



# GigaVUE Cloud Suite Deployment Guide - Azure

## **GigaVUE Cloud Suite**

Product Version: 6.4

Document Version: 1.0

Last Updated: Tuesday, February 27, 2024

(See Change Notes for document updates.)

**Copyright 2024 Gigamon Inc.. All rights reserved.**

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

**Trademark Attributions**

Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at [www.gigamon.com/legal-trademarks](http://www.gigamon.com/legal-trademarks). All other trademarks are the trademarks of their respective owners.

Gigamon Inc.  
3300 Olcott Street  
Santa Clara, CA 95054  
408.831.4000

# Change Notes

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

<b>Product Version</b>	<b>Document Version</b>	<b>Date Updated</b>	<b>Change Notes</b>
6.4.00	1.0	09/08/2023	The original release of this document with 6.4.00 GA.

# Contents

<b>GigaVUE Cloud Suite Deployment Guide - Azure</b> .....	<b>1</b>
Change Notes .....	3
Contents .....	4
<b>GigaVUE Cloud Suite Deployment Guide – Azure</b> .....	<b>9</b>
<b>Overview of GigaVUE Cloud Suite for Azure</b> .....	<b>9</b>
Components of GigaVUE Cloud Suite for Azure .....	11
Architecture of GigaVUE Cloud Suite for Azure .....	13
Hybrid Cloud .....	13
Cloud Overview Page .....	13
Virtual Dashboard Widgets .....	13
<b>Get Started with GigaVUE Cloud Suite for Azure</b> .....	<b>16</b>
License Information .....	16
Volume Based License (VBL) .....	16
Apply License .....	22
Before You Begin .....	22
Prerequisites .....	22
VPN Connectivity .....	27
Obtain GigaVUE-FM Image .....	27
Enable Subscription for GigaVUE Cloud Suite for Azure .....	28
Enable Subscription using CLI .....	29
Enable Subscription using Azure Portal .....	31
Install and Upgrade GigaVUE-FM .....	32
Install GigaVUE-FM on Azure .....	32
Install GigaVUE-FM Using Azure VM Dashboard .....	32
Install GigaVUE-FM Using Azure Market Place .....	32
Permissions and Privileges .....	34
Prerequisite .....	34
Managed Identity (recommended) .....	37
Application ID with client secret .....	38
<b>Deployment Options for GigaVUE Cloud Suite for Azure</b> .....	<b>39</b>
Deploy GigaVUE Fabric Components using Azure .....	39
Deploy GigaVUE Fabric Components using GigaVUE-FM .....	40
Traffic Acquisition Method as UCT-V .....	40
Traffic Acquisition Method as Customer Orchestrated Source .....	41

<b>Deploy GigaVUE Cloud Suite for Azure</b> .....	<b>42</b>
Create Azure Credentials .....	42
Prepare UCT-V to Monitor Traffic .....	44
Supported Operating Systems for UCT-V .....	44
Linux UCT-V Installation .....	45
Windows UCT-V Installation .....	50
Create Images with the Agent Installed .....	55
Uninstall UCT-V .....	55
Uninstall Linux UCT-V .....	56
Uninstall Windows UCT-V .....	57
Upgrade or Reinstall UCT-V .....	57
Install Custom Certificate .....	57
Upload Custom Certificates using GigaVUE-FM .....	57
Upload Custom Certificate using Third Party Orchestration .....	58
Adding Certificate Authority .....	59
CA List .....	59
Create Monitoring Domain .....	59
Manage Monitoring Domain .....	62
Configure GigaVUE Fabric Components in GigaVUE-FM .....	65
Configure UCT-V Controller .....	67
Configure GigaVUE V Series Proxy .....	70
Configure GigaVUE V Series Node .....	71
Configure Role-Based Access for Third Party Orchestration .....	73
Users .....	74
Add Users .....	74
How to Unlock User Account .....	77
Create Roles .....	78
Create Roles .....	78
Create User Groups .....	82
Create User Groups .....	82
Configure GigaVUE Fabric Components in Azure .....	84
Overview of Third-Party Orchestration .....	84
Prerequisites .....	85
Disable GigaVUE-FM Orchestration in Monitoring Domain .....	87
Configure UCT-V Controller in Azure .....	88
Configure UCT-V in Azure .....	91
Configure GigaVUE V Series Node and GigaVUE V Series Proxy in Azure .....	93
Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure .....	97
Prerequisite .....	97
Upgrade UCT-V Controller .....	97
Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy .....	99

<b>Configure Monitoring Session</b> .....	<b>103</b>
Create a Monitoring Session .....	103
Edit Monitoring Session .....	105
Enable Prefiltering, Precryption, and Secure Tunnel .....	106
Prefiltering .....	106
Interface Mapping .....	108
Create Ingress and Egress Tunnels .....	109
Create Raw Endpoint .....	114
Create a New Map .....	115
Example- Create a New Map using Inclusion and Exclusion Maps .....	119
Add Applications to Monitoring Session .....	119
Deploy Monitoring Session .....	120
View Monitoring Session Statistics .....	122
View Health Status on the Monitoring Session Page .....	123
Health .....	123
V Series Node Health .....	123
Target Source Health .....	124
Visualize the Network Topology .....	124
<b>Configure Application Intelligence Solutions on GigaVUE V Series Nodes for Azure</b> .....	<b>125</b>
Configure Environment .....	126
Create Environment .....	126
Create Credentials .....	127
Create Azure Credentials .....	128
Connect to Azure .....	128
Create Connection .....	129
Create Source Selectors .....	134
Create Tunnel Specifications .....	136
User Defined Application .....	138
Create Rules under User Defined Application .....	138
Supported Protocols and Attributes .....	139
Mindata .....	143
Supported RegExp Syntax .....	143
Limitations .....	144
Configure Application Intelligence Session .....	144
Prerequisites .....	145
Create an Application Intelligence Session in Virtual Environment .....	145
Slicing and Masking in Application Filtering Intelligence .....	148
Configuring Application Filtering Intelligence with Slicing .....	148
Configuring Application Filtering Intelligence with Masking .....	148
Configuring Application Filtering Intelligence with Slicing and Masking .....	149

Application Metadata Intelligence .....	149
Create Application Metadata Intelligence Session for Virtual Environment .....	150
Create NetFlow Session for Virtual Environment .....	154
NetFlow Dashboard .....	158
<b>Secure Tunnels .....</b>	<b>159</b>
Supported Platforms .....	160
Configure Secure Tunnel .....	160
Precrypted Traffic .....	160
Mirrored Traffic .....	160
Prerequisites .....	161
Configure Secure Tunnel from UCT-V to GigaVUE V Series Node .....	161
Configure Secure Tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2 .....	162
Viewing Status of Secure Tunnel .....	166
<b>Preryption™ .....</b>	<b>166</b>
How Gigamon Preryption Technology Works .....	167
Why Gigamon Preryption .....	168
Key Features .....	168
Key Benefits .....	168
How Gigamon Preryption Technology Works .....	169
Preryption Technology on Single Node .....	169
Preryption Technology on Multi-Node .....	170
Supported Platforms .....	171
Prerequisites .....	172
Note .....	172
Configure Preryption in UCT-V .....	172
<b>Monitor Cloud Health .....</b>	<b>174</b>
Configuration Health Monitoring .....	174
Traffic Health Monitoring .....	175
Create Threshold Template .....	176
Apply Threshold Template .....	176
Edit Threshold Template .....	177
Supported Resources and Metrics .....	178
View Health Status .....	180
<b>Fabric Health Analytics for Virtual Resources .....</b>	<b>182</b>
Virtual Inventory Statistics and Cloud Applications Dashboard .....	182
<b>Administer GigaVUE Cloud Suite for Azure .....</b>	<b>188</b>
Set Up Email Notifications .....	188
Configure Email Notifications .....	188
Configure Proxy Server .....	189

Configure Azure Settings .....	191
Role Based Access Control .....	191
About Events .....	193
About Audit Logs .....	195
<b>Additional Sources of Information .....</b>	<b>197</b>
Documentation .....	197
How to Download Software and Release Notes from My Gigamon .....	199
Documentation Feedback .....	200
Contact Technical Support .....	201
Contact Sales .....	201
Premium Support .....	202
The VÜE Community .....	202
<b>GigaVUE-FM Version Compatibility Matrix .....</b>	<b>203</b>
<b>Glossary .....</b>	<b>205</b>



# GigaVUE Cloud Suite Deployment Guide – Azure

This guide describes how to install, configure and deploy the GigaVUE Cloud solution on the Microsoft® Azure cloud. Use this document for instructions on configuring the GigaVUE Cloud components and setting up the traffic monitoring sessions for the Azure Cloud.

