series Nodes	Tool/ GigaVUE HC Series instance	Not Applicable	Not Applicable	ICMP	Echo Request	Allows GigaVUE V Series Node to health check tunnel destination traffic (Optional)
					Echo Response	
GigaVUE V Series Nodes	GigaVUE-FM	Any (1024-65535)	Any (1024-65535)	TCP	Custom TCP	Allows GigaVUE V Series Nodes to communicate the traffic health updates with GigaVUE-FM
GigaVUE V Series Nodes	GigaVUE-FM	Any (1024-65535)	9600	TCP	Custom TCP	Allows GigaVUE-FM to receive certificate requests from GigaVUE V Series Node.

Required VMware Virtual Center Privileges

This section lists the minimum privileges required for the GigaVUE-FM user in Virtual Center. You assign privileges to Virtual Center users by selecting **Administration** from the left navigation pane. Then select **Roles** under the **Access Control**. Roles should be applied at the vSphere Virtual Center level and not the Data Center or Host levels.

The following table lists the minimum required permissions for GigaVUE-FM to manage the virtual center user with roles specified above.

Category	Required Privilege	Purpose
Datastore	Allocate space	V Series Node Deployment
Distributed Switch	VSPAN Operation	VDS Tapping
Folder	Create Folder	V Series Node Deployment
Host	**Configuration** • Network Configuration	VSS Tapping
	Inventory • Modify Cluster	Pin V Series Node to the host in cluster configurations. This prevents automatic migration.
Network	• Assign network • Configure	• V Series Node Deployment/VSS Tapping • V Series Node Deployment
Resource	Assign virtual machine to resource pool	V Series Node Deployment
vApp	• Import • vApp instance configuration • vApp application configuration	V Series Node Deployment
Virtual machine	**Configuration** • Add new disk • Add or remove device • Modify device settings • Rename	V Series Node Deployment V Series Node Deployment/VSS Tapping
	Interaction • Connect devices • Power on • Power Off • Reset	V Series Node Deployment
	Inventory ▪ Create from existing ▪ Remove	V Series Node Deployment
	Provisioning ▪ Clone virtual machine	V Series Node Deployment

Default Login Credentials

You can login to the GigaVUE V Series Node 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: Enter the password provided during the fabric launch configuration. Refer Configure GigaVUE V Series Nodes for VMware ESXi for more detailed information on fabric launch configuration.

Install and Upgrade GigaVUE-FM

You have the flexibility of installing GigaVUE-FM across various supported platforms. Additionally, you can effectively manage deployments in any of the cloud platform as long as there exists IP connectivity for seamless operation.

You can install and upgrade the GigaVUE-FM fabric manager (GigaVUE-FM) on cloud platforms or on-premises.

- Installation: Refer to GigaVUE-FM Installation and Upgrade Guide available in the Gigamon Documentation Library.
- Upgrade: Refer toUpgrade GigaVUE-FM topic in GigaVUE-FM Installation and Upgrade Guide.

Deploy GigaVUE Cloud Suite for VMware (ESXi)

To integrate GigaVUE V Series Nodes with VMware vCenter, perform the following steps:

- Upload GigaVUE V Series Node Image into GigaVUE-FM
- Create Monitoring Domain for VMware ESXi
- Configure GigaVUE V Series Nodes for VMware ESXi
- Rediscover

The below table provides step-by-step instructions on configuring GigaVUE Cloud Suite for VMware for providing visibility to physical and virtual traffic. Refer to the VMware ESXi System Requirements and Prerequisites for Integrating V Series Nodes with VMware vCenter sections for prerequisites that are required to be configured.

Step No	Task	Refer the following topics
1	Upload the GigaVUE V Series Node Image (OVA FIle) into GigaVUE-FM	Upload GigaVUE V Series Node Image into GigaVUE-FM
2	Create a Monitoring Domain	Create Monitoring Domain for VMware ESXi
3	Deploy GigaVUE V Series Nodes using GigaVUE-FM	Configure GigaVUE V Series Nodes for VMware ESXi Refer to *Deploy GigaVUE V Series Nodes using GigaVUE-FM* section.
4	Create Monitoring session	Create a Monitoring Session (VMware)
5	Create a Ingress and Egress Tunnels to tunnel traffic	Create Ingress and Egress Tunnel (VMware vCenter)
6	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
7	Deploy Monitoring Session	Deploy Monitoring Session
8	View Monitoring Session Statistics	View Monitoring Session Statistics

Upload GigaVUE V Series Node Image into GigaVUE-FM

This step is optional, you can also upload the GigaVUE V Series Node Image into GigaVUE-FM, when deploying the GigaVUE V Series Node. Refer to Configure GigaVUE V Series Nodes for VMware ESXi.

To upload the V Series image into GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, and then click **Settings > OVA Files**. The OVA Files page appears.
2. In the OVA Files page, click **Browse** to select the *gigamon-gigavue-vseries-node-x.x.x-0-xxxxxx.ova* file.
3. Click **Upload to Server** to upload the selected OVA image file to GigaVUE-FM server.

> **NOTE:** The maximum number of OVA files that can be uploaded to GigaVUE-FM for VMware vCenter is three.

Integrate Private CA

If you want to integrate your own PKI infrastructure with GigaVUE-FM, you must generate a Certificate Signing Request (CSR) and get the CSR signed by the Certificate Authority (CA) and upload it back in GigaVUE-FM.

Rules and Notes

- The root CA must always be placed in a separate file.
- When using multiple intermediate CAs, ensure that they are placed in a single file in the correct order. The last intermediate CA in the chain should be placed at the top, followed by the preceding CAs in descending order.

Generate CSR

To create intermediate CA certificate:

1. Go to ⚙ **> System > Certificates**.
2. In the top navigation bar, from the **PKI** drop-down list select **CSR**. The **Generate Intermediate CA Certificate** page appears.
3. In the **Country** field, enter the name of your country.
4. In the **Organization** field, enter your organization name.
5. In the **Organization Unit** field, enter the department or unit name.
6. In the **Common Name** field, enter the common name associated with the certificate.
7. From the **Algorithm** drop-down list, select the desired encryption algorithm used to encrypt your private key.
8. Click the **Generate CSR** button to create and download the CSR.

The CSR is downloaded successfully.

Upload CA Certificate

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

To upload the signed CA certificate to GigaVUE-FM:

1. Go to ⚙ **> System > Certificates**.
2. In the top navigation bar, from the **PKI** drop-down list select **CA**. The **CA Certificate** page appears.
3. From the **Actions** drop-down list, select **Upload CA**. The **Upload CA** popup appears.

4. Click **Choose File** next to **Intermediate CA** to upload the signed intermediate CA certificate.
5. Click **Choose File** next to **Root CA** to upload the corresponding root or intermediate CA that signed the given intermediate CA.

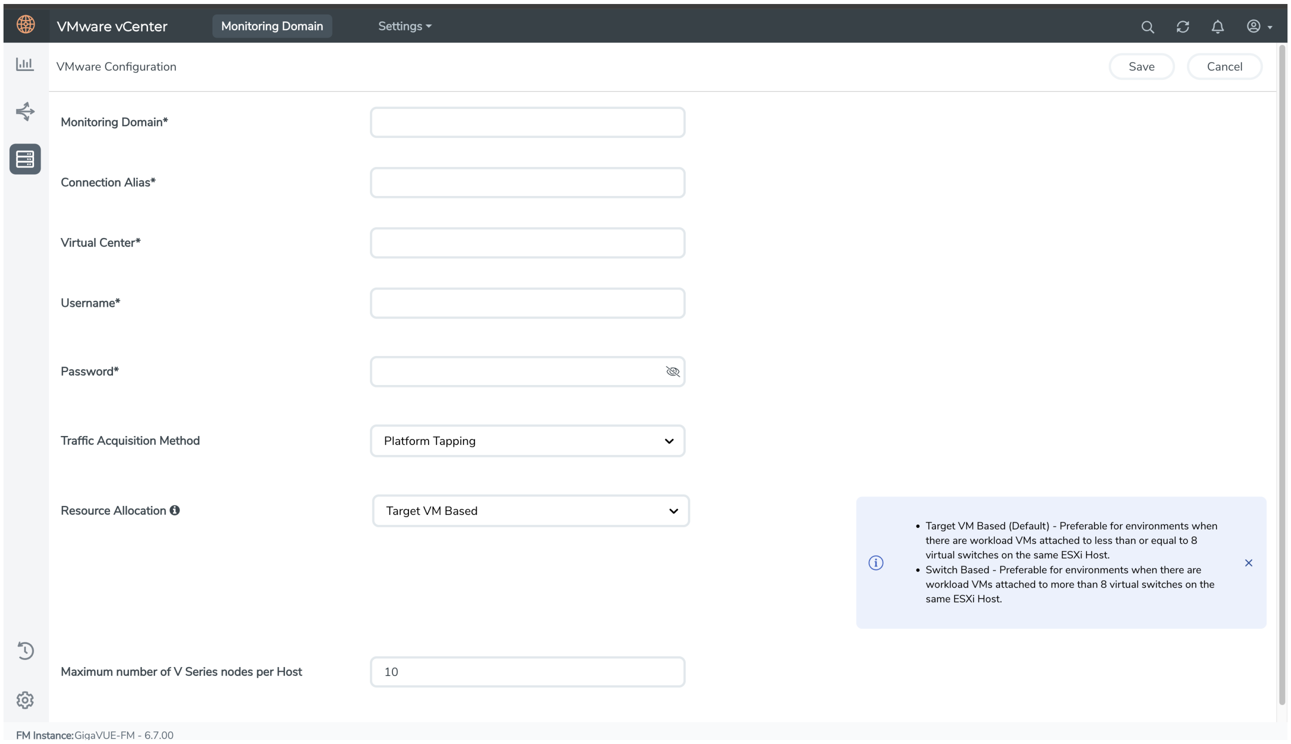
You can view the uploaded CA certificate in the **CA Certificate** page.

Create Monitoring Domain for VMware ESXi

This chapter describes how to create a monitoring domain for deploying GigaVUE V Series Nodes in VMware vCenter environment through GigaVUE-FM. You must establish a connection between GigaVUE-FM and VMware vCenter. Creating a monitoring domain in GigaVUE-FM allows you to establish a connection between vCenter and GigaVUE-FM.

To create a monitoring domain in GigaVUE-FM for VMware vCenter:

1. Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. On the **Monitoring Domain** page, click **New**. The **VMware Configuration page** appears.



Monitoring Domain*

Connection Alias*

Virtual Center*

Username*

Password*

Traffic Acquisition Method: Platform Tapping

Resource Allocation: Target VM Based

- Target VM Based (Default) - Preferable for environments when there are workload VMs attached to less than or equal to 8 virtual switches on the same ESXi Host.
- Switch Based - Preferable for environments when there are workload VMs attached to more than 8 virtual switches on the same ESXi Host.

Maximum number of V Series nodes per Host: 10

FM Instance:GigaVUE-FM - 6.7.00

3. In the **VMware Configuration** page, enter or select the following details:

Field	Description
Monitoring Domain	Name of the monitoring domain
Connection Alias	Name of the connection
Virtual Center	IP address or FQDN of the vCenter **NOTE:** To ensure the validity of VMware virtual central certificates issued by a trusted Certificate Authority (CA), you must enable the Trust Store. Refer to Cloud solution in Trust Store section in GigaVUE Administration Guide.
Username	Username of the vCenter user with minimum privileges as described in Prerequisites for Integrating V Series Nodes with VMware vCenter section. **NOTE:** Whenever you change the vCenter credentials in VMware vCenter, you should update that in GigaVUE-FM by editing the Monitoring Domain. Otherwise, the connection status will be in an authentication failure state.
Password	vCenter password used to connect to the vCenter

Field	Description
Traffic Acquisition Method	Select a Traffic Acquisition Method. **Platform Tapping**: Platform tapping can be done in two ways. • VSS: Platform Tapping can be used when a workload Virtual Machine is connected to a Virtual Standard Switch network. Promiscuous network will be created on VSS switch by GigaVUE-FM for tapping the traffic. • VDS: Platform Tapping can be used when a workload Virtual Machine is connected to a Virtual Distributed Switch portgroup. Port Mirroring will be created on the VDS switch by GigaVUE-FM for tapping the traffic **Customer Orchestrated Source**: If you select Customer Orchestrated Source as the tapping method, you can use a tunnel or raw endpoint as a source where the traffic is directly tunneled to GigaVUE V Series Nodes. **NOTE:** If you wish to deploy AMX application in the Monitoring Session for this Monitoring Domain, select the Traffic Acquisition Method as Customer Orchestrated Source.
Resource Allocation **NOTE:** This field is applicable only when using **Platform Tapping** as the **Traffic Acquisition Method**.	When deploying multiple GigaVUE V Series Node in a single host, select any one of the following options: **Target VM Based**: Choose this option if your deployment workload VMs attached to less than or equal to 8 vSwtiches on the same ESXi host. This type of resource allocation will distribute the workload VMs across the multiple GigaVUE V Series Node deployed on the same ESXi host. **Switch Based**: A single GigaVUE V Series Node can tap a maximum of 8 vSwitches. Choose this option if you have traffic monitoring VMs running on ESXi hosts that are connected to more than 8 vSwitches in a single host. The vSwitches are mapped to the GigaVUE V Series Node in a round-robin manner. In this model vSwitches are evenly distributed across the available GigaVUE V Series Nodes on the same host. **NOTE:** Ensure to undeploy all the Monitoring Session associated with the connection before changing the **Resource Allocation** type.
Maximum Number of V Series Nodes per Host	Enter the maximum number of GigaVUE V Series Nodes that can be deployed in a single host. The default value is 10.

4. Click **Save**. The **VMware Fabric Launch Configuration** page appears. Refer to Configure GigaVUE V Series Nodes for VMware ESXi for more detailed information on how to deploy GigaVUE V Series Nodes in the **VMware Fabric Launch Configuration** page.

Notes:

- Ensure that all V Series Nodes within a single Monitoring Domain are running the same version. Mixing different versions in the same Monitoring Domain may lead to inconsistencies when configuring Monitoring Session traffic elements.
- Similarly, when upgrading a V Series Node, ensure that the GigaVUE-FM version is the same or higher than the V Series Node version.

The Monitoring Domain created in this section will be listed in the **Monitoring Domain** page.

Points to Note:

- Whenever you change the vCenter credentials in VMware vCenter, you should update that in GigaVUE-FM by editing the Monitoring Domain. Otherwise, the connection status will be in an authentication failure state.
- When the Monitoring Domain is in a "Not Connected" state, updating the vCenter credentials will only refresh the information stored in the GigaVUE-FM database. To establish the connection:
  1. Navigate to the **Monitoring Domain** page.
  2. Click **Actions** button and click **Connect**.

  By following these steps, you can ensure that your vCenter credentials are updated and the connection is properly established.

You can perform the following actions in the Monitoring domain page:

Actions	Description
Edit	Use to edit a monitoring domain.
Deploy Fabric	Use to deploy GigaVUE V Series Nodes.
Upgrade Fabric	Use to upgrade GigaVUE V Series Nodes. Refer to Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi for more detailed information on how to upgrade.
Delete Monitoring Domain	Use to delete a Monitoring Domain.
Delete Fabric Nodes	Use to delete a GigaVUE V Series Node.
Connect / Disconnect	**Disconnect**- When the Monitoring Domain is in Connected state, this option appears. Use this option to stop the communication between GigaVUE-FM and the VMware vCenter. **Connect**- When the Monitoring Domain is in disconnected state, this option appears. Use this option to start the communication between GigaVUE-FM and the VMware vCenter.
Rediscover	The changes made in vCenter for the GigaVUE V Series Node will be reflected in GigaVUE-FM. Refer to Rediscover topic for more detailed information.

Actions	Description
Power On	You can select an individual GigaVUE V Series Node and power it on. The status of the GigaVUE V Series Node is changed to **Ok**.
Power Off	You can select an individual GigaVUE V Series Node and power it off. If the GigaVUE V Series Node is turned off from GigaVUE-FM, then it will not be considered as part of Cloud Health Monitoring and GigaVUE-FM will not try to turn it on. The status of the GigaVUE V Series Node is changed to **Down**.
Reboot	You can select an individual GigaVUE V Series Node and reboot it.
Edit SSL Configuration	You can use this option to add Certificate Authority and the SSL Keys when using the Secure Tunnels.
Generate Sysdump	You can select one or multiple GigaVUE V Series Nodes (Upto maximum 10) to generate the sysdump files. The generation of sysdump takes few minutes in GigaVUE V Series Node, you can proceed with other tasks and upon completion the status will be shown in GUI. These sysdump files can be used to troubleshoot the system. Refer to Debuggability and Troubleshooting for more information.
Manage Certificates	You can use this button to perform the following actions: • **Re-issue**- Certificates can be reissued to address security compromises, key changes, or configuration updates, like validity period adjustments. • **Renew**- Renewing a certificate just extends its expiration date and usually happens automatically unless you decide to do it during scheduled downtime. Auto-renewal is performed based on the duration specified in the **Certificate Settings** page. Refer to Configure Certificate Settings for more details.

To view and manage the generated sysdump files, select the GigaVUE V Series Node and click the **Sysdump** tab in the lower pane.

To view the certificates associated with the fabric, select the fabric nodes and click the **Certificates** tab in the lower pane.

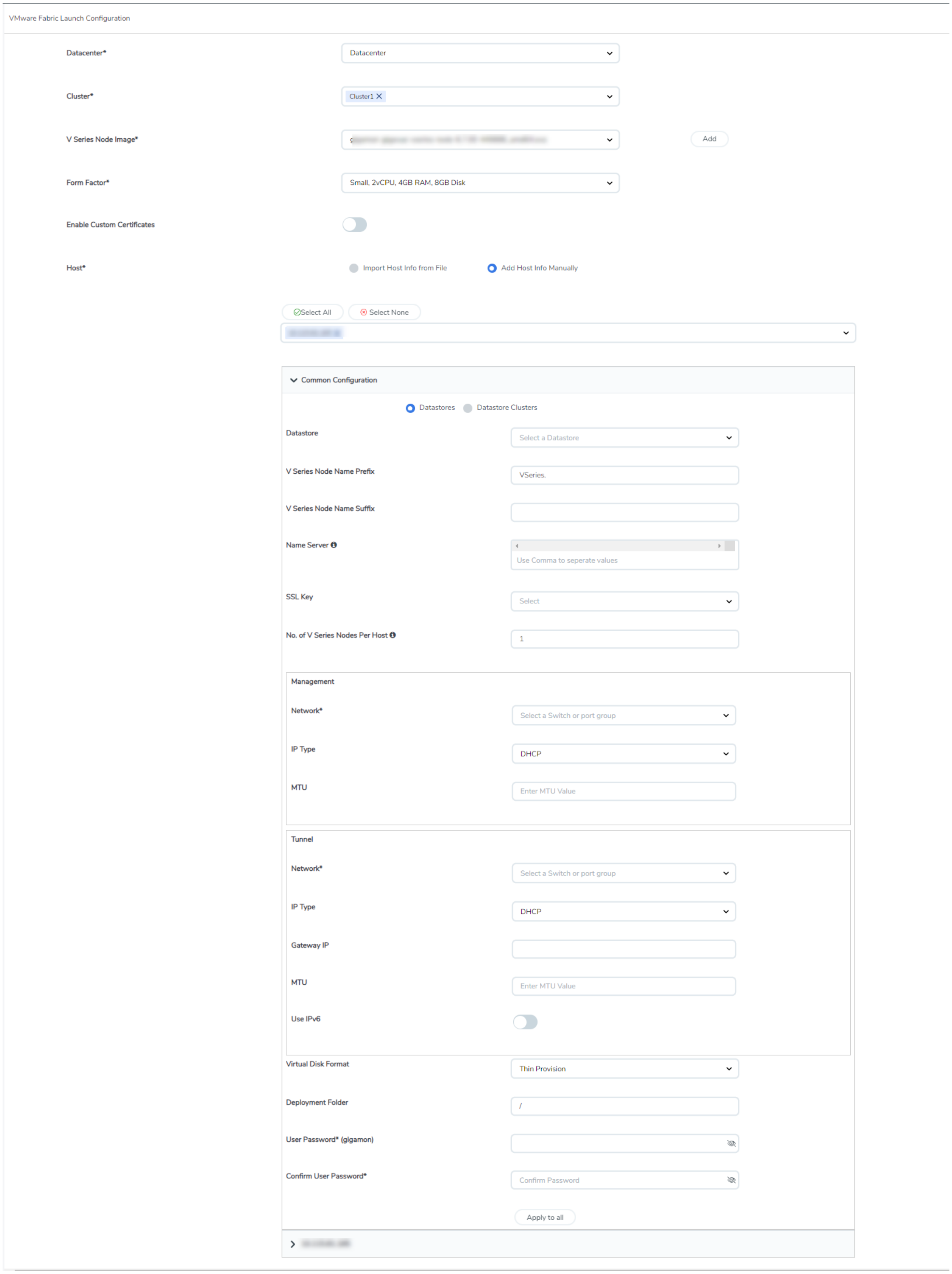
Configure GigaVUE V Series Nodes for VMware ESXi

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

To deploy GigaVUE V Series Nodes using GigaVUE-FM, follow the steps given below:

1. After creating a monitoring domain, you are navigated to the **VMware Fabric Launch Configuration** page.

2. You can also open **VMware Fabric Launch Configuration** page from the **Monitoring Domain** page. To launch the **VMware Fabric Launch Configuration** from the Monitoring Domain, go to **Inventory > VIRTUAL > VMware vCenter (V Series)**. Click **Actions > Deploy Fabric**. The **VMware Fabric Launch Configuration** page appears.



VMware Fabric Launch Configuration

Datacenter*	Datacenter
Cluster*	Cluster1 ✕
V Series Node Image*	[redacted]
Form Factor*	Small, 2vCPU, 4GB RAM, 8GB Disk
Enable Custom Certificates	○
Host*	○ Import Host Info from File ● Add Host Info Manually

[redacted]

Common Configuration

● Datastores ○ Datastore Clusters

Datastore	Select a Datastore
V Series Node Name Prefix	VSeries.
V Series Node Name Suffix	
Name Server	Use Comma to seperate values
SSL Key	Select
No. of V Series Nodes Per Host	1

Management

Network*	Select a Switch or port group
IP Type	DHCP
MTU	Enter MTU Value

Tunnel

Network*	Select a Switch or port group
IP Type	DHCP
Gateway IP	
MTU	Enter MTU Value
Use IPv6	○

Virtual Disk Format	Thin Provision
Deployment Folder	/
User Password* (gigamon)	
Confirm User Password*	Confirm Password

[redacted]

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

Field	Description
Datacenter	vCenter Data Center with the ESXi hosts to be provisioned with GigaVUE V Series Nodes.
Cluster	Cluster where you want to deploy the GigaVUE V Series Nodes.
V Series Node Image	Select the OVA file uploaded in the Upload GigaVUE V Series Node Image into GigaVUE-FM, from the drop-down menu. You can also add OVA files when launching the fabric. To add OVA files: a. Click on the **Add** button. b. The **Upload Image** dialog box opens. In the **Upload Image** dialog box, click **Browse** to select the *gigamon-gigavue-vseries-node-x.x.x-0-xxxxxx.ova* file. c. Click **Upload to Server** to upload the selected OVA image file to GigaVUE-FM server.
Form Factor	Instance size of the GigaVUE V Series Node. Refer Prerequisites for Integrating V Series Nodes with VMware vCenter for more information. • Small Form Factor is not supported when using applications like Application Visualization, Application Metadata, Application Filtering. • Select 80GB Disk Space, when using AMX Application.
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 a handshake error occurs. **NOTE:** If the certificate expires after the successful deployment of the fabric components, then the fabric components move to failed state.
Certificate **NOTE:** This field appears only when **Enable Custom Certificates** field is enabled.	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes. For more detailed information, refer to Install Custom Certificate.
Hosts	Select the ESXi hosts for GigaVUE V Series Node deployment. Select **Import Host Info from file** or **Add Host Info Manually**. **Import Host Info from file:** To import host details from a .csv file: a. Download the .csv template file. b. Enter the required values in the Excel sheet and save the file. c. Click Browse and select the .csv file saved in the previous step.