Refer to the following sections for details:

- [About GigaVUE Cloud Suite for Azure](#)
- [Get Started with GigaVUE Cloud Suite for Azure](#)
- [Deployment Options for GigaVUE Cloud Suite for Azure](#)
- [Deploy GigaVUE Cloud Suite for Azure](#)
- [Configure Monitoring Session](#)
- [Configure Application Intelligence Solutions on GigaVUE V Series Nodes for Azure](#)
- [Secure Tunnels](#)
- [Precryption™](#)
- [Monitor Cloud Health](#)
- [Fabric Health Analytics for Virtual Resources](#)
- [Administer GigaVUE Cloud Suite for Azure](#)
- [GigaVUE-FM Version Compatibility Matrix](#)

## Overview of GigaVUE Cloud Suite for Azure

GigaVUE® Cloud Suite for Azure extends complete visibility to workloads running in Azure and provides your security and observability tools with actionable network-level intelligence. GigaVUE Cloud Suite for Azure resides in the VNets and aggregates flows from all compute sites, including from native traffic mirroring nodes. Gigamon provides advanced traffic processing to generate metadata of traffic flows beyond traditional logging. This helps detect vulnerabilities or undesired activities and ensures effective and comprehensive cloud security with continuous monitoring.

All the elements of this cloud suite reside entirely in the cloud; they acquire traffic from every compute site through UCT-V (agent-like instances provisioned on each Virtual Machine). Gigamon auto-scales to adapt dynamically to changes in your virtual machine.

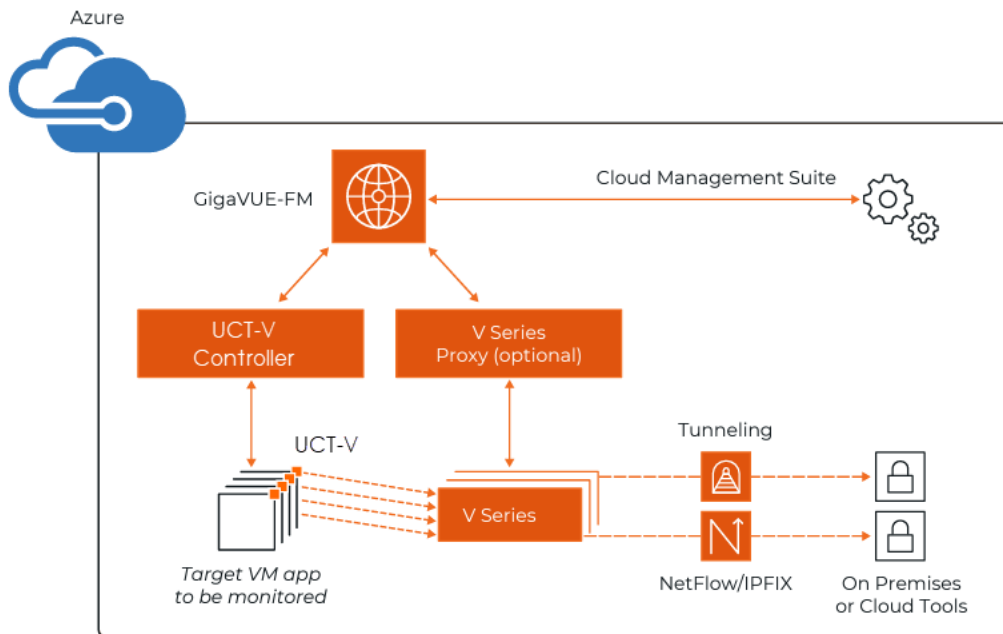
GigaVUE Cloud Suite for Azure provides the following benefits:

**Improves tool capacity:** Virtual security and monitoring tasks are offloaded from tools to improve effectiveness, reduce scaling and minimize costs.

**Fully automates the infrastructure:** Automatically identifies new and relocated workloads, instantiates and scales visibility nodes, and configures new traffic policies as needed.

**Simplifies operation:** Centralizes orchestration and management with a single-pane-of-glass visualization portal across any hybrid network.

**Helps accelerate cloud migrations:** Unifies on-premise and hybrid cloud environments with a common deep observability pipeline, centralized control, and complete.



## Components of GigaVUE Cloud Suite for Azure

The GigaVUE Cloud Suite for Azure consists of the following components:

Component	Description
GigaVUE® Fabric Manager (GigaVUE-FM)	A web-based fabric management interface that provides a single pane of glass visibility and management of both the physical and virtual traffic that forms the GigaVUE Cloud for Azure. GigaVUE-FM manages the configuration of the rest of the components in your cloud platform.
UCT-Vs (earlier known as G-vTAP Agent)	An agent that is installed in your virtual machines. This agent mirrors the selected traffic from the virtual machines to the GigaVUE V Series Node.
UCT-V Controllers (earlier known as G-vTAP Controller)	Manages multiple UCT-Vs and orchestrates the flow of mirrored traffic to GigaVUE V Series nodes. GigaVUE-FM uses one or more UCT-V Controllers to communicate with the UCT-Vs.
Next generation UCT-V (earlier known as Next Generation G-vTAP Agent)	Next generation UCT-V is a lightweight solution that acquires traffic from Virtual Machines and in-turn improves the performance of the UCT-V mirroring capability. The solution has a prefiltering capability at the tap level that reduces the traffic flow from the agent to GigaVUE V Series Node and in-turn reduces the V Series load. Next generation UCT-V gets activated only on Linux systems with a Kernel version above 5.4. Prefiltering allows you to filter the traffic in UCT-Vs before sending it to the GigaVUE V Series Nodes. For prefiltering the traffic, GigaVUE-FM allows you to create a prefiltering policy template and the template can be applied to a monitoring session.
GigaVUE V Series Proxy	The GigaVUE V Series Proxy is an optional component. If GigaVUE-FM cannot directly reach the GigaVUE V Series Nodes (management interface) directly over the network, a Proxy should be used. It can also be used if there is a large number of nodes connected to GigaVUE-FM or if you wish to keep IP addresses of the nodes private. It manages multiple GigaVUE V Series Nodes and orchestrates the flow of traffic from GigaVUE V Series Nodes to the monitoring tools. GigaVUE-FM uses one or more GigaVUE V Series Proxies to communicate with the GigaVUE V Series Nodes. A single GigaVUE V Series Proxy can be launched to provide the GigaVUE-FM network communication to hundreds of GigaVUE V Series Nodes present in private networks behind the Proxy.
GigaVUE V Series Nodes	A visibility node that aggregates mirrored traffic. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to on premise device or tools. GigaVUE Cloud Suite for Azure uses the standard VXLAN tunnel to deliver traffic to tool endpoints.