<table>
<thead>
<tr><th>Field</th><th>Description</th></tr>
</thead>
<tbody>
<tr><td></td><td>
<ul>
<li>To deploy more than one GigaVUE V Series Node on the same host, add more rows in the Excel sheet with the same host value for each extra GigaVUE V Series Node you want to deploy.</li>
<li>If your GigaVUE-FM version is above 6.5 and GigaVUE V Series Nodes are on a version below 6.5, Name Server and MTU is not supported. Therefore, these fields in the .csv file must be empty.</li>
</ul>
<p><b>Add Host Info Manually:</b></p>
<p>Select the ESXi hosts for GigaVUE V Series Node deployment.</p>
<p>The Common Configuration drop-down wizard appears. Expand the <b>Common Configuration</b> drop-down wizard and update the following details to apply the configuration to all the selected hosts.</p>
<p>You can expand the individual hosts and add or delete GigaVUE V Series Node. You can expand the individual GigaVUE V Series Node and modify the configurations that were applied in the <b>Common Configuration</b>.</p>
<table>
<tr><td colspan="2"><b>Common Configuration</b></td></tr>
<tr><td><b>Datastore</b></td><td>Network datastore shared among all ESXi hosts.</td></tr>
<tr><td><b>V Series Node Name Prefix</b></td><td>Enter a prefix for the GigaVUE V Series Node name.</td></tr>
<tr><td><b>V Series Node Name Suffix</b></td><td>Enter a suffix for the GigaVUE V Series Node name.</td></tr>
<tr><td><b>Name Server</b></td><td>The server that stores the mapping between the domain names and the IP address. The maximum number of name servers that can be entered is three. Enter valid IPv4 addresses, separated by comma.</td></tr>
<tr><td><b>No. of V Series Nodes per Host</b></td><td>Enter the number of GigaVUE V Series Nodes to be deployed in each host.</td></tr>
<tr><td colspan="2"><b>Management</b></td></tr>
<tr><td>Network</td><td>Management network for GigaVUE V Series Nodes.</td></tr>
<tr><td>IP Type</td><td>Select the management network IP type as Static or DHCP.</td></tr>
<tr><td>Gateway IP
<b>NOTE:</b> This field appears only when the Management <b>IP type</b> is Static.</td><td>Gateway IP address of the Management Network.</td></tr>
<tr><td>Netmask Length
<b>NOTE:</b> This field appears only when the</td><td>Management network's subnet mask value in CIDR format. Eg. 21 for /21.</td></tr>
</table>
</td></tr>
</tbody>
</table>

Field	Description	
	Management **IP type** is Static.	
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that can be transferred as a single entity in a network connection. Enter value between 1280 to 9000.
	Data Interfaces - When using **Customer Orchestrated Source** as the Traffic Acquisition Method, you must configure two data interfaces.	
	Use IPv6 **NOTE:** This field appears only when **Customer Orchestrated Source** as the Traffic Acquisition Method.	Enable to use IPv6.
	Network	Tunnel Network for the GigaVUE V Series Nodes.
	IP Type	Select the tunnel network IP address type as Static or DHCP.
	Gateway IP (optional)	Gateway IP address of the Tunnel Network.
	Netmask Length **NOTE:** This field appears only when the Tunnel **IP type** is Static.	Tunnel network's subnet mask value in CIDR format. Eg. 21 for /21.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that can be transferred as a single entity in a network connection. Enter value between 1280 to 9000.
	IPv6 Prefix Length **NOTE:** This field appears only when the **Use IPv6** toggle button is enabled.	Enter the IPv6 prefix length as 64.
	Virtual Disk Format	Select the Virtual Disk Format from the drop-down menu
	Deployment Folder	Enter the folder name in vCenter, under which the GigaVUE V Series Nodes must be deployed.
	Password	Enter the password you wish to use for the GigaVUE V Series Node.

4. Click **Deploy**. After the GigaVUE V Series Node is deployed in vCenter, it appears on the **Monitoring Domain** page under the Monitoring Domain in which the GigaVUE V Series Node is deployed.

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

Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi

This section provides information on the different ways to upgrade the GigaVUE V Series Nodes and step-by-step instructions on how to upgrade GigaVUE V Series Nodes.

> **IMPORTANT NOTE:**
>
> Before upgrading the Fabric Components to version 6.10.00 or above, ensure the following actions are performed:
>
> - Open the required ports in the cloud platform. Refer to Network Firewall Requirement for GigaVUE Cloud Suite for more details.
> - When using FMHA configuration, follow the steps given provided in the Configure Secure Communication between Fabric Components in FMHA section.

GigaVUE V Series Nodes can be upgraded using the following two ways:

1. You can upgrade all the GigaVUE V Series Node in a monitoring Domain by following the below instructions
   a. Select the Monitoring Domain.
   b. Click **Actions > Upgrade Fabric.**
2. You can upgrade a single or a group of GigaVUE V Series Node. When upgrading a group of GigaVUE V Series Nodes, ensure all the GigaVUE V Series Nodes deployed on the same ESXi hosts are selected.

Keep in mind the following when upgrading the GigaVUE V Series Nodes:

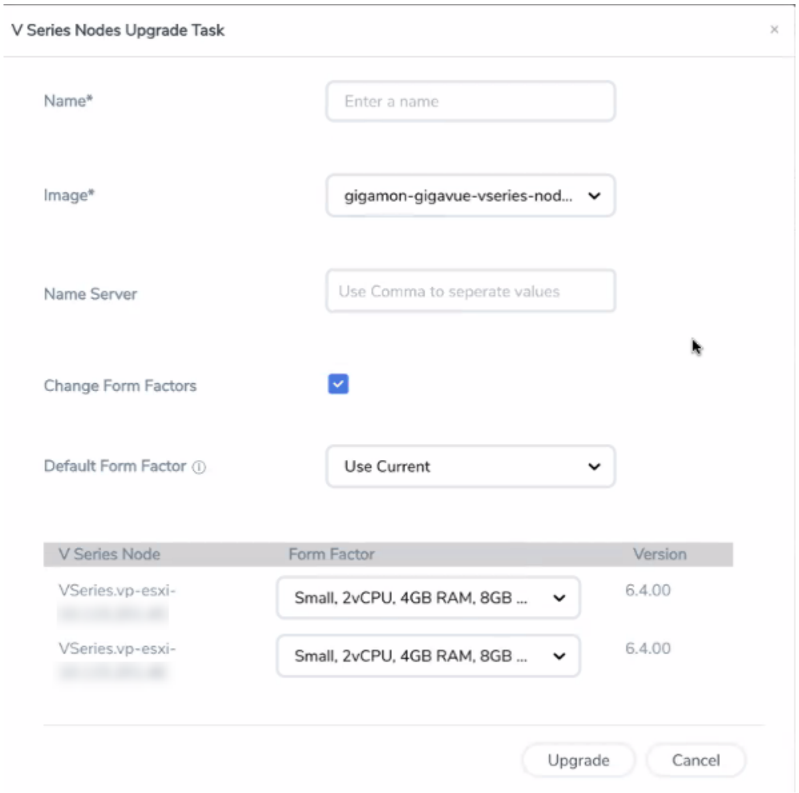
- You can select an entire monitoring domain and upgrade all the GigaVUE V Series Nodes in that particular monitoring domain, or you can select an entire host and upgrade all the GigaVUE V Series Node deployed in that particular host. When multiple GigaVUE V Series Nodes are deployed on the same ESXi host and only if a part of GigaVUE V Series Nodes are selected in that particular host, then the **Upgrade Fabric** button is disabled.

- When upgrading GigaVUE V Series Nodes, if a host of a particular GigaVUE V Series Node is under maintenance mode, then the **Upgrade Fabric** button is disabled. Unselect the GigaVUE V Series Node whose host is under maintenance mode, and upgrade that GigaVUE V Series Node once the host is out of the maintenance mode.

NOTE: GigaVUE-FM only supports (n, n-1, n-2) GigaVUE V Series Node versions.

To upgrade the GigaVUE V Series Node in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. Select an entire monitoring domain or an entire host and click **Actions**. From the drop-down list, select **Upgrade Fabric**, and the **V Series Node Upgrade Task** dialog box appears.



V Series Nodes Upgrade Task

Name* : Enter a name

Image* : gigamon-gigavue-vseries-nod...

Name Server : Use Comma to seperate values

Change Form Factors ☑

Default Form Factor : Use Current

V Series Node	Form Factor	Version
VSeries.vp-esxi-[redacted]	Small, 2vCPU, 4GB RAM, 8GB ...	6.4.00
VSeries.vp-esxi-[redacted]	Small, 2vCPU, 4GB RAM, 8GB ...	6.4.00

3. Enter a name for the V Series Node upgrade task.
4. Select the latest GigaVUE V Series Node OVA image from the **Image** drop-down list.
5. When upgrading the GigaVUE V Series Nodes to any version equal to or greater than 6.5.00, the **Name Server** field is displayed. This field is optional. Name Server is a server that stores the mapping between the domain names and the IP address. The maximum number of name servers that can be entered is three. Enter valid IPv4 address, separated by comma.
6. If you want to modify the form factor (instance) size, click the **Change Form Factors** check box.

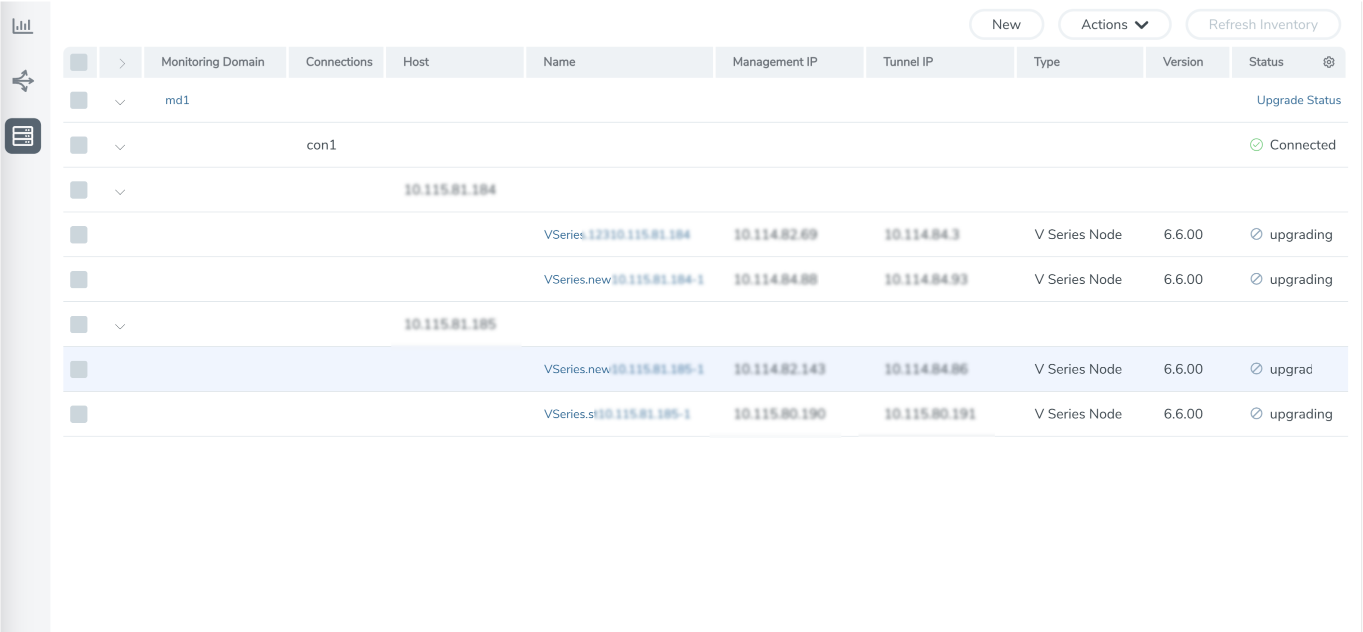
7. Select the form factor from the Default Form Factor drop-down menu to change the form factor of all the selected V Series Nodes. You can use the **Use Current** option to use the existing form factor of the individual GigaVUE V Series Node.
8. You can also change the form factor of a individual GigaVUE V Series Node from the **Form Factor** drop-down menu of the respective GigaVUE V Series Node. The form factor selected here overwrites the form factor selected in the **Default Form Factor**.

   > **NOTE:** All the GigaVUE V Series Node with Static IP address retain their old IP address even after the upgrade.