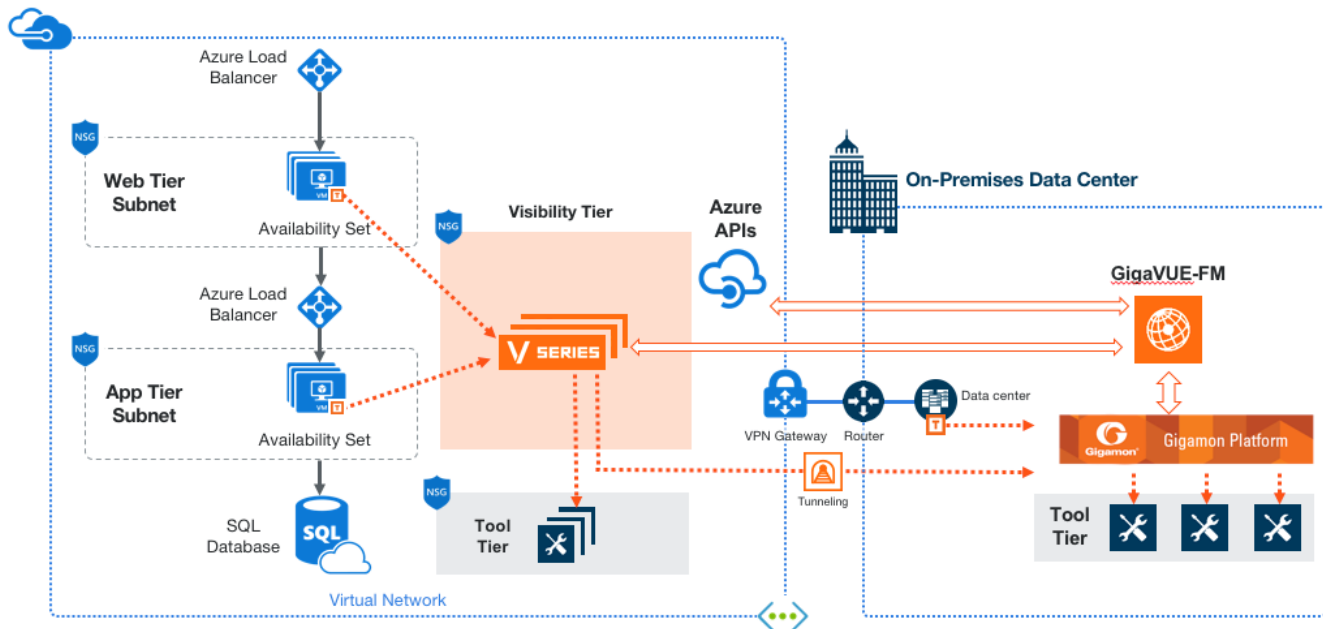
This solution is launched by subscribing to the GigaVUE Cloud Suite for Azure in the Azure Marketplace. Once the GigaVUE-FM is launched in Azure, the rest of the solution components are launched from GigaVUE-FM. Refer to [Install GigaVUE-FM on Azure](#) for more detailed information on how to launch GigaVUE-FM in Azure.

You can only configure the GigaVUE fabric components in a Centralized VNet only. In case of a shared VNet, you must select a VNet as your Centralized VNet for GigaVUE fabric configuration.

# Architecture of GigaVUE Cloud Suite for Azure

## Hybrid Cloud

In the hybrid cloud deployment model, you can send the customized traffic to the tools in Azure as well as the tools in the enterprise data center.



## Cloud Overview Page

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

Go to **Traffic > Virtual > Orchestrated Flows > Overview**. The Cloud Homepage appears.

## Virtual Dashboard Widgets

This section describes the widgets that can be viewed on the overview page.

- Overview
- V Series Alarms
- Connection Status
- Usage (VBL)
- Summary (Monitoring Session details)
- Traffic Rate
- Aggregate Summary

## Overview

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

## V Series Alarms

The V Series Alarms widget presents a pie chart that helps you to quickly to 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 to view the connection status of connections configured in the monitoring domain. Each type of connection status 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 connected.

## Usage

The Usage widget displays the amount of 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 particular day.

## Summary

This widget allows you to view the list of all the available monitoring session along with the respective monitoring domain, platform, connection, their health status, V Series Node health status and the deployment status of the connection. You can click on the monitoring session name to view the **Edit Monitoring session** page of the respective monitoring session.

## Traffic Rate

The traffic rate widget displays the rate of traffic flowing through the GigaVUE V Series Nodes. Each line in the graph indicates the rate of traffic flow for transmitting, receiving, and their ratio which is specified by the legend.

## 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.

# Get Started with GigaVUE Cloud Suite for Azure

This chapter describes how to plan and start the GigaVUE Cloud Suite for Azure deployment on the Microsoft® Azure cloud.

Refer to the following sections for details:

- [License Information](#)
- [Before You Begin](#)
- [Install and Upgrade GigaVUE-FM](#)
- [Install GigaVUE-FM on Azure](#)
- [Permissions and Privileges](#)

## License Information

The GigaVUE Cloud Suite Cloud suite is available in both the public Azure cloud and in Azure Government, and supports the Volume Based License (VBL) model that you can avail from the Azure Market Place.

Refer to the following topics for detailed information:

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

## Volume Based License (VBL)

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

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



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

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

## Base Bundles

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

- CoreVUE
- NetVUE
- SecureVUEPlus

The bundles are available as SKUs<sup>1</sup>. The number in the SKU indicates the total volume allowance of the SKU for that base bundle. For example, VBL-250T-BN-CORE has a daily volume allowance of 250 terabytes for CoreVUE bundle.

### Bundle Replacement Policy

Refer to the following notes:

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

## Add-on Packages

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

### Rules for add-on packages:

- Add-on packages can only to be added when there is an active base bundle available in GigaVUE-FM.
- The base bundle limits the total volume usage of the add-on package.

---

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

- If your add-on package has volume allowance less than the base bundle, then your add-on package can only handle volume allocated for add-on package.
- When the life term of an add-on package extends beyond the base bundle, then when the base bundle expires, the volume allowance of the add-on package will be reduced to zero until a new base bundle is added.

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

GigaVUE Data Sheets
<a href="#">GigaVUE Cloud Suite for VMware Data Sheet</a>
<a href="#">GigaVUE Cloud Suite for AWS Data Sheet</a>
<a href="#">GigaVUE Cloud Suite for Azure Data Sheet</a>
<a href="#">GigaVUE Cloud Suite for OpenStack</a>
<a href="#">GigaVUE Cloud Suite for Nutanix</a>
<a href="#">GigaVUE Cloud Suite for Kubernetes</a>

## How GigaVUE-FM Tracks Volume-Based License Usage

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


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

For releases prior to 6.4:

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

## Manage Volume-based Licenses

To manage active Volume-based License:

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

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

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

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

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

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

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

Use the following buttons to manage your VBL.


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

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

For details about:	Reference section	Guide
How to generate Volume-based License reports	<a href="#">Generate VBL Usage Reports</a>	GigaVUE Administration Guide
Volume-based Licensed report details	<a href="#">Volume Based License Usage Report</a>	GigaVUE Administration Guide
Fabric health analytics dashboards for Volume-based Licenses usage	<a href="#">Dashboards for Volume Based Licenses Usage</a>	GigaVUE-FM User Guide

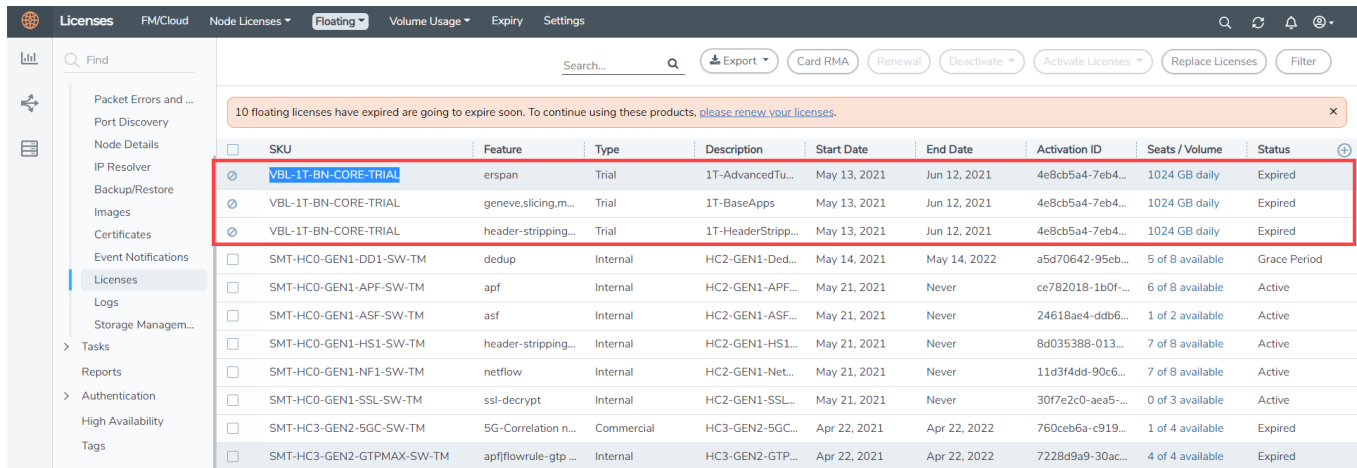
## Activate Volume-based Licenses

To activate Volume-based licenses:

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

## Default Trial Licenses

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



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

This license includes the following applications:


- ERSPAN
- Geneve
- Slicing
- Masking
- Trailer
- Tunneling
- Load Balancing
- Enhanced Load Balancing
- Flowmap
- Header-stripping
- Add header

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

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

### Delete Default Trial Licenses

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

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

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

## Apply License

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

## Before You Begin

You must create an account and configure a VNet as per your requirements. This section describes the requirements for launching the GigaVUE-FM VM.

- [Prerequisites](#)
- [VPN Connectivity](#)
- [Obtain GigaVUE-FM Image](#)
- [Enable Subscription for GigaVUE Cloud Suite for Azure](#)

## Prerequisites

To enable the flow of traffic between the components and the monitoring tools, you must create the following requirements:

- [Resource Group](#)
- [Virtual Network](#)
- [Subnets for VNet](#)
- [Network Interfaces \(NICs\) for VMs](#)
- [Network Security Groups](#)
- [Virtual Network Peering](#)
- [Access control \(IAM\)](#)
- [Default Login Credentials](#)
- [Recommended Instance Types](#)

### Resource Group

The resource group is a container that holds all the resources for a solution.

To create a resource group in Azure, refer to [Create a resource group](#) topic in the Azure Documentation.

## Virtual Network

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks.

You can only configure the GigaVUE fabric components in a Centralized VNet only. In case of a shared VNet, you must select a VNet as your Centralized VNet for GigaVUE fabric configuration.

To create a virtual network in Azure, refer to [Create a virtual network](#) topic in the Azure Documentation.

## Subnets for VNet

The following table lists the two recommended subnets that your VNet must have to configure the GigaVUE Cloud Suite Cloud components in Azure.

You can add subnets when creating a VNet or add subnets on an existing VNet. Refer to [Add a subnet](#) topic in the Azure Documentation for detailed information.

Subnet	Description
Management Subnet	Subnet that the GigaVUE-FM uses to communicate with the GigaVUE V Series Nodes and Proxy.
Data Subnet	<p>A data subnet can accept incoming mirrored traffic from agents to the GigaVUE V Series Nodes or be used to egress traffic to a tool from the GigaVUE V Series Nodes. There can be multiple data subnets.</p> <ul style="list-style-type: none"> <li>▪ Ingress is VXLAN from agents</li> <li>▪ Egress is either VXLAN tunnel to tools or to GigaVUE HC Series tunnel port, or raw packets through a NAT when using NetFlow.</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> If you are using a single subnet, then the Management subnet will also be used as a Data Subnet.</p> </div>
Tool Subnet	<p>A tool subnet can accept egress traffic to a tool from the GigaVUE V Series Nodes. There can be only one tool subnet.</p> <ul style="list-style-type: none"> <li>▪ Egress is either VXLAN tunnel to tools or to GigaVUE HC Series tunnel port, or raw packets through a NAT when using NetFlow.</li> </ul>

## Network Interfaces (NICs) for VMs

When using UCT-V as the traffic acquisition method, for the UCT-Vs to mirror the traffic from the VMs, you must configure one or more Network Interfaces (NICs) on the VMs.

- **Single NIC**—If there is only one interface configured on the VM with the UCT-V, the UCT-V sends the mirrored traffic out using the same interface.
- **Multiple NICs**—If there are two or more interfaces configured on the VM with the UCT-V, the UCT-V monitors any number of interfaces but has an option to send the mirrored traffic out using any one of the interfaces or using a separate, non-monitored interface.

## Network Security Groups

A network security group defines the virtual firewall rules for your VM to control inbound and outbound traffic. When you launch GigaVUE-FM, GigaVUE V Series Proxy, GigaVUE V Series Nodes, and UCT-V Controllers in your VNet, you add rules that control the inbound traffic to VMs, and a separate set of rules that control the outbound traffic.

To create a network security group and add in Azure, refer to [Create a network security group](#) topic in the Azure Documentation.

It is recommended to create a separate security group for each component using the rules and port numbers.

In your Azure portal, select a network security group from the list. In the Settings section select the Inbound and Outbound security rules to the following rules.

Following are the Network Firewall Requirements.

The following table lists the Network Firewall Requirements for GigaVUE V Series Node deployment.

Direction	Type	Protocol	Port	CIDR	Purpose
<b>GigaVUE-FM</b>					
Inbound	<ul style="list-style-type: none"> <li>• HTTPS</li> <li>• SSH</li> </ul>	TCP	<ul style="list-style-type: none"> <li>• 443</li> <li>• 22</li> </ul>	Administrator Subnet	Management connection to GigaVUE-FM
Inbound	Custom TCP Rule	TCP	5671	GigaVUE V Series Node IP	Allows GigaVUE V Series Nodes to send traffic health updates to GigaVUE-FM Allows Next Generation UCT-V to send statistics to GigaVUE-FM
Outbound	Custom TCP Rule	TCP(6)	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate with



Direction	Type	Protocol	Port	CIDR	Purpose
					GigaVUE-FM
Outbound (optional)	Custom TCP Rule	TCP	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series node
<b>UCT-V Controller</b>					
Inbound	Custom TCP Rule	TCP(6)	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate with GigaVUE-FM
Inbound (This is the port used for Third Party Orchestration)	Custom TCP Rule	TCP(6)	8891	UCT-V or Subnet IP	Allows UCT-V Controller to communicate registration requests from UCT-V and forward the same to GigaVUE-FM
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM.
Outbound	Custom TCP Rule	TCP(6)	9901	UCT-V Controller IP	Allows UCT-V Controller to communicate with UCT-Vs
<b>UCT-V</b>					
Inbound	Custom TCP Rule	TCP(6)	9901	UCT-V Controller IP	Allows UCT-Vs to communicate with UCT-V Controller
Outbound (This is the port used for Third Party Orchestration)	Custom TCP Rule	TCP(6)	8891	UCT-V or Subnet IP	Allows UCT-V to communicate with UCT-V Controller for registration and Heartbeat
Outbound	<ul style="list-style-type: none"> <li>• UDP</li> <li>• IP</li> </ul>	<ul style="list-style-type: none"> <li>• UDP (VXLAN)</li> <li>• IP Protocol (L2GRE)</li> </ul>	VXLAN (default 4789)	UCT-V or Subnet IP	Allows UCT-Vs to (VXLAN/L2GRE) tunnel traffic to V Series nodes
Outbound	Custom TCP Rule	TCP	11443	UCT-V subnet	Allows UCT-V to securely transfer the traffic to GigaVUE V Series Node
<b>GigaVUE V Series Proxy (optional)</b>					
Inbound	Custom TCP Rule	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP	TCP	8889	GigaVUE V	Allows V Series Proxy to

Direction	Type	Protocol	Port	CIDR	Purpose
	Rule			Series Node IP	communicate with V Series node
<b>GigaVUE V Series Node</b>					
Inbound	Custom TCP Rule	TCP	8889	<ul style="list-style-type: none"> <li>GigaVUE-FM IP</li> <li>V Series Proxy IP</li> </ul>	Allows V Series Proxy or GigaVUE-FM to communicate with V Series node
Inbound	<ul style="list-style-type: none"> <li>UDP</li> <li>IP</li> </ul>	<ul style="list-style-type: none"> <li>UDP (VXLAN)</li> <li>IP Protocol (L2GRE)</li> </ul>	<ul style="list-style-type: none"> <li>VXLAN (default 4789)</li> <li>L2GRE</li> </ul>	UCT-V or Subnet IP	Allows UCT-Vs to (VXLAN/L2GRE) tunnel traffic to V Series nodes
Inbound	UDP	UDPGRE	4754	Ingress Tunnel	Allows to UDPGRE Tunnel to communicate and tunnel traffic to V Series nodes
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM
Outbound	Custom UDP Rule	<ul style="list-style-type: none"> <li>UDP (VXLAN)</li> <li>IP Protocol (L2GRE)</li> </ul>	VXLAN (default 4789)	Tool IP	Allows V Series node to communicate and tunnel traffic to the Tool
Outbound (optional)	ICMP	ICMP	<ul style="list-style-type: none"> <li>echo request</li> <li>echo reply</li> </ul>	Tool IP	Allows V Series node to health check tunnel destination traffic
Bi-directional	Custom TCP Rule	TCP	11443	GigaVUE V Series Node subnet	Allows to securely transfer the traffic in between GigaVUE V Series Nodes.