9. Click **Upgrade** to launch the GigaVUE V Series Node upgrade.

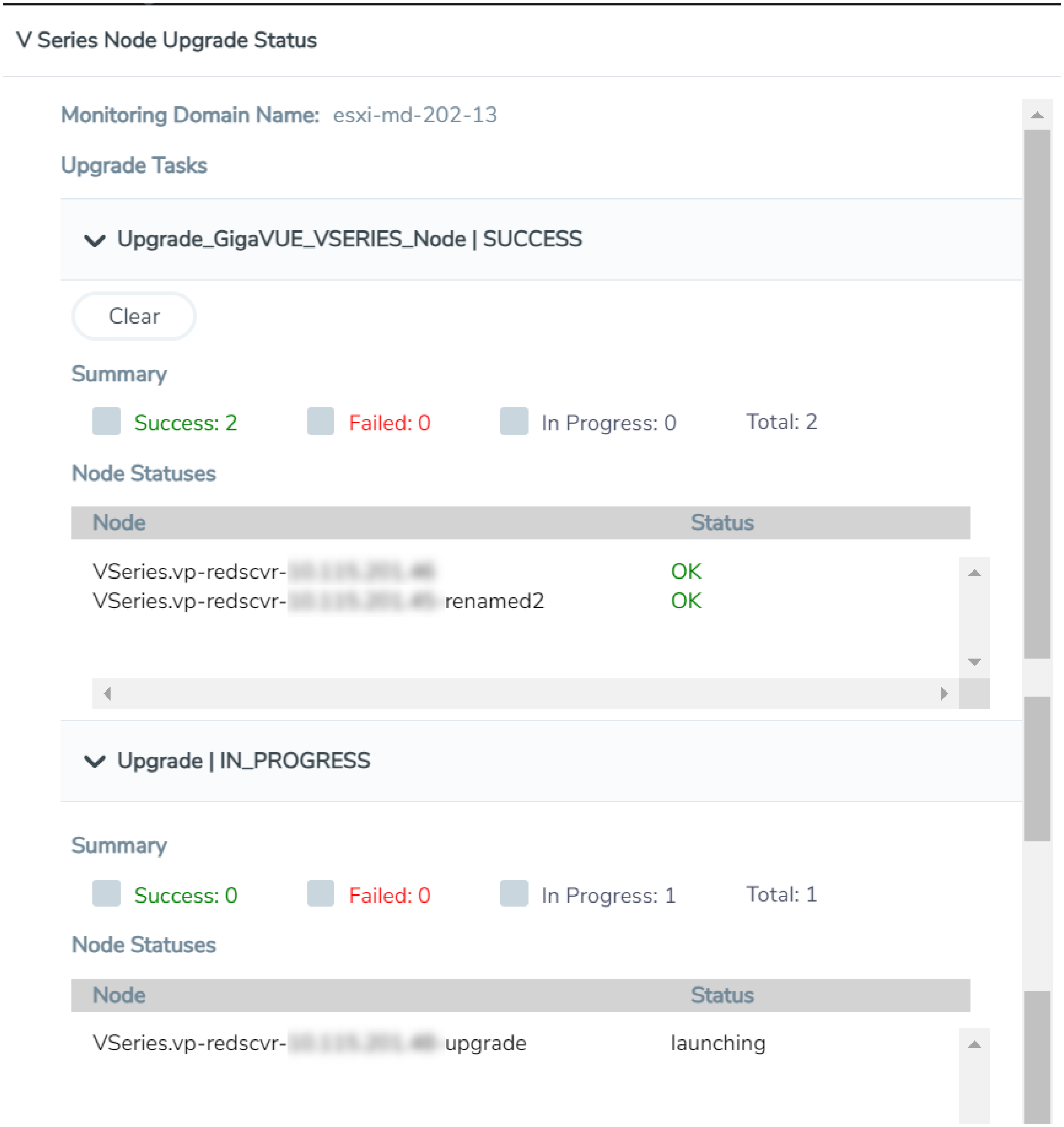
> **NOTE:** Both the new and the current GigaVUE V Series Nodes appear in the same Monitoring Domain until the new nodes replaces the current and the status changes to **Ok**.

You can view the status of the upgrade in the Status column of the **Monitoring Domain** page.



Monitoring Domain	Connections	Host	Name	Management IP	Tunnel IP	Type	Version	Status
md1								Upgrade Status
	con1							✓ Connected
		10.115.81.184						
			VSeries.12310.115.81.184	10.114.82.69	10.114.84.3	V Series Node	6.6.00	⊘ upgrading
			VSeries.new10.115.81.184-1	10.114.84.88	10.114.84.93	V Series Node	6.6.00	⊘ upgrading
		10.115.81.185						
			VSeries.new10.115.81.185-1	10.114.82.143	10.114.84.86	V Series Node	6.6.00	⊘ upgrad
			VSeries.st10.115.81.185-1	10.115.80.190	10.115.80.191	V Series Node	6.6.00	⊘ upgrading

To view the detailed upgrade status click **Upgrade Status**, the **V Series Node Upgrade Status** dialog box appears.



V Series Node Upgrade Status

Monitoring Domain Name: esxi-md-202-13

Upgrade Tasks

Upgrade_GigaVUE_VSERIES_Node | SUCCESS

Summary

□ Success: 2 □ Failed: 0 □ In Progress: 0 Total: 2

Node Statuses

Node	Status
VSeries.vp-redscvr-[redacted]	OK
VSeries.vp-redscvr-[redacted] renamed2	OK

Upgrade | IN_PROGRESS

Summary

□ Success: 0 □ Failed: 0 □ In Progress: 1 Total: 1

Node Statuses

Node	Status
VSeries.vp-redscvr-[redacted] upgrade	launching

- Click **Clear** to delete the monitoring domain upgrade status history of successfully upgraded nodes.
- If the GigaVUE V Series Node upgrade fails or is interrupted for any reason, click on the **Retry** button on the **V Series Node Upgrade Status** dialog box.

NOTE: You cannot modify the node configurations when you are using **Retry** option. GigaVUE -FM uses the same values defined in the initial fabric upgrade configuration.

Configure Secure Communication between Fabric Components in FMHA

IMPORTANT: After upgrading GigaVUE-FM to version 6.10 or later, complete the following steps before upgrading the Fabric Components to version 6.10 or later.

Follow these steps to configure secure communication in FMHA mode:

1. Access the active GigaVUE-FM via CLI.
2. Archive the stepCA directory using the following commands:
```
sudo su
cd /var/lib
tar -cvf /home/admin/stepca.tar stepca
```
3. Change the permissions of the tar file using the following commands:
```
chmod 666 /home/admin/stepca.tar
```
4. Copy the tar file to all standby instances in the **/home/admin/ directory** using scp:
```
scp /home/admin/stepca.tar <standby-node>:/home/admin/
```
5. Download the **runstepca_fmha** script from Community Portal.
6. Access the standby instance using CLI.
7. Copy the script in the standby instance in the **/home/admin directory** and execute it using the following command:
```
sh /home/admin/runstepca_fmha
```

Configure Monitoring Session

GigaVUE-FM collects inventory data on all V Series nodes deployed in your environment through vCenter connections. 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.

NOTE: Pre-filtering is not supported on VMware ESXi running with V Series nodes.

Refer to the following topics for details:

Create a Monitoring Session (VMware)

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 to your Monitoring Session. Similarly, when an instance is removed, it updates the Monitoring Sessions.

For the connections without UCT-Vs, there are no targets that are automatically selected. You can use Customer Orchestrated Source in the Monitoring Session to accept a tunnel from anywhere.

You can create multiple Monitoring Sessions per Monitoring Domain.

To create a new Monitoring Session:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. Click **New Monitoring Session** to open the New Monitoring Session configuration page.
3. In the **Alias** field, enter a name for the Monitoring Session.
4. From the **Monitoring Domain** drop-down list, select the desired Monitoring Domain or click **Create New** to create a new Monitoring Domain. Refer to Create a Monitoring Domain section in the respective cloud guides..
5. From the **Connections** drop-down list, select the required connections that are to be included as part of the Monitoring Domain.

6. Enable the **Distribute Traffic** option to identify duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring.

> **NOTE:** Distributed Deduplication is only supported on GigaVUE V Series Node version 6.5.00 and later.

7. Click **Save**. The Monitoring Session Overview page appears.

Monitoring Session Page (VMware)

You can view the following tabs on the Monitoring Session page:

Tab	Description
Overview	You can view the high level information of the selected Monitoring Session such as, connections, tunnel details, health status, deployment status, and information related to Application Intelligence statistics. You can also view the statistics of the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. You can filter the statistics based on the elements associated with the Monitoring Session. For more information, refer to View Monitoring Session Statistics
Sources	Displays the sources and target details monitored by the Monitoring Session. You can view and edit the connection details of the Monitoring Session. You can view the deployment status, number of targets, and targets source health. **NOTE:** In the case of OVS Mirroring, the Sources tab also displays the Hypervisor details along with the Instances.
Traffic Processing	You can view, add, and configure applications, tunnel endpoints, raw endpoints, and maps. You can view the statistical data for individual applications and also apply threshold template, enable user defined applications, and enable or disable distributed De-duplication. Refer to Configure Monitoring Session Options (VMware ESXi) for more detailed information.
V Series Nodes	You can view the V Series nodes associated with the Monitoring Session. In the split view, you can view details such as name of the V Series Node, health status, deployment status, Host VPC, version, and Management IP. You can also change the interfaces mapped to an individual GigaVUE V Series Node. Refer to Interface Mapping section for details.
Topology	Displays the fabric and monitored instances based on the connections configured in your network. You can select a specific connection to explore its associated subnets and instances in the topology view, offering a clear visualization of the monitored network elements. Refer to Visualize the Network Topology (VMware ESXi).

The Monitoring Session page **Actions** button has the following options. The Actions menu is placed common in all the tabs explained above.

Button	Description
Delete	Deletes the selected Monitoring Session.
Clone	Duplicates the selected Monitoring Session.
Deploy	Deploys the selected Monitoring Session.
Undeploy	Undeploys the selected Monitoring Session.

You can use the ▷ icon on the left side of the Monitoring Session page to view the Monitoring Sessions list. Click ≡ to filter the Monitoring Sessions list. In the side bar, you can:

- Create a new Monitoring Session
- Rename a Monitoring Session
- Hover over, click the check box of the required Monitoring Session(s) and perform bulk actions (Delete, Deploy, or Undeploy).

Configure Monitoring Session Options (VMware ESXi)

In the Monitoring Session page, you can perform the following actions in the **TRAFFIC PROCESSING** tab.

- Apply Threshold Template
- Enable User Defined Applications
- Enable Distributed De-duplication

To navigate to **TRAFFIC PROCESSING** tab, follow the steps given below:

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select a Monitoring Session from the Monitoring Sessions list view on the left side of the screen and click **TRAFFIC PROCESSING** tab.

You can perform the following actions in the **TRAFFIC PROCESSING** page:

Apply Threshold Template

To apply threshold:

1. In the **TRAFFIC PROCESSING** page, select **Thresholds** under **Options** menu.
2. You can select an existing threshold template from the **Select Template** drop-down list, or you can create a new template using **New Threshold Template** option and apply it. Refer to Traffic Health Monitoring section for more details on Threshold Template. Click **Save** to save the newly created template.
3. Click **Apply** to apply the template to the Monitoring Session.

> **NOTE:** You can apply the Threshold configuration to a Monitoring Session before it is deployed. Furthermore, undeploying the Monitoring Session does not remove the applied Thresholds.

You can also view the related details of the applied thresholds, such as Traffic Element, Metric, Type, Trigger Values, and Time Interval in the **Threshold** window. Click **Clear Thresholds** to clear the applied thresholds across the selected Monitoring Session.

Enable User Defined Applications

To enable user defined application, follow the steps given below:

1. In the Monitoring Session **TRAFFIC PROCESSING** page, click **User Defined Applications** under **Options** menu.
2. Enable the **User-defined Applications** toggle button.
3. You can add from the existing applications or create new User-Defined Application from the **Actions** drop-down. Refer to User Defined Application.

Enable Distributed De-duplication

In the TRAFFIC PROCESSING page, click **Distributed De-duplication** under **Options** menu. Enabling the Distributed De-duplication option identifies duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring. Refer to Distributed De-duplication.

> **Notes:**
>
> - Distributed De-duplication is only supported on V Series version 6.5.00 and later.
> - From version 6.9, Traffic Distribution option is renamed to Distributed De-duplication.

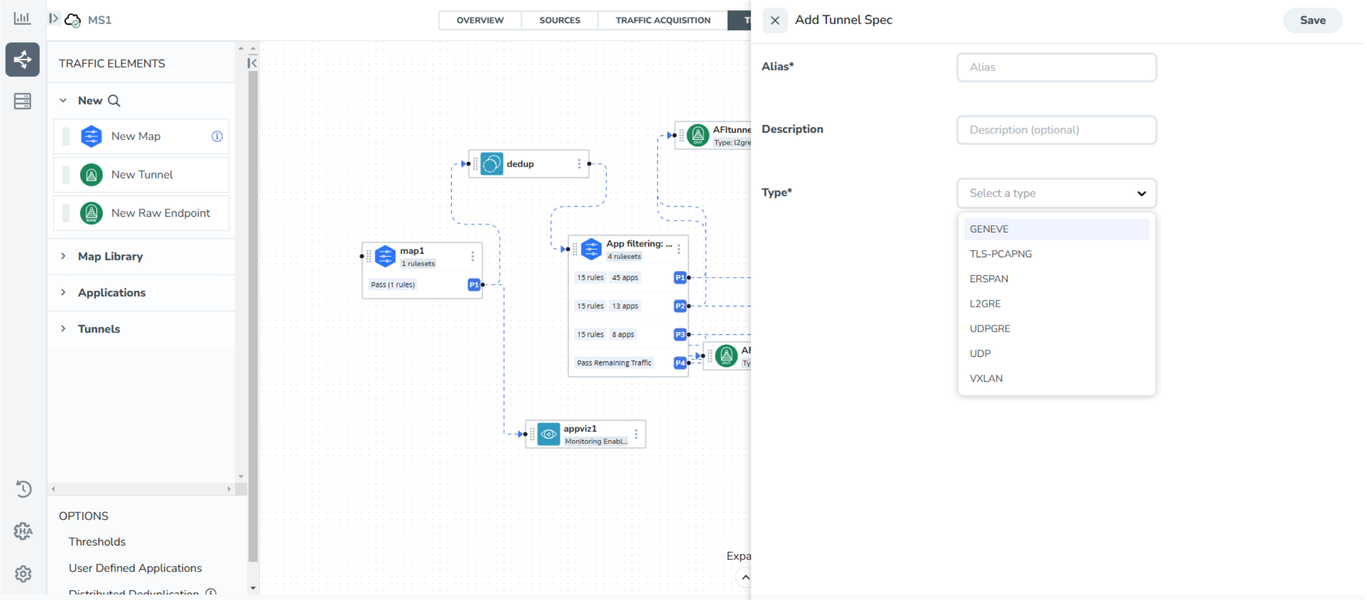
Create Ingress and Egress Tunnel (VMware vCenter)

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, UDPGRE, TLS-PCAPNG, UDP, or ERSPAN tunnel.