## Virtual Network Peering

Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure. Virtual Network Peering is only applicable when multiple Virtual Networks are used in a design. Refer to [Virtual Network Peering](#) topic in Azure documentation for more details.

## Access control (IAM)

You must have full resource access to the control the GigaVUE Cloud Suite cloud components. Refer to [Check access for a user](#) topic in the Azure documentation for more details.

## Default Login Credentials

You can login to the GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controller 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 not configured.
GigaVUE V Series proxy	You can login to the GigaVUE V Series Node by using ssh. The default username and password is not configured.
UCT-V Controller	You can login to the GigaVUE V Series Node by using ssh. The default username and password is not configured.

## Recommended Instance Types

**NOTE:** Additional instance types are also supported. Refer to Support, Sales, or Professional Services for deployment optimization.

Product	Instance Type	vCPU	RAM
GigaVUE V Series Node	Standard_D4s_v4	4 vCPU	16 GB
	Standard_D8S_V4	8 vCPU	32 GB
GigaVUE V Series Proxy	Standard_B1s	1 vCPU	1 GB
UCT-V Controller	Standard_B1s	1 vCPU	1 GB

## VPN Connectivity

GigaVUE-FM requires Internet access to integrate with the public API endpoints to integrate with the GigaVUE Cloud Suite Cloud platform. If there is no Internet access, refer to [Configure Proxy Server](#).

## Obtain GigaVUE-FM Image

The image for the GigaVUE Cloud Suite Cloud is available in both the Azure Public Cloud and in the Azure Government portal.

## GigaVUE Cloud Suite Cloud Suite in Azure Public Cloud

GigaVUE Cloud Suite Cloud is available in the Azure Marketplace with the Volume Based License options.

## GigaVUE Cloud Suite Cloud Suite in Azure Government

Azure Government is an isolated Azure region that contains specific regulatory and compliance requirements of the US government agencies.

To monitor the VMs that contain all categories of Controlled Unclassified Information (CUI) data and sensitive government data in the Azure Government (US) Region, the Azure Government solution provides the same robust features in Azure Government as in the Azure public cloud.

## Enable Subscription for GigaVUE Cloud Suite for Azure

For GigaVUE-FM to be able to launch the fabric images, you must accept the terms of the end user license agreements (EULAs) and enable programmatic access. This can be done in the Azure portal or through Azure Portal Cloud Shell. Refer to the following topics for more detailed information:

- [Enable Subscription using CLI](#)
- [Enable Subscription using Azure Portal](#)

**NOTE:** For accepting EULA, you need to have Owner role on the Subscription.

## Enable Subscription using CLI

## 1. BYOL FM: The following example shows how to accept EULA for BYOL FM using Azure Portal Cloud Shell

```

az vm image terms accept --urn gigamon-inc:gigamon-gigavue-cloud-suite:gfm-azure:6.4.00
{
  "accepted": true,
  "id": "/subscriptions/6447eb55-9d09-481b-89bc-52e96bb52823/providers/Microsoft.MarketplaceOrdering/offertypes/Microsoft.MarketplaceOrdering/offertypes/publishers/gigamon-inc/offers/gigamon-gigavue-cloud-suite/plans/gfm-azure/agreements/current",
  "licenseTextLink": "https://mpcprodsa.blob.core.windows.net/legalterms/3E5ED_legalterms_GIGAMON%253a2DINC%253a24GIGAMON%253a2DGIGAVUE%253a2DCLLOUD%253a2DSUITE%253a24GFM%253a2DAZURE%253a24BGSZOQHPVC4M4GL4ZK5K752EDRWRVJPTVJ7LMSHSRRRN5TYHJR47WNYMJH2ULRWBWUG5CN04E6LF34G43TGV3S OGRXJ4OCBMLHLBTXQ.txt",
  "marketplaceTermsLink": "https://mpcprodsa.blob.core.windows.net/marketplaceterms/3EDEF_marketplaceterms_VIRTUALLMACHINE%253a24AAK20AIZEAWW5H4MSP5KSTVB6NDKKRTUBAU23BRFTWN4YC2MQLJUB5ZEYUOUJBVF3YK34CIVPZL2HWYASPGDUY502FWEGRBYOXWZE5Y.txt",
  "name": "gfm-azure",
  "plan": "gfm-azure",
  "privacyPolicyLink": "https://www.gigamon.com/privacy-policy.html",
  "product": "gigamon-gigavue-cloud-suite",
  "publisher": "gigamon-inc",
  "retrieveDatetime": "2023-05-02T20:09:36.1347592Z",
  "signature":
  "SZL3CYR5MMU5QC5FEBIDHLMOYE7DD4CBSMLOVRMCKAAUD5CKLG4RIWPALULYWCFWCENMFF77RCXM4CM2B24WV3PGEFW7UL4VMI3BVI",
  "systemData": {
    "createdAt": "2023-05-02T20:09:38.101210+00:00",
    "createdBy": "6447eb55-9d09-481b-89bc-52e96bb52823",
    "createdByType": "ManagedIdentity",
    "lastModifiedAt": "2023-05-02T20:09:38.101210+00:00",
    "lastModifiedBy": "6447eb55-9d09-481b-89bc-52e96bb52823",
    "lastModifiedByType": "ManagedIdentity"
  },
  "type": "Microsoft.MarketplaceOrdering/offertypes"
}

```

2. Fabric Images (need to accept on all 3): The following examples show how to accept EULA for different fabric components using Azure Portal Cloud Shell

#### For UCT-V Controller

```
az vm image terms accept --urn gigamon-inc:gigamon-gigavue-cloud-suite:uctv-cntlr:6.4.00
{
  "accepted": true,
  .....
  "type": "Microsoft.MarketplaceOrdering/offertypes"
}
```

#### For GigaVUE V Series Node

```
az vm image terms accept --urn gigamon-inc:gigamon-gigavue-cloud-suite:vseries-node:6.4.00
{
  "accepted": true,
  .....
  "type": "Microsoft.MarketplaceOrdering/offertypes"
}
```

#### For GigaVUE V Series Proxy

```
az vm image terms accept --urn gigamon-inc:gigamon-gigavue-cloud-suite:vseries-proxy:6.4.00
{
  "accepted": true,
  .....
  "type": "Microsoft.MarketplaceOrdering/offertypes"
}
```

## Enable Subscription using Azure Portal

Enable the subscription for GigaVUE-FM and its fabric components like GigaVUE V Series Node, UCT-V Controller, and GigaVUE V Series Proxy. The following steps provide detailed information on how to accept the terms using Azure Portal.

1. Go to Market Place, search Gigamon.
2. Select **Gigamon GigaVUE Cloud Suite for Azure** from the search results. Select the required image from the **Plan** drop-down menu.
3. Click the "**Want to deploy programmatically? Get started**" link.
4. Review the terms of service and the subscription name and then click **Enable**.

## Install and Upgrade GigaVUE-FM

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

- Cloud—To install GigaVUE-FM inside your Azure environment, you can launch the GigaVUE-FM instance in your VNet.
  - Installation: Refer to [Install GigaVUE-FM on Azure](#).
  - Upgrade: Refer to Upgrade GigaVUE-FM in Azure topic in GigaVUE-FM Installation and Upgrade Guide.
- On-premises—To install and upgrade GigaVUE-FM in your enterprise data center, refer to GigaVUE-FM Installation and Upgrade Guide available in the [Gigamon Documentation Library](#).
  - Installation: Refer to GigaVUE-FM Installation and Upgrade Guide.
  - Upgrade: Refer to Upgrade GigaVUE-FM topic in GigaVUE-FM Installation and Upgrade Guide.

## Install GigaVUE-FM on Azure

The GigaVUE-FM can be launched from the Azure VM dashboard or Azure Marketplace.

### Install GigaVUE-FM Using Azure VM Dashboard

Go to **Azure VM Dashboard > Virtual Machines**, click **Create** to create an Azure Virtual Machine. Refer to [Create a Linux virtual machine in the Azure](#) topics in Azure Documentation for more information. Enter the details as mentioned in [Table 1: GigaVUE-FM Installation Steps](#).

### Install GigaVUE-FM Using Azure Market Place

Go to Azure Market Place, search for Gigamon. The latest version of Gigamon GigaVUE Cloud Suite for Azure appears. Open the latest version of GigaVUE-FM. Review and accept the terms for Gigamon GigaVUE Cloud Suite for Azure. Refer to [Enable Subscription for GigaVUE Cloud Suite for Azure](#) for more detailed information on how to enable the subscription and accept the terms of use. Refer to [Create a Linux virtual machine in the Azure](#) topics in Azure Documentation for more information. Enter the details as mentioned in [Table 1: GigaVUE-FM Installation Steps](#).

The following table describes the important fields.



Table 1: GigaVUE-FM Installation Steps

Field	Description
<b>Basics</b>	
Subscription	Select your subscription.
Resource Group	Select an existing resource group or create a new resource group. For more information, refer to <a href="#">Create a resource group</a> topic in the Azure Documentation.
Virtual machine name	Enter a name for the VM.
Region	Select a region for Azure VM.
Image	Select the latest GigaVUE-FM images.  <b>NOTE:</b> You cannot select multiple images for a VM. Refer to <a href="#">Configure GigaVUE Fabric Components in Azure</a> for more details on configuring GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controller in Azure.
Size	The recommended instance types are as follows: <ul style="list-style-type: none"> <li>● GigaVUE-FM - <b>Standard_D4s_v3</b></li> <li>● UCT-V Controller - <b>Standard_B1ms</b></li> <li>● V Series Node - <b>Standard_D4s_v4</b></li> <li>● V Series Proxy - <b>Standard_B1ms</b></li> </ul>
Authentication Type	We support only SSH public key authentication type <ul style="list-style-type: none"> <li>● SSH public key <ul style="list-style-type: none"> <li>○ Enter the administrator username for the VM.</li> <li>○ Enter the SSH public key pair name.</li> </ul> </li> </ul>
<b>Disks</b>	
Disk Size	The required disk size for GigaVUE-FM is <b>2 x 40GB</b> .
<b>Networking</b>	
Virtual Network	Select an existing VNet or create a new VNet. For more information, refer to <a href="#">Create a virtual network</a> topic in the Azure Documentation. On selecting an existing VNet, the <b>Subnet</b> and the <b>Public IP</b> values are auto-populated.
Configure network security group	Select an existing network security group or create a new network security group. For more information, refer to <a href="#">Network Security Groups</a> . Configure the Network Security Group to allow GigaVUE-FM to communicate with the rest of the components.

**NOTE:** Verify the summary before proceeding to create. It will take several minutes for the VM to initialize. After the initialization is completed, you can verify the VM through the Web interface.

After the deployment, navigate to the VM overview page, copy the **Public IP address**, and paste it in a new web browser tab.

If GigaVUE-FM is deployed in Azure, use **admin123A!!** as the password for the **admin** user to login to GigaVUE-FM. You must change the default password after logging in to GigaVUE-FM.

## Permissions and Privileges

When you first connect GigaVUE-FM to Azure, you need the appropriate authentication for Azure to verify your identity and check if you have permission to access the resources that you are requesting. This is used for GigaVUE-FM to integrate with Azure APIs and to automate the fabric deployment and management.

### Prerequisite

Have pre-defined custom roles or create new custom roles, that can be attached to the resource group or subscription level. Refer to [Custom Roles](#) topic for more detailed information on how to create custom roles.

### Custom Roles

The 'built-in' roles provided by Microsoft are open to all resources. You can create a custom role if required. For more information, refer to [Azure custom roles](#) topic in the Azure Documentation.

You can use the following command to create custom roles in CLI:

```
az role definition create --role-definition <Custom Role>.json
```

The following examples provides the minimum permissions that are required for GigaVUE-FM to deploy the fabric components and/or inventory the UCT-V. The permissions can be applied at the resource group level or subscription level:

#### Example 1: Create Custom Role for GigaVUE-FM to deploy visibility fabric components and inventory UCT-V

```
{
  "name": "GigaVue-FM-Service-Role"
  "roleName": "CustomRoleFabricDeploymentAndInventory",
  "description": "The minimum requirements for FM to deploy Fabric Components and inventory UCT-V",
  "assignableScopes": [
    "/subscriptions/<SubscriptionID>/resourceGroups/<resourceGroup name>"
  ],
}
```

```

"permissions": [
  {
    "actions": [
      "Microsoft.Compute/virtualMachines/read",
      "Microsoft.Compute/virtualMachines/write",
      "Microsoft.Compute/virtualMachines/delete",
      "Microsoft.Compute/virtualMachines/start/action",
      "Microsoft.Compute/virtualMachines/powerOff/action",
      "Microsoft.Compute/virtualMachines/restart/action",
      "Microsoft.Compute/virtualMachines/instanceView/read",
      "Microsoft.Compute/locations/vmSizes/read",
      "Microsoft.Compute/images/read",
      "Microsoft.Compute/disks/read",
      "Microsoft.Compute/disks/write",
      "Microsoft.Compute/disks/delete",
      "Microsoft.Network/networkInterfaces/read",
      "Microsoft.Network/networkInterfaces/write",
      "Microsoft.Network/virtualNetworks/subnets/join/action",
      "Microsoft.Network/virtualNetworks/subnets/read",
      "Microsoft.Network/networkInterfaces/join/action",
      "Microsoft.Network/networkInterfaces/delete",
      "Microsoft.Network/publicIPAddresses/read",
      "Microsoft.Network/publicIPAddresses/write",
      "Microsoft.Network/publicIPAddresses/delete",
      "Microsoft.Network/publicIPAddresses/join/action",
      "Microsoft.Network/virtualNetworks/read",
      "Microsoft.Network/virtualNetworks/virtualMachines/read",
      "Microsoft.Network/networkSecurityGroups/read",
      "Microsoft.Network/networkSecurityGroups/join/action",
      "Microsoft.Network/publicIPAddresses/read",
      "Microsoft.Network/publicIPAddresses/write",
      "Microsoft.Network/publicIPAddresses/delete",
      "Microsoft.Network/publicIPAddresses/join/action",
      "Microsoft.Resources/subscriptions/locations/read",
      "Microsoft.Resources/subscriptions/resourceGroups/read",
      "Microsoft.Resources/subscriptions/resourcegroups/resources/read"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]
}

```

### Example 2: Create Custom Role for GigaVUE-FM to only inventory UCT-V

```

{
  "name": "GigaVue-FM-Service-Role"
  "roleName": "CustomRoleInventoryUCT-V ",
  "description": "Minimum requirements for FM to inventory UCT-V",
  "/subscriptions/<Subscription ID>/resourceGroups/<resourceGroup name>"
},
"permissions": [
  {
    "actions": [

```

```

    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/images/read",
    "Microsoft.Compute/disks/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Resources/subscriptions/resourceGroups/resources/read"
  ],
  "notActions": [],
  "dataActions": [],
  "notDataActions": []
}
]
}

```

You can use the following snippet in the above JSON file to assign your custom role at either resource group level or subscription level

For Resource group level:

```

"assignableScopes": [
  "/subscriptions/<Subscription ID>/resourceGroups/<resourceGroup name>"
],

```

For Subscription level:

```

"assignableScopes": [
  "/subscriptions/<Subscription ID>/"
],

```

To add a role assignment, refer to [Steps to assign an Azure role](#).

GigaVUE-FM supports two types of authentications with Azure. Refer to the following sections for more detailed information on how to enable each type of authentication for GigaVUE-FM and how to assign the above created custom roles for GigaVUE-FM:

- [Managed Identity \(recommended\)](#)
- [Application ID with client secret](#)

## Managed Identity (recommended)

Managed Identity (MSI) is a feature of Azure Active Directory. When you enable MSI on an Azure service, Azure automatically creates an identity for the service VM in the Azure AD tenant used by your Azure subscription.