> **NOTE:** GigaVUE-FM allows you to configure ingress tunnels in the Monitoring Session, when the **Traffic Acquisition Method** is UCT-V.

To create a new tunnel endpoint:

1. After creating a new Monitoring Session or on an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab. The GigaVUE-FM Monitoring Session canvas page appears.
2. In the canvas, click the icon on the left side of the page to view the traffic processing elements. Select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.
3. Enter the **Alias**, **Description**, and **Type** details. Refer to Details - Add Tunnel Specifications table.



4. Click **Save**.

To delete a tunnel, click the ⋮ menu button of the required tunnel and click **Delete**.

To apply a threshold template to Tunnel End Points, click the ⋮ menu button of the required tunnel end point on the canvas and click **Details**. In the quick view, go to **Threshold** tab. For more details on how to create or apply a threshold template, refer to Monitor Cloud Health topic in the respective Cloud guides.

Tunnel End Points configured can also be used to send or receive traffic from GigaVUE HC Series and GigaVUE TA Series. Provide the IP address of the GigaVUE HC Series and GigaVUE TA Series as the Source or the Destination IP address as required when configuring Tunnel End Points.

After configuring the tunnels and deploying the Monitoring Session, you can view the number of ingress and egress tunnels configured for a Monitoring Session. Click the numbers of tunnels displayed in the **OVERVIEW** tab to view the tunnel names and their respective **ADMIN STATUS** and **HEALTH STATUS**.

Table 1: Details - Add Tunnel Specifications

Field	Description
Alias	The name of the tunnel endpoint.
Description	The description of the tunnel endpoint.
Admin State **Note:** This option appears only after the Monitoring session deployment.	Use this option to send or stop the traffic from GigaVUE-FM to the egress tunnel endpoint. Admin State is enabled by default. You can use this option to stop sending traffic to unreachable tools or tools that are in a down state. Each egress tunnel configured on the GigaVUE V Series Node has an administrative state that enables GigaVUE-FM to halt the tunnel's traffic flow. The tunnels will only be disabled by GigaVUE-FM when it receives a notification via REST API indicating that a tool or group of tools is down. **Note:** This option is not supported for TLS-PCAPNG tunnels.
Type	The type of the tunnel. Select from the below options to create a tunnel. ERSPAN, L2GRE, VXLAN, TLS-PCAPNG, UDP, or UDPGRE.
VXLAN	
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. **Note:** In the scenario where secure tunnels need to be established between a GigaVUE V Series Node and a GigaVUE HC Series, you can utilize the **Configure Physical Tunnel** option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device. Refer to the Secure Tunnels.	
In	Choose **In** (Decapsulation) for creating an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.

Field	Description	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the 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	The port from which the connection will be established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
Out	Choose **Out** (Encapsulation) for creating an egress tunnel from the GigaVUE V Series Node to the destination endpoint.	
	Remote Tunnel IP	For egress tunnel, the 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) is a value that 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 being 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. The 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.
	Multi Tunnel	Enable the multi-tunnel flag to create multiple tunnels for flow distribution to the 5G-Cloud application. Refer to 5G-Cloud Ericson SCP Support. **Applicable Platforms**: OpenStack, Third Party Orchestration, VMware ESXi **NOTE:** You can configure either a single-tep or multi-tep setup for the egress tunnel. Switching between these configurations is not allowed; to make changes, you must undeploy and redeploy the Monitoring Session.

Field	Description	
	Source L4 Port	The port from which the connection will be established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
UDPGRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose **In** (Decapsulation) for creating an ingress tunnel, which will carry 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, the 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 a value between 0 and 4294967295.
	Source L4 Port	The port from which the connection will be established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
L2GRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. **NOTE:** In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the **Configure Physical Tunnel** option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . Refer to the Secure Tunnels.		
In	Choose **In** (Decapsulation)to create an ingress tunnel, which will carry 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, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels.

Field	Description	
		It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a 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, the 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) is a value that 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 being 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. The 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 a 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, the 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	
NOTE: In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the **Configure Physical Tunnel** option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . Refer to Secure Tunnels section.		
In	**IP Version**	The version of the Internet Protocol. Only IPv4 is supported.
	Remote Tunnel IP	For ingress tunnel, the 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.
	Source L4 Port	The port from which the connection will be established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Key Alias	Select the Key Alias from the drop-down.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version 1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the 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.

Field	Description	
Out	**IP Version**	The version of the Internet Protocol. Only IPv4 is supported.
	Remote Tunnel IP	For ingress tunnel, the 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) is a value that 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 being 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. The accepted value is between 0 and 1048575.
	Source L4 Port	The port from which the connection will be established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version 1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the 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.
UDP:		

Field	Description	
Out	**L4 Destination IP Address**	Enter the IP address of the tool port or when using Application Metadata Exporter (AMX), enter the IP address of the AMX application. Refer to Application Metadata Exporter for more detailed information.
	Source L4 Port	The port from which the connection will be established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.

Create Raw Endpoint (VMware vCenter)

This section provides step-by-step instructions on configuring a RAW Endpoint (REP) in the Monitoring Session.

Rules and Notes

- Ingress REP is supported only when the Traffic Acquisition Method is selected as **Customer Orchestrated Source** when configuring the Monitoring Domain. Refer to Create Monitoring Domain for VMware ESXi for more detailed information on how to select the traffic acquisition method.
- GigaVUE-FM expects the IP address to be configured on the GigaVUE V Series Node interface which will be used for creating RAW Endpoint (REP).

Points to Note:

When deploying GigaVUE V Series Nodes in the Monitoring Domain, the number of interfaces varies based on the Traffic Acquisition Method. Refer below for more detailed information:

Traffic Acquisition Method	Display Name	Interface Name	Role	Comments
Customer Orchestrated Source	Network Adapter 1	ens160	Management	
	Network Adapter 2	ens192	Data	Supports Tunnel and RAW endpoint. Can be used for Ingress and Egress REP

Traffic Acquisition Method	Display Name	Interface Name	Role	Comments
	Network Adapter 3	ens224	Data	Supports Tunnel and RAW endpoint. Can be used for Ingress and Egress REP
Platform Tapping	Network Adapter 1	ens160	Management	
	Network Adapter 2	ens192	Data	Supports Tunnel and Egress RAW endpoint.
	Network Adapter 3 - 10	-	Data	Reserved and used for platform tapping (Port Mirroring)

Configure Raw Endpoint in Monitoring Session

Raw End Point (REP) is used to pass traffic from an interface. REP is used to ingress data from a physical interface attached to GigaVUE V Series Nodes. You can optionally use this end point to send traffic to the applications deployed in the monitoring session.

To add Raw Endpoint to the Monitoring Session:

1. Drag and drop **New Raw Endpoint** from the **New** expand menu to the graphical workspace.
2. On the new raw endpoint icon, click the ⋮ menu button and select **Details**. The **Raw** quick view page appears.
3. Enter the Alias and Description details for the Raw End Point and click **Save**.
4. To deploy the Monitoring Session after adding the Raw Endpoint:
   a. Click **Deploy** from the **Actions** drop-down list on the **TRAFFIC PROCESSING** page. The **Deploy Monitoring Session** dialog box appears.
   b. Select the V Series Nodes for which you wish to deploy the Monitoring Session.
   c. 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 V Series Nodes. Click **Deploy**.
5. Click **Export** to download all or selected V Series Nodes in CSV and XLSX formats.

Create a New Map (VMware ESXi)

For new users, the free trial bundle will expire after 30 days, and the GigaVUE-FM prompts you to buy a new license. For licensing information, refer to GigaVUE Licensing Guide.

A map is used to filter the traffic flowing through the GigaVUE V Series Nodes. It is a collection of one or more rules (R). The traffic passing through a map can match one or more rules defined in the map.

Keep in mind the following when creating a map:

Parameter	Description
Rules	A rule (R) contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the targets and the (egress or ingress) direction of tapping the network traffic.
Priority	Priority determines the order in which the rules are executed. The priority value can range from 1 to 5, with 1 being the highest and 5 is the lowest priority.
Pass	The traffic from the virtual machine will be passed to the destination.
Drop	The traffic from the virtual machine is dropped when passing through the map.
Traffic Filter Maps	A set of maps that are used to match traffic and perform various actions on the matched traffic.
Inclusion Map	An inclusion map determines the instances to be included for monitoring. This map is used only for target selection.

Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, and exclusion maps in the Monitoring Session. The below formula describes how ATS works: **Selected Targets = Traffic Filter Maps ∩ Inclusion Maps - Exclusion Maps** Below are the filter rule types that work in ATS: • mac Source • mac Destination • ipv4 Source • ipv4 Destination • ipv6 Source • ipv6 Destination • VM Name Destination • VM Name Source • VM Tag Destination - Not applicable to Nutanix. • VM Tag Source - Not applicable to Nutanix. • VM Category Source - Applicable only to Nutanix. • VM Category Destination - Applicable only to Nutanix. • Host Name -Applicable only to Nutanix and VMware. The traffic direction is as follows: • For any rule type as Source - the traffic direction is egress. • For Destination rule type - the traffic direction is ingress. • For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress. **Notes:** • For OpenStack environment, Subnet Name Source and Subnet Name Destination are the exclusion filters available as part of Exclusion Maps with Traffic Acquisition method as OVS Mirroring in the Monitoring Domain. • If no ATS rule filters listed above are used, all VMs and vNICS are selected as targets. When any ATS rule results in a null set, no target is selected and V Series Node does not receive traffic from any VM or vNIC.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

Rules and Notes:

- Directional rules do not work on single NIC VMs that are running a Windows UCT-V.
- Loopback captures bidirectional traffic from both ingress and egress. To prevent duplicate tapping, only egress tapping is permitted.

- If you are running GigaVUE Cloud Suite on OpenStack, you can add a subnet to the exclusion map. To do this, create an exclusion map and select the Subnet name in the ruleset.
- 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 "Review Map Statistics with Map Rule Counters" section in *GigaVUE Fabric Management Guide* for detailed information.

To create a new map:

1. Drag and drop **New Map** from the **New** expand menu to the graphical workspace. The **Map** quick view appears.
2. On the new Map quick view, click on **General** tab and enter the required information as described below.
   a. Enter the **Name** and **Description** of the new map.
   b. Enable the **Application Filtering** option if you wish to use Application Filtering Intelligence. Enabling this option allows you to filter traffic based on Application name or family. Refer to Application Filtering Intelligence.

      > **NOTE:** 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

3. Click on **Rule Sets** tab.
   a. **To create a new rule set:**
      i. Click **Actions > New Ruleset**.
      ii. Enter a **Priority** value from 1 to 5 for the rule with 1 being the highest and 5 is the lowest priority.
      iii. Enter the Application Endpoint in the Application EndPoint ID field.
      iv. Select a required condition from the drop-down list.
      v. Select the rule to **Pass** or **Drop** through the map.
   b. **To create a new rule:**
      i. Click **Actions > New Rule**.
      ii. Select a required condition from the drop-down list. Click ... and select **Add Condition** to add more conditions.
      iii. Select the rule to **Pass** or **Drop** through the map.
4. Click **Save**.

Through the map, packets can be dropped or passed based on the highest to lowest rule priority. You can add 5 rule sets on a map. Use the + and - buttons to add or remove a rule set in the map. Each rule set can have only 25 rules per map and each rule can have a maximum of 4 conditions. To add ATS rules for an Inclusion/Exclusion map, you must select at least one rule condition. Refer to Example- Create a New Map using Inclusion and Exclusion Maps for more detailed information on how to configure Inclusion and Exclusion maps using ATS.

You can also perform the following action in the Monitoring session canvas.

- To edit a map, click the ⋮ menu button of the required map on the canvas and click **Details**, or click **Delete** to delete the map.
- To apply threshold template to maps, select the required map on the canvas and click **Details**. The quick view appears, click on the Thresholds tab. For more details on how to create or apply threshold templates, refer to Monitor Cloud Health.
- Hover over the rules and apps buttons on the map to view the rule and applications configured for the selected map. Click the rules and apps buttons to open the quick view menu for RULESETS.

Example- Create a New Map using Inclusion and Exclusion Maps

Consider a Monitoring Session with 5 cloud instances. Namely target-1-1, target-1-2, target-1-3, target-2-1, target-2-2.

1. Drag and drop a new map template to the workspace. The New map quick view appears.
2. In the **GENERAL** tab, enter the name as Map 1 and enter the description. In the **RULESETS** tab, enter the priority and Application Endpoint ID.
3. Select the condition as VM Name and enter the **target**. This includes the instances target-1-1, target-1-2, target-1-3, target-2-1, and target-2-2.
4. Click on the Expand icon at the bottom of the Monitoring session canvas. The Inclusion Maps and Exclusion Maps section appears.
5. Drag and drop a new map template to the Inclusion Maps region. The New Map quick view appears. Enter the Name and Description of the map.
   a. In the **GENERAL** tab, enter the name as Inclusionmap1 and enter the description. In the **RULESETS**, enter the priority and Application Endpoint ID.
   b. Select the condition as VM Name and enter the VM Name as **target-1**. Then the instance with VM name **target-1-1, target-1-2,** and **target-1-3** will be included.

6. Drag and drop a new map template to the Exclusion Maps region. The New Map quick view appears. Enter the details as mentioned in the above section.
   a. In the **GENERAL** tab, enter the name as Exclusionmap1 and enter the description. In the **RULESETS** tab, enter the priority and Application Endpoint ID.
   b. Select the condition as VM Name and enter the VM Name as **target-1-3**. Then the instance **target-1-3** will be excluded.

   Based on this configuration, the Automatic Target Selection will select the instances target-1-1 and target-1-2 as target.

Map Library

To reuse a map,

1. In the Monitoring Session page, click **TRAFFIC PROCESSING**. The GigaVUE-FM canvas page appears.
2. Click the map you wish to save as a template. Click **Details**. The Application quick view appears.
3. Click **Add to Library**. Select an existing group from the **Select Group** list or create a **New Group** with a name.
4. Enter a description in the **Description** field, and click **Save**.

The Map is saved to the **Map Library** in the **TRAFFIC PROCESSING** canvas page. This map can be used from any of the Monitoring Session. To reuse the map, drag and drop the saved map from the Map Library.

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
- Slicing
- Masking
- De-duplication
- Load Balancing
- PCAPng Application
- GENEVE Decap
- Header Stripping
- Application Metadata Exporter

- SSL Decrypt
- GigaSMART NetFlow Generation
- 5G-Service Based Interface Application
- 5G-Cloud Application

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

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** landing page appears.
2. Navigate to **V SERIES NODES** tab and click **Interface Mapping**.
3. The **Deploy Monitoring Session** dialog box appears. Select the GigaVUE V Series Nodes for which you wish to map the interface.
4. 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**.

> **NOTE:** When using Raw and Tunnel In, Interface Mapping is mandatory before you deploy the Monitoring Session.

Deploy Monitoring Session

To deploy the Monitoring Session:

1. Drag and drop the following items to the canvas as required:
   a. Ingress tunnel (as a source) from the **New** section.
   b. Maps from the **Map Library** section.
   c. Inclusion and Exclusion maps from the Map Library to their respective section at the bottom of the workspace.
   d. GigaSMART apps from the **Applications** section.
   e. Egress tunnels from the **Tunnels** section.

2. After placing the required items in the canvas, hover your mouse on the map, click the dotted lines, 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.

3. (Not applicable for NSX-T solution and Customer Orchestrated Source as Traffic Acquisition Method) Click **SOURCES** tab to view details about the subnets and monitored instances.
4. Click **Deploy** from the **Actions** menu to deploy the Monitoring Session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on all the V Series Nodes.
5. You can view the Monitoring Session Deployment Report in the **SOURCES** and **V SERIES NODES** tab. When you click on the Status link, the Deployment Report is displayed. If the Monitoring Session is not deployed properly, then one of the following errors is displayed in the Status column.
   - Success—The session is not deployed on one or more instances due to V Series Node failure.
   - Failure—The session is not deployed on any of the V Series Nodes or Instances.

   The **Monitoring Session Deployment Report** displays the errors that appeared during deployment.

View Monitoring Session Statistics

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

You can view the high level information of the selected Monitoring Session such as, connections, tunnel details, health status, deployment status, and information related to Application Intelligence statistics. You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab.

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

- You can view the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis.
- 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 in the **TOTAL TRAFFIC** section of the **OVERVIEW** page.
- You can also view the statistics of the Monitoring Session deployed in the individual V Series Nodes. To view the statistics of the individual GigaVUE V Series Node, select the

name of the **V Series Node** for which you want to view the statistics from the GigaVUE V Series Node drop-down list on the bottom left corner of the **OVERVIEW** page.

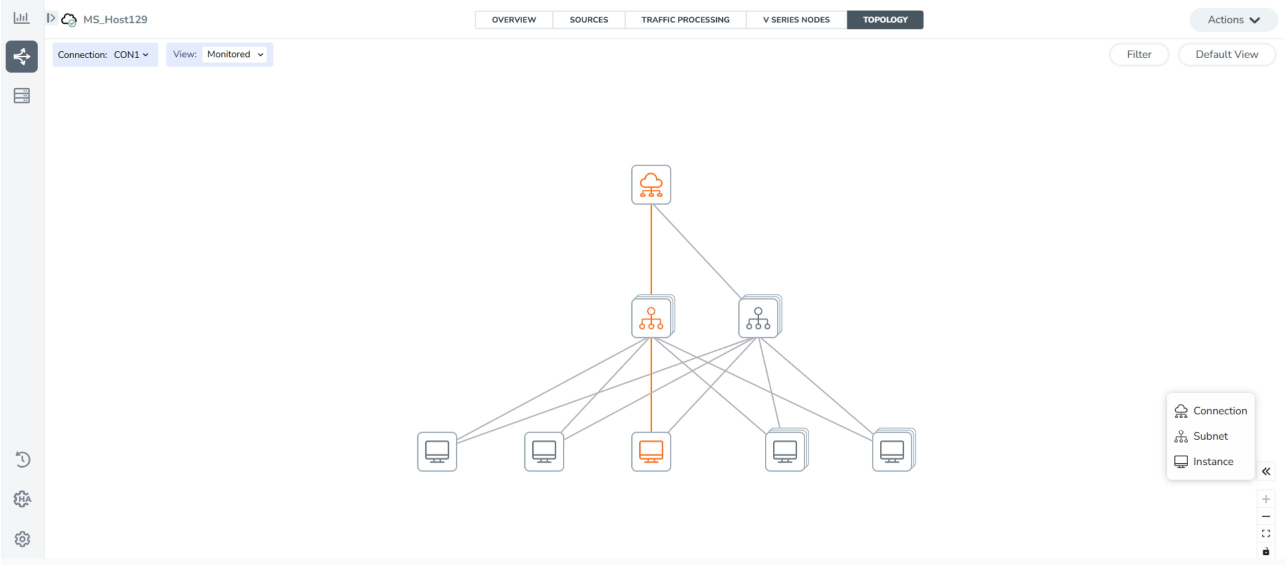
> Raw EndPoint (REP) is a part of the monitoring session but can also receive the bypassed traffic that is not filtered by the map, so it is recording more packets than expected. For example, if the map has a rule as IPv4, but the REP can receive the bypassed (non-ipv4) traffic. The recorded number of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

Visualize the Network Topology (VMware ESXi)

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 in GigaVUE-FM:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. After creating a new Monitoring Session or on an existing Monitoring Session, navigate to the **TOPOLOGY** tab. The Topology page appears.
3. Select a connection from the **Connection** list. The topology view of the monitored subnets and instances in the selected session are displayed.
4. Select the instance type from **View**. The available instance types are Fabric and Monitored.



5. (Optional) Hover over the subnet or VM group icons to view details such as the subnet ID, subnet range, and the total number of subnets and instances. Click the subnet or VM group icons to explore the subnets or instances 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, OS Type, 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 monitored instances.
- Use **+** or **-** icons to zoom in and zoom out the topology view.
- Click the **Fit View** icon to fit the topology diagram according to the width of the page.

Migrate Application Intelligence Session to Monitoring Session

Starting from Software version 6.5.00, Application Intelligence solution can be configured from Monitoring Session Page. After upgrading to 6.5.00, you cannot create a new Application Intelligence Session or edit an existing Application Intelligence Session for virtual environment from the **Application Intelligence** page. The following operations can only be performed using the existing Application Intelligence Session:

- View Details
- Delete
- Forced Delete

It is highly recommended to migrate the existing sessions to Monitoring Session for full functionality. GigaVUE-FM will migrate all your virtual Application Intelligence sessions and their connections seamlessly. All sessions will be rolled back to their original states if the migration fails.

Points to Note:

- You must be a user with write access for the **Traffic Control Management** Resource in GigaVUE-FM to perform this migration. Refer to Create Roles section In GigaVUE Administration Guide for more detailed information on how to configure roles with write access for the Traffic Control Management resource.
- If any of the existing Application Intelligence Session is in PENDING or SUSPENDED, then the migration will not be triggered. Resolve the issue and start the migration process.

- If any of the existing Application Intelligence Session is in FAILED state due to incorrect configuration, then the migration will not be triggered. Resolve the issue and start the migration process.
- If an existing Monitoring Session has a same name as the Application Intelligence Session, then the migration will not be triggered. Change the existing Monitoring Session name to continue with the migration process.
- If any of the existing Application Intelligence Session has Application Filtering configured with Advanced Rules as Drop Rule and No Rule Match Pass All in the 5th rule set, you cannot continue with the migration. In the Monitoring Session either only Pass All or Advanced Rules as Drop is supported in the fifth Rule Set. Please delete this session and start the migration.
- When migrating the Application Intelligence Session, in rare scenarios, the migration process might fail after the pre-validation. In such cases, all the Application Intelligence Session roll back to the Application Intelligence page. Contact Technical Support for migrating the Application Intelligence Session in these scenarios.

To migrate your existing Application Intelligence Session to Monitoring Session Page, follow the steps given below:

1. On the left navigation pane, select **Traffic > Solutions >Application Intelligence**. You cannot create a new Application Intelligence Session from this page.
2. When you have an existing virtual Application Intelligence Session in the above page, the **Migrate Virtual Application Intelligence** dialog box appears.
3. Review the message and click **Migrate.**
4. The **Confirm Migration** dialog box appears. The list Application Intelligence Session that will be migrated appears here.
5. Review the message and click **Migrate**.
6. GigaVUE-FM checks for the requirements and then migrates the Application Intelligence Sessions to the Monitoring Session Page.
7. Click on the **Go to Monitoring Session Page** button to view the Application Intelligence Session that are migrated to the monitoring session page.

All the virtual Application Intelligence Sessions in the Application Intelligence page is migrated to the Monitoring Session Page.

Post Migration Notes for Application Intelligence

After migrating Application Intelligence session to Monitoring Session page, you must consider the following things:

1. If you wish to enable Secure tunnels after migrating the Application Intelligence Session, follow the steps given below.
   a. Enable Secure Tunnels in the **Options** page. Refer to Configure Monitoring Session Options (VMware ESXi) topic more detailed information on how to enable secure tunnel for a monitoring Session.
   b. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears. Select the Monitoring Session for which you enabled Secure Tunnels. Click **Actions > Undeploy**. The monitoring session is undeployed.
   c. Select the Monitoring Session for which you enabled Secure Tunnels. Click **Actions > Edit**. The **Edit Monitoring Session** Canvas page appears.
   d. Add the Application Intelligence applications.
   e. Modify the Number of Flows as per the below table:

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

   NOTE: Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k.

   f. Click **Deploy**. Refer to Application Intelligence section in the GigaVUE V Series Applications Guide for more detailed information on how to deploy the Application Intelligence applications.

2. When GigaVUE-FM version is 6.5.00, and the GigaVUE V Series Node version is below 6.5.00, after migrating theApplication Intelligence Session to the Monitoring Session and redeploying the monitoring session, a momentary loss in the statistical data of the Application Visualization application will be seen while redeploying the monitoring session.

3. After migrating the Application Intelligence Session to monitoring session, if you wish to make any configuration changes, then the GigaVUE V Series Node version must be greater than or equal to 6.3.00.

Monitor Cloud Health

GigaVUE-FM allows you to monitor the traffic and configuration health status of the monitoring session and its individual components. This section provides detailed information on how to view the traffic and configuration health status of the monitoring session and its individual components. Refer to the following topics for more detailed information on configuration health, traffic health and how to view the health status:

- Configuration Health Monitoring
- Traffic Health Monitoring
- View Health Status

Configuration Health Monitoring

The configuration health status provides us 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:

Configuration Health Monitoring	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware	GigaVUE Cloud Suite for Nutanix
GigaVUE V Series Nodes	✓	✓	✓	✓	✓
UCT-V	✓	✓	✓	×	×
VPC Mirroring	✓	×	×	×	×
OVS Mirroring and VLAN Trunk Port	×	×	✓	×	×

To view the configuration health status, refer to the View Health Status section.

Traffic Health Monitoring

GigaVUE-FM allows you to monitor the traffic health status of the entire Monitoring Session and also the individual V Series Nodes for which the Monitoring Session is configured. Traffic health monitoring focuses on identifying any discrepancies (packet drop or overflow etc) in the traffic flow. When any such discrepancies are identified, GigaVUE-FM propagates the health status to corresponding Monitoring Session. GigaVUE-FM monitors the traffic health status in near real-time. GigaVUE V Series Node monitors the traffic, when the traffic limit goes beyond the upper or lower threshold values that is configured, it notifies GigaVUE-FM, based on which traffic health is computed.