Managed Identity (MSI) is only available when GigaVUE-FM is launched inside Azure. If GigaVUE-FM is launched in one VNet and the GigaVUE V Series Nodes are deployed in a different VNet, then Virtual Network Peering must be configured. Refer to the [Virtual Network Peering](#) for more details on how to configure Virtual Network Peering.

There are 2 steps to have MSI work:

1. Enable MSI on the VM running in GigaVUE-FM. It can be done in using Azure portal or CLI.
  - a. Azure Portal: Refer to [Configure managed identities using the Azure portal](#) in the Azure documentation for detailed instructions
  - b. Azure CLI:
    - For resource group level: **az vm identity assign -g <Resource group where FM is deployed> -n <GigaVUE-FM name> -scope <resource group id>**
    - For subscription level: **az vm identity assign -g <Resource group where FM is deployed> -n <GigaVUE-FM name> -scope <subscription id>**

For more information, refer to [Configure managed identities for Azure resources using Azure CLI](#) topic in the Azure Documentation.

2. Assign permissions to this VM on all the resources where you need GigaVUE-FM to manage.

After enabling MSI, you can assign custom roles to GigaVUE-FM at a resource group level or subscription level:

### Assign a Custom Role using CLI


1. Assign a custom role at resource group level where you will deploy the fabric:
 

```
az vm identity assign -g <Resource group where FM is deployed> -role <Custom Role> -n <GigaVUE-FM name> --scope <resource group id>
```
2. Assign a custom role at the subscription level to view the complete account details:
 

```
az vm identity assign -g <Resource group where FM is deployed> -role <Custom Role> -n <GigaVUE-FM name> --scope <subscription id>
```

If you want to update the Role, you can edit the JSON file, and then update the Role in Azure using the following CLI command:

```
az role definition update --role-definition <Custom Role>.json
```

You can run these commands in the Azure Portal in a cloud shell (icon in the upper right of the portal as seen here): .

## Assign a Custom Role using Azure Portal

You can assign roles to GigaVUE-FM using Azure Portal for Resource Group Level or Subscription Level. Refer to [Assign Azure roles](#) topic in Azure Documentation for detailed information.

## Application ID with client secret

GigaVUE-FM supports application id with client secret authentication. When using GigaVUE-FM to connect to Azure, it uses a service principal. A service principal is an account for a non-human such as an application to connect to Azure. When GigaVUE-FM is launched outside Azure, Application ID with client secret is preferred.

To create a service principal in Azure, refer to the following topics in the Azure Documentation:

- [Create an Azure service principal with the Azure CLI](#)
- [Create an Azure service principal with Azure PowerShell](#)
- [Create an Azure service principal with Azure Portal](#)



GigaVUE-FM must be able to access the URLs listed in the [Allow the Azure portal URLs on your firewall or proxy server](#) in order to connect to Azure.

Following are the required endpoints for Azure GovCloud:

- authentication\_endpoint = <https://login.microsoftonline.us/>
- azure\_endpoint = <https://management.usgovcloudapi.net/>

After creating service principal in Azure, you can add custom roles. Refer to [Assign a Custom Role using CLI](#) or [Assign a Custom Role using Azure Portal](#) for detailed information on how to assign roles.

The key fields required for GigaVUE-FM to connect to Azure are Subscription ID, Tenant ID, Application ID, and Application Secret.

- When creating the service principal using the Azure CLI, the output of that command will display the "appid" and "password" fields. These two are the Application ID and Application Secret fields that are required for GigaVUE-FM to connect to Azure. Copy them.
- Now, using the Azure CLI again, do an 'account show' command and copy the Subscription ID and the Tenant ID of your subscription.

The Subscription ID, Tenant ID, Application ID, and Application Secret will be used when creating credentials in GigaVUE-FM. Refer to [Create Azure Credentials](#) for step-by-step instructions.

**DISCLAIMER:** These are general guidelines for enabling a deployment in Azure. Since the Azure interface is subject to change and is outside Gigamon's purview, please see Azure documentation for instructions on using Azure.

# Deployment Options for GigaVUE Cloud Suite for Azure

This section provides a detailed information on the multiple ways in which GigaVUE Cloud Suite for Azure can be configured to provide visibility for physical and virtual traffic. There are three different ways in which GigaVUE Cloud Suite for Azure can be configured based on the traffic acquisition method and the method in which you want to deploy fabric components. Refer to the [Before You Begin](#) section for prerequisites that are required to be configured. For more detailed information and the work flow refer the following topics:

- [Deploy GigaVUE Fabric Components using Azure](#)
- [Deploy GigaVUE Fabric Components using GigaVUE-FM](#)
  - [Traffic Acquisition Method as UCT-V](#)
  - [Traffic Acquisition Method as Customer Orchestrated Source](#)

## Deploy GigaVUE Fabric Components using Azure

GigaVUE-FM allows you to use Azure as an orchestrator to deploy GigaVUE fabric nodes and then use GigaVUE-FM to configure the advanced features supported by these nodes. Refer the following table for the step-by-step instructions.

Step No	Task	Refer the following topics
1	Obtain GigaVUE-FM Image	<a href="#">Obtain GigaVUE-FM Image</a>
2	Install GigaVUE-FM on Azure	<a href="#">Install GigaVUE-FM on Azure</a>
3	Check and provide permissions and privileges	<a href="#">Permissions and Privileges</a>
4	Install UCT-V Agents  <b>NOTE:</b> When using Azure as your orchestration system you can only use G-TAP Agents.	For Linux: <a href="#">Linux UCT-V Installation</a> For Windows: <a href="#">Windows UCT-V Installation</a>
5	Create Azure Credentials to monitor workloads across multiple Azure subscriptions	<a href="#">Create Azure Credentials</a>
6	Create a Monitoring Domain  <b>NOTE:</b> Ensure that the Use FM to Launch Fabric	<a href="#">Create Monitoring Domain</a>

Step No	Task	Refer the following topics
	toggle button is disabled.	
7	Configure GigaVUE Fabric Components <b>NOTE:</b> Select UCT-V as the Traffic Acquisition Method.	Disable GigaVUE-FM Orchestration in Monitoring Domain
8	Create Monitoring session	Configure Monitoring Session
9	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
10	Deploy Monitoring Session	Deploy Monitoring Session
11	View Monitoring Session Statistics	View Monitoring Session Statistics

## Deploy GigaVUE Fabric Components using GigaVUE-FM

You can deploy GigaVUE fabric components using GigaVUE-FM using one of the following two traffic acquisition methods:

### Traffic Acquisition Method as UCT-V

Follow instruction in the below table, if you wish to use UCT-V as your traffic acquisition method. When using UCT-V the traffic from the Virtual Machines are acquired using the UCT-V and it is sent to the GigaVUE V Series Nodes.

Step No	Task	Refer the following topics
1	Obtain GigaVUE-FM Image	Obtain GigaVUE-FM Image
2	Install GigaVUE-FM on Azure	Install GigaVUE-FM on Azure
3	Check and provide permissions and privileges	Permissions and Privileges
4	Install UCT-V Agents	For Linux: <a href="#">Linux UCT-V Installation</a> For Windows: <a href="#">Windows UCT-V Installation</a>
5	Create Azure Credentials to monitor workloads across multiple Azure subscriptions	Create Azure Credentials
6	Create a Monitoring Domain <b>NOTE:</b> Ensure that the Use FM to Launch Fabric toggle button is enabled.	Create Monitoring Domain
7	Configure GigaVUE Fabric Components <b>NOTE:</b> Select UCT-V as the Traffic Acquisition Method.	Disable GigaVUE-FM Orchestration in Monitoring Domain



Step No	Task	Refer the following topics
8	Create Monitoring session	<a href="#">Configure Monitoring Session</a>
9	Add Applications to the Monitoring Session	<a href="#">Add Applications to Monitoring Session</a>
10	Deploy Monitoring Session	<a href="#">Deploy Monitoring Session</a>
11	View Monitoring Session Statistics	<a href="#">View Monitoring Session Statistics</a>

## Traffic Acquisition Method as Customer Orchestrated Source

Follow instruction in the below table if you wish to use Customer Orchestrated Source as your traffic acquisition method. In this case you can use tunnels as a source where the traffic is directly tunneled to V Series nodes without deploying UCT-V or UCT-V controllers.