> **NOTE:** When GigaVUE-FM and GigaVUE V Series Nodes are deployed in different cloud platforms, then the GigaVUE-FM public IP address must be added to the **Data Notification Interface** as the Target Address in the Event Notifications page. Refer to the section in the *GigaVUE Administration Guide* for configuration details.

This feature is supported for GigaVUE V Series Nodes on the respective cloud platforms:

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware
- Third Party Orchestration

The following section gives step-by-step instructions on creating and applying threshold templates across a Monitoring Session or an application, and viewing the traffic health status. Refer to the following section for more detailed information:

- Supported Resources and Metrics
- Create Threshold Templates
- Apply Threshold Template
- Clear Thresholds

Keep in mind the following points when configuring a threshold template:

- By default, Threshold Template is not configured to any Monitoring Session. If you wish to monitor the traffic health status, then create and apply threshold template to the Monitoring Session.
- Editing or redeploying the Monitoring Session will reapply all the threshold policies associated with that Monitoring Session.
- Deleting the Monitoring Session will clear all the threshold policies associated with that Monitoring Session.
- Threshold configuration can be applied before deploying a Monitoring Session and remains even if the session is undeployed.
- After applying threshold template to a particular application, you need not deploy the Monitoring Session again.

Supported Resources and Metrics

The following table lists the resources and the respective metrics supported for traffic health monitoring

Resource	Metrics	Threshold types	Trigger Condition
Tunnel End Point	1. Tx Packets 2. Rx Packets 3. Tx Bytes 4. Rx Bytes 5. Tx Dropped 6. Rx Dropped 7. Tx Errors 8. Rx Errors	1. Difference 2. Derivative	1. Over 2. Under
RawEnd Point	1. Tx Packets 2. Rx Packets 3. Tx Bytes 4. Rx Bytes 5. Tx Dropped 6. Rx Dropped 7. Tx Errors 8. Rx Errors	1. Difference 2. Derivative	1. Over 2. Under
Map	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Slicing	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Masking	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Dedup	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
HeaderStripping	1. Tx Packets	1. Difference	1. Over

	2. Rx Packets 3. Packets Dropped	2. Derivative	2. Under
TunnelEncapsulation	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
LoadBalancing	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
SSLDecryption	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Application Metadata	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
AMI Exporter	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Geneve	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
5G-SBI	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
SBIPOE	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
PCAPNG	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under

Create Threshold Templates

To create threshold templates:

1. Go to **Inventory > Resouces > Threshold Templates**.
2. The **Threshold Templates** page appears. Click **Create** to open the New Threshold Template page.
3. Enter the appropriate information for the threshold template as described in the following table.

Field	Description
Threshold Template Name	The name of the threshold template.
Thresholds	
Traffic Element	Select the resource for which you wish to apply the threshold template. Ex: TEP, REP, Maps, Applications like Slicing, De-dup etc
Time Interval	Frequency at which the traffic flow needs to be monitored.
Metric	Metrics that need to be monitored. For example: Tx Packets, Rx Packets.
Type	**Difference**: The difference between the stats counter at the start and end time of an interval, for a given metric. **Derivative**: Average value of the statistics counter in a time interval, for a given metric.
Condition	**Over**: Checks if the statistics counter value is greater than the 'Set Trigger Value'. **Under**: Checks if the statistics counter value is lower than the 'Set Trigger Value'.
Set Trigger Value	Value at which a traffic health event is raised, if statistics counter goes below or above this value, based on the condition configured.
Clear Trigger Value	Value at which a traffic health event is cleared, if statistics counter goes below or above this value, based on the condition configured.

4. Click **Save**. The newly created threshold template is saved, and it appears on the **Threshold** templates page.

Apply Threshold Template

You can apply your threshold template across the entire Monitoring Session and also to a particular application.

Apply Threshold Template to Monitoring Session

To apply the threshold template across a Monitoring Session, follow the steps given below:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. In the **TRAFFIC PROCESSING** tab, select **Thresholds** under **Options** menu.

3. From the **Select Template** drop-down list, select the template you wish to apply across the Monitoring Session.
4. Click **Apply**.

> **NOTE:** You can apply the Threshold configuration to a Monitoring Session before it is deployed. Furthermore, undeploying the Monitoring Session does not remove the applied Thresholds.

Apply Threshold Template to Applications

To apply the threshold template to a particular application in the Monitoring Session follow the steps given below:

> **NOTE:** Applying threshold template across Monitoring Session will not over write the threshold value applied specifically for an application. When a threshold value is applied to a particular application, it over writes the existing threshold value for that particular application.

1. On the **Monitoring Session** page. Click **TRAFFIC PROCESSING** tab. The Monitoring Session canvas page appears.
2. Click on the application for which you wish to apply or change a threshold template and click **Details**. The **Application** quick view opens.
3. Click on the **Thresholds** tab. Select the template you wish to apply from the Threshold Template drop-down menu or enter the threshold values manually.
4. Click **Save**.

Clear Thresholds

You can clear the thresholds across the entire Monitoring Session and also to a particular application.

Clear Thresholds for Applications

To clear the thresholds of a particular application in the Monitoring Session follow the steps given below:

1. On the **Monitoring Session** page, click **TRAFFIC PROCESSING** tab. The Monitoring Session canvas page appears.
2. Click on the application for which you wish to clear the thresholds and click **Details**. The **Application** quick view opens.
3. Click on the **Thresholds** tab. Click **Clear All** and then Click **Save**.

Clear Thresholds across the Monitoring Session

To clear the applied thresholds across a Monitoring Session follow the steps given below:

1. In GigaVUE-FM, on the left navigation pane, go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. Select the Monitoring Session and navigate to **TRAFFIC PROCESSING > Options > Thresholds**, click **Clear Thresholds**.
3. The **Clear Threshold** pop-up appears. Click **Ok**.

NOTE: Clearing thresholds at Monitoring Session level does not clear the thresholds that were applied specifically at the application level. To clear thresholds for a particular application refer to Clear Thresholds for Applications

View Health Status

You can view the health status of the Monitoring Session on the Monitoring Session details page. The health status of the Monitoring Session is healthy only if both the configuration health and traffic health are healthy.

View Health Status of an Application

To view the health status of an application across an entire Monitoring Session:

1. After creating a Monitoring Session, go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. Select a Monitoring Session and navigate to **TRAFFIC PROCESSING** tab.
2. Click on the application for which you wish to see the health status and select **Details**. The quick view page appears.
3. Click on the **HEALTH STATUS** tab.

This displays the configuration health and traffic health of the application and also the thresholds applied to that particular application.

NOTE: The secure tunnel status is refreshed for every 5 minutes, and the GigaVUE-FM does not display UCT-V secure tunnel status that is older than 7 minutes. If the secure tunnel in the UCT-V is removed, it takes up to 7 minutes to reset the status on the GigaVUE-FM.

View Health Status for Individual GigaVUE V Series Nodes

You can also view the health status of the view the health status of an individual GigaVUE V Series Node. To view the configuration health status and traffic health status of the V Series Nodes:

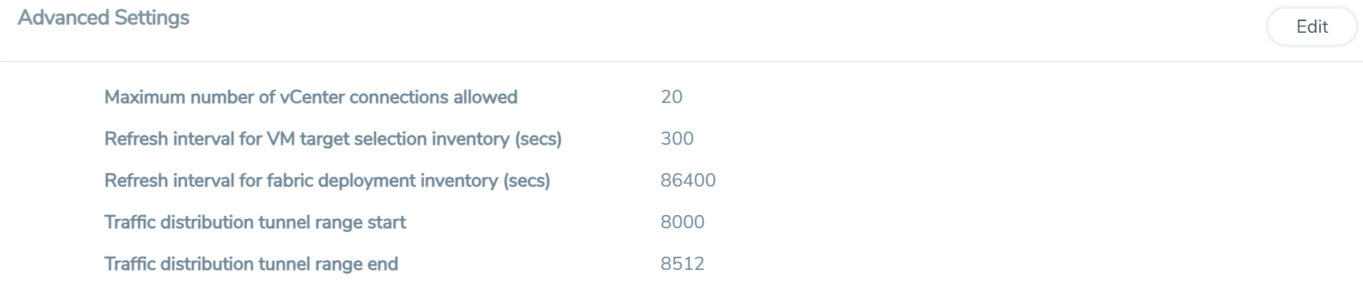
1. On the Monitoring Session page, click the required Monitoring Session from the list view.
2. In the **Overview** tab, you can view the health status of the required GigaVUE V Series Node from the chart options.

Configure VMware Settings

This section provides information on how to configure the maximum number of connections, refresh intervals for instance and non-instance inventory, and maximum batch size for monitoring session updates.

To configure the VMware Settings:

Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, and then click **Settings > Advanced Settings** to edit the VMware vCenter settings.



Advanced Settings

Maximum number of vCenter connections allowed	20
Refresh interval for VM target selection inventory (secs)	300
Refresh interval for fabric deployment inventory (secs)	86400
Traffic distribution tunnel range start	8000
Traffic distribution tunnel range end	8512

Refer to the following table for details:

Settings	Description
Maximum number of vCenter connections allowed	Specifies the maximum number of vCenter 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 VMware vCenter
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for updating the state of GigaVUE-FM fabrics deployed in VMware vCenter
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.

Configure Certificate Settings

To configure certificate settings:

1. Go to **Inventory > VIRTUAL**. Select your cloud platform.
2. Click **Settings > Certificate Settings**. The **Certificate Settings** page appears.
3. From the **Algorithm** drop-down list, select the algorithm that determines the cryptographic security of the certificate.

   > **NOTE:** If selecting RSA 8192, note that certificate generation may take longer due to the increased key size.

4. In the **Validity** field, enter the total validity period of the certificate.
5. In the **Auto Renewal** field, enter the number of days before expiration the auto-renewal process should begin.
6. Click **Save**.

Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics[1] 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 section in *GigaVUE Fabric Management Guide* for more detailed information on Analytics.

Rules and Notes:

- You cannot edit or delete these default dashboards. However, you can clone the dashboards and visualizations. Refer to the Clone Dashboard section in GigaVUE-FM Installation and Upgrade Guidefor more details.
- Use the Time Filter option to select the required time interval for which you need to view the visualization.

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

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: • 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: • Platform • Health Status	*V Series Node Status by Platform*	Number of healthy and unhealthy V Series Nodes for each of the supported cloud platforms.
		Monitoring Session Status by Platform	Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms
		Connection Status by Platform	Number of healthy and unhealthy connections for each of the supported cloud platforms
		GCB Node Status by Platform	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 receiving and transmitting packets of the V Series node. You can filter the visualizations based on the following control	*V Series Node Maximum CPU Usage Trend*	Line chart that displays maximum CPU usage trend of the V Series node in 5 minutes interval, for the past one hour.

Dashboard	Displays	*Visualizations*	Displays
	filters: • Platform • Connection • V Series Node		**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.
		V Series Node with Most CPU Usage For Past 5 minutes	Line chart that displays Maximum CPU usage of the V Series node for the past 5 minutes. **NOTE:** You cannot use the time based filter options to filter and visualize the data.
		V Series Node Rx Trend	Receiving trend of the V Series node in 5 minutes interval, for the past one hour.
		V Series Network Interfaces with Most Rx for Past 5 mins	Total packets received by each of the V Series network interface for the past 5 minutes. **NOTE:** You cannot use the time based filter options to filter and visualize the data.
		V Series Node Tunnel Rx Packets/Errors	Displays the reception of packet at the Tunnel RX. This is the input to V Series Node, Grouping by tunnel identifier comprising {monDomain, conn, VSN, tunnelName}, before aggregation.

Dashboard	Displays	*Visualizations*	Displays
		V Series Node Tunnel Tx Packets/Errors	TX is for output tunnels from VSN. V Series Node Tunnel Tx Packets/Errors
Dedup	Displays visualizations related to Dedup application. You can filter the visualizations based on the following control filters: - Platform - Connection - V Series Node	*Dedup Packets Detected/Dedup Packets Overload*	Statistics of the total de-duplicated packets received (ipV4Dup, ipV6Dup and nonIPDup) against the de-duplication application overload.
		Dedup Packets Detected/Dedup Packets Overload Percentage	Percentage of the de-duplicated packets received against the de-duplication application overload.
		Total Traffic In/Out Dedup	Total incoming traffic against total outgoing traffic
Tunnel (Virtual)	Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets. You can select the following control filters, based on which the visualizations will get updated: - **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. - **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.	*Tunnel Bytes*	Displays received tunnel traffic vs transmitted tunnel traffic, in bytes. - For input tunnel, transmitted traffic is displayed as zero. - For output tunnel, received traffic is displayed as zero.

Dashboard	Displays	*Visualizations*	Displays
	The following statistics are displayed for the tunnel: • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets • Received Dropped Packets • Transmitted Errored Packets • Transmitted Dropped Packets		
		Tunnel Packets	Displays packet-level statistics for input and output tunnels that are part of a monitoring session.
App (Virtual)	Displays Byte and packet level statistics for the applications for the chosen monitoring session on the selected V Series node. You can select the following control filters, based on which the visualizations will get updated: • **Monitoring session** • **V Series node** • **Application**: Select the required application. By default, the visualizations displayed includes all the applications. By default, the following statistics are displayed: • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Errored Packets • Dropped Packets	*App Bytes*	Displays received traffic vs transmitted traffic, in Bytes.

Dashboard	Displays	*Visualizations*	Displays
		App Packets	Displays received traffic vs transmitted traffic, as the number of packets.
End Point (Virtual)	Displays Byte and packet level statistics for the un-tunneled traffic deployed on the V Series nodes. The following statistics that are shown for Endpoint (Virtual): • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets • Received Dropped Packets • Transmitted Errored Packets • Transmitted Dropped Packets The endpoint drop-down shows *<V Series Node Management IP address : Network Interface>* for each endpoint. You can select the following control filters, based on which the visualizations will get updated: • **Monitoring session** • **V Series node** • **Endpoint:** Management IP of the V Series node followed by the Network Interface (NIC)	*Endpoint Bytes*	Displays received traffic vs transmitted traffic, in Bytes.
		Endpoint Packets	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.

Debuggability and Troubleshooting

Refer to the following topics for details:

Sysdumps

A sysdump is a collection of logs and system data that are used for debugging purposes. A sysdump is generated when a GigaVUE V Series Node crashes (e.g., kernel, application, or hardware crash).

> **NOTE:** If the fabric component is deleted or unreachable, the sysdump files cannot be downloaded.

Sysdumps—Rules and Notes

Keep in mind the following points before you generate sysdumps:

- You can generate only one sysdump file at a time for a GigaVUE V Series Node.
- You cannot generate a sysdump file when another sysdump file generation is in progress.
- The limit of sysdump files available per GigaVUE V Series Node is six. When you generate a seventh sysdump file, the file overwrites the first sysdump file.
- You can download only one sysdump file per GigaVUE V Series Node at a time.
- You can delete sysdump files in bulk for a GigaVUE V Series Node.
- To ensure efficient usage, the system will limits the number of simultaneous sysdump generation requests to 10 GigaVUE V Series Nodes.
- GigaVUE V Series Node sysdumps are not stored in Fabric Manager but generated and stored on the GigaVUE V Series Node itself.

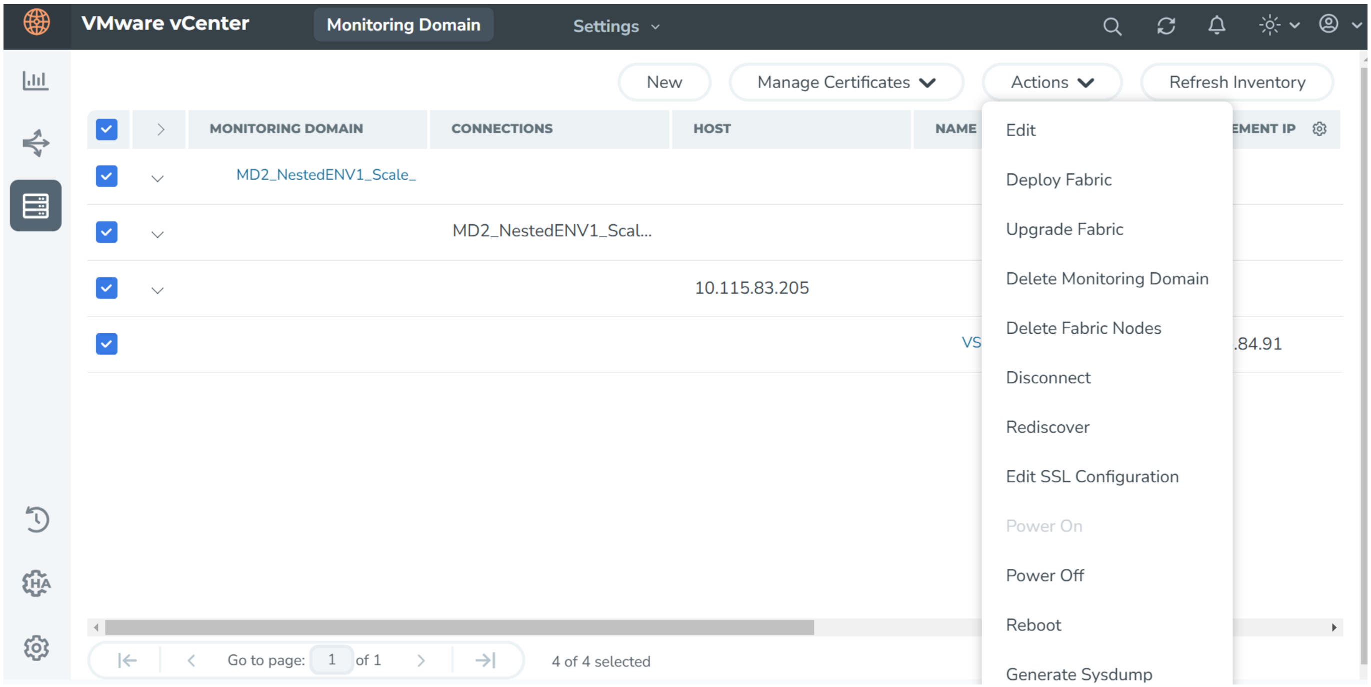
Generate a Sysdump File

To generate a sysdumps file:

1. Go to **Inventory > VIRTUAL > VMware ESXi > Monitoring Domain.** The **Monitoring Domain** page appears.
2. Select the required node, and use one of the following options to generate a sysdump file:

- Click **Actions > Generate Sysdump**.
- In the lower pane, go to **Sysdump**, and click **Actions > Generate Sysdump**.

To view the latest status, click **Refresh**.



MONITORING DOMAIN	CONNECTIONS	HOST	NAME	EMENT IP
MD2_NestedENV1_Scale_				
	MD2_NestedENV1_Scal...			
		10.115.83.205		
			VS	.84.91

To download a sysdump file, select the file in the lower pane, and then click **Actions > Download**.
To delete a sysdump file, select the file in the lower pane, and then select a sysdump file to delete. Click **Actions > Delete**. To bulk delete, select all the sysdump files, and then click **Actions > Delete All.**

FAQs - Secure Communication between GigaVUE Fabric Components

This section addresses frequently asked questions about Secure Communication between GigaVUE Fabric Components and GigaVUE-FM. Refer to Secure Communication between GigaVUE Fabric Components section for more details.

1. **Is there a change in the upgrade process for GigaVUE-FM and GigaVUE V Series Node?**

   There are no modifications to the behavior across any of the upgrade paths. You may proceed with upgrades without the necessity for any additional steps. Upon upgrading the nodes, the corresponding certificates will be deployed in accordance with the respective node versions.

GigaVUE-FM	GigaVUE V Series Nodes	Custom Certificates Selected (Y/N)	Actual Node Certificate
6.10	6.10	Y	GigaVUE-FM PKI Signed Certificate
6.10	6.9 or earlier	Y	Custom Certificate
6.10	6.9 or earlier	N	Self Signed Certificate

2. **What is the new authentication type used between GigaVUE-FM and the GigaVUE Fabric Components? Is backward compatibility supported?**

   Backward compatibility is supported, ensuring that fabric components running on version 6.9 or earlier remain compatible with GigaVUE-FM 6.10. The following authentication types are supported across different versions.

GigaVUE-FM	GigaVUE Fabric Components	Authentication
6.10	6.10	Tokens + mTLS Authentication (Secure Communication)
6.10	6.9 or earlier	User Name and Password

3. **What are the new ports that must be added to the security groups?**

   The following table lists the ports numbers that needs to be opened for the respective fabric components.

Component	Port
GigaVUE-FM	9600
GigaVUE V Series Node	80
GigaVUE V Series Proxy	8300, 80
UCT-V Controller	8300, 80
UCT-V	8301, 8892, 9902 For more details, refer to Prerequisites for AWS.

4. **Are there any changes to the registration process for deploying the fabric components using Third Party Orchestration?**

   Starting from version 6.10, you must place tokens in the gigamon-cloud.conf file instead of username and password. To generate the token in GigaVUE-FM, go to **Settings > Authentication > User Management > Token**. Refer to Configure Tokens for Third Party Orchestration for more details.

   Example Registration Data for UCT-V:

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        token: <Token>
        remoteIP: <IP address of the UCT-V Controller 1, <IP address of the UCT-V Controller
2>
        sourceIP: <IP address of UCT-V> (Optional Field)
```

5. **Are there any changes to the UCT-V manual installation and upgrade process?**

   Starting from version 6.10, you must add tokens during manual installation and upgrades. You must create a configuration file named gigamon-cloud.conf with the token and place it in the /tmp directory during UCT-V installation or after installing UCT-V you can add the configuration file in the /etc directory.

   > **NOTE:** UCT-V will not be added to GigaVUE-FM without this token.

6. **Can you use your own PKI infrastructure to issue certificates for the Fabric Components?**

   Integrating your Public Key Infrastructure (PKI) with GigaVUE-FM is not feasible. However, you can provide your Intermediate Certificate Authority (CA) to sign the node certificate.

7. **What happens to the existing custom certificates introduced in the 6.3 release?**
   - The custom certificate feature is not supported for the fabric components with version 6.10 or higher, even if a custom certificate is selected in the Monitoring Domain. However, this feature remains available for older versions.
   - When a fabric component with version 6.9 or earlier with custom certificates upgrades to version 6.10, new fabric components will be launched with certificates signed by the GigaVUE-FM, and custom certificates will no longer be used in fabric components with version 6.10 or above versions.
   - When GigaVUE-FM is running on version 6.10 and deploying fabric components with version 6.9 or earlier, selecting a custom certificate ensures that the fabric components are deployed with the specified custom certificates.

8. **How to issue certificates after upgrading the fabric components to 6.10?**

   When the upgrade process begins, GigaVUE-FM will transmit the certificate specifications to the new fabric components using the launch script. The fabric components will then utilize these specifications to generate its own certificate.

9. **Is secure communication supported in FMHA deployment?**

   Yes, it is supported. However, you must follow a few manual steps before upgrading the fabric components to 6.10. Refer to Configure Secure Communication between Fabric Components in FMHA for more details.

   > **NOTE:** This step is essential exclusively if you are using cloud deployments in FMHA mode and need to deploy or upgrade the fabric components to version 6.10 or later.

Additional Sources of Information

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

- Documentation
- Documentation Feedback
- Contact Technical Support
- Contact Sales
- The VÜE Community

Documentation

This table lists all the guides provided for GigaVUE 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 6.10 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware how to unpack, assemble, rackmount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-HCT Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide
GigaVUE-TA100 Hardware Installation Guide

GigaVUE Cloud Suite 6.10 Hardware and Software Guides
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 Appliances Guide
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
GigaVUE Application Intelligence Solutions Guide
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Applications Guide
GigaVUE Cloud Suite Deployment Guide - AWS
GigaVUE Cloud Suite Deployment Guide - Azure
GigaVUE Cloud Suite Deployment Guide - OpenStack
GigaVUE Cloud Suite Deployment Guide - Nutanix
GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
Universal Cloud TAP - Container Deployment Guide

GigaVUE Cloud Suite 6.10 Hardware and Software Guides

Gigamon Containerized Broker Deployment Guide

GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions

GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions

Reference Guides

GigaVUE-OS CLI Reference Guide

library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices

GigaVUE-OS Security Hardening Guide

GigaVUE Firewall and Security Guide

GigaVUE Licensing Guide

GigaVUE-OS Cabling Quick Reference Guide

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

GigaVUE-OS Compatibility and Interoperability Matrix

compatibility information and interoperability requirements for Gigamon devices

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

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

Factory Reset Guidelines for GigaVUE-FM and GigaVUE-OS Devices

Sanitization guidelines for GigaVUE Fabric Management Guide and GigavUE-OS devices.

Release Notes

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

new features, resolved issues, and known issues in this release ;

important notes regarding installing and upgrading to this release

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

> **NOTE:** Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software and Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.

In-Product Help

GigaVUE-FM Online Help

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

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

Documentation Feedback Form		
About You	**Your Name**	
	Your Role	
	Your Company	

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The VÜE Community

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

Visit the VÜE Community site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

The VÜE Community is a great way to get answers fast, learn from experts and collaborate directly with other members around your areas of interest.

Register today at community.gigamon.com

Questions? Contact our Community team at community@gigamon.com.

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

follower in clustering node relationship (formerly slave or non-master)

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

root timing; transmits sync info to clocks in its network segment (formerly grandmaster)

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)