Step No	Task	Refer the following topics
1	Obtain GigaVUE-FM Image	<a href="#">Obtain GigaVUE-FM Image</a>
2	Install GigaVUE-FM on Azure	<a href="#">Install GigaVUE-FM on Azure</a>
3	Check and provide permissions and privileges	<a href="#">Permissions and Privileges</a>
2	Create a Monitoring Domain  <b>NOTE:</b> Ensure that the <b>Use FM to Launch Fabric</b> toggle button is enabled.	<a href="#">Create Monitoring Domain</a>
3	Configure GigaVUE Fabric Components  <b>NOTE:</b> Select Customer Orchestrated Source as the Traffic Acquisition Method.	<a href="#">Disable GigaVUE-FM Orchestration in Monitoring Domain</a>
4	Create Monitoring session	<a href="#">Configure Monitoring Session</a>
5	Create Ingress and Egress Tunnel Endpoints	<a href="#">Create Ingress and Egress Tunnels</a>
6	Add Applications to the Monitoring Session	<a href="#">Add Applications to Monitoring Session</a>
7	Deploy Monitoring Session	<a href="#">Deploy Monitoring Session</a>
8	View Monitoring Session Statistics	<a href="#">View Monitoring Session Statistics</a>

# Deploy GigaVUE Cloud Suite for Azure

This chapter describes how to connect, launch, and deploy the fabric components of GigaVUE Cloud Suite for Azure.

Refer to the following topics for details:

- [Create Azure Credentials](#)
- [Prepare UCT-V to Monitor Traffic](#)
- [Install Custom Certificate](#)
- [Adding Certificate Authority](#)
- [Create Monitoring Domain](#)
- [Configure GigaVUE Fabric Components in GigaVUE-FM](#)
- [Configure Role-Based Access for Third Party Orchestration](#)
- [Disable GigaVUE-FM Orchestration in Monitoring Domain](#)
- [Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure](#)

Refer [Deploying GigaVUE Cloud Suite for Azure using V Series with Hybrid architecture](#) for more detailed information.

## Create Azure Credentials

You can monitor workloads across multiple Azure subscriptions within one monitoring domain. All the deployed GigaVUE fabric nodes are shared among many Azure subscriptions to reduce the cost since each Azure subscription used to have a set of GigaVUE fabric nodes.



- After launching GigaVUE-FM in Azure, the **Managed Identity** authentication credential is automatically added to the Azure Credential page as the default credential.
- You can only add the **Application ID with Client Secret** authentication credentials to the Azure Credential page.

To create Azure credentials:

1. Go to **Inventory > VIRTUAL > Azure**, and then click **Settings > Credential**. The Azure Credential page appears.
2. In the Azure Credential page, click **Add**. The **Configure Credential** wizard appears.

3. Enter or select the appropriate information for the Azure credential as described in the following table.

Field	Description
Name	An alias used to identify the Azure credential.
Authentication Type	<p><b>Application ID with Client Secret:</b> Connection with Azure with a service principal. Enter the values for the following fields.</p> <ul style="list-style-type: none"> <li>o <b>Tenant ID</b>—a unique identifier of the Azure Active Directory instance.</li> <li>o <b>Application ID</b>—a unique identifier of an application in Azure platform.</li> <li>o <b>Application Secret</b>—a password or key to request tokens.</li> </ul> <p>Refer to <a href="#">Application ID with client secret</a> for more detailed information on how to create service principal and assign custom roles.</p>
Azure Environment	Select an Azure environment where your workloads are located. For example, Azure_US_Government.

4. Click **Save**. You can view the list of available credentials in the Azure Credential page.

## Prepare UCT-V to Monitor Traffic

A UCT-V is the primary Gigamon monitoring module that is installed in your Virtual Machines (VMs). This agent mirrors the selected traffic from the VMs, encapsulates it using VXLAN tunneling, and forwards it to the GigaVUE Cloud Suite® V Series node.

**NOTE:** The UCT-V installation is applicable only when the UCT-V is your traffic acquisition method.

A UCT-V consists of a source interface and a destination interface. The network packets collected from the source interface are sent to the destination interface. From the destination interface, the packets traverse through VXLAN tunnel interface to the GigaVUE V Series node.

A source interface can be configured with one or more Network Interface Cards (NICs). While configuring a source interface, you can specify the direction of the traffic to be monitored in the VM. The direction of the traffic can be egress, ingress, or both.

Refer to the following sections for more information:

- [Linux UCT-V Installation](#)
- [Windows Agent Installation](#)
- [Create Images with the Agent Installed](#)

## Supported Operating Systems for UCT-V

**Supported Operating System for UCT-V<sup>1</sup> is v6.4.00**

**Supported Operating Systems for G-vTAP Agents are v1.8-3, v1.8-4, v1.8-5, v1.8-7, v6.1.00, v6.2.00, v6.3.00**

Operating System	Supported Versions
Ubuntu/Debian	Versions 18-04 and above are supported.
CentOS/RHEL/Fedora	Versions 7.5 and above.
Amazon Linux	Versions 1 and 2 (For version 2, package iproute-tc must be installed first)
Windows Server	Versions 2012 through 2022
Windows Client	Versions 10 and 11
RHEL	Versions 8.8 and above.

<sup>1</sup>From Software version 6.4.00, G-vTAP Agent is renamed to UCT-V.

GigaVUE-FM version 6.4 supports UCT-V version 6.4 as well as (n-2) versions. It is always recommended to use the latest version of UCT-V with GigaVUE-FM, for better compatibility.

## Linux UCT-V Installation

Refer to the following sections for the Linux agent installation:

- [Single NIC Configuration](#)
- [Dual NIC Configuration](#)
- [Install UCT-V](#)

### Single NIC Configuration

A single NIC/vNIC acts both as the source and the destination interface. A UCT-V with a single NIC/vNIC configuration lets you monitor the ingress or egress traffic from the NIC/vNIC. The monitored traffic is sent out using the same NIC/vNIC.

For example, assume that there is only one interface eth0 in the monitoring VM. In the UCT-V configuration, you can configure eth0 as the source and the destination interface, and specify both egress and ingress traffic to be selected for monitoring purpose. The egress and ingress traffic from eth0 is mirrored and sent out using the same interface.

**NOTE:** Using a single NIC/vNIC as the source and the destination interface may cause increased latency in sending the traffic out from the VM.

Example of the UCT-V config file for a single NIC/vNIC configuration:

Grant permission to monitor ingress and egress traffic at iface

```
# eth0 mirror-src-ingress mirror-src-egress mirror-dst
```

### Dual NIC Configuration

A UCT-V lets you configure two NICs/vNICs. One NIC/vNIC can be configured as the source interface and another NIC/vNIC can be configured as the destination interface.

For example, assume that there is eth0 and eth1 in the monitoring VM. In the UCT-V configuration, eth0 can be configured as the source interface and egress traffic can be selected for monitoring purpose. The eth1 interface can be configured as the destination interface. So, the mirrored traffic from eth0 is sent to eth1. From eth1, the traffic is sent to the GigaVUE V Series Node.

Example of the UCT-V config file for a dual NIC/vNIC configuration:

Grant permission to monitor ingress and egress traffic at iface

```
# 'eth0' to monitor and 'eth1' to transmit the mirrored packets.
```

```
# eth0 mirror-src-ingress mirror-src-egress
# eth1 mirror-dst
```

## Install UCT-V

You must have sudo/root access to edit the UCT-V configuration file.

For dual or multiple NIC/ENI configuration, you may need to modify the network configuration files to make sure that the extra NIC/ENI will initialize at boot time.

**NOTE:** Before installing UCT-V **.deb** or **.rpm** packages on your Linux VMs, you must install packages like Python3 and Python modules (netifaces, urllib3, and requests).

You can install the UCT-Vs either from Debian or RPM packages.

Refer to the following topics for details:

- [Install UCT-V from Ubuntu/Debian Package](#)
- [Install UCT-V from RPM package](#)
- [Install UCT-V from Red Hat Enterprise Linux and CentOS with Selinux Enabled](#)

### Install UCT-V from Ubuntu/Debian Package

To install from a Debian package:

1. Download the UCT-V **6.4.00** Debian (.deb) package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Copy this package to your instance. Install the package with root privileges, for example:

```
$ ls gigamon-gigavue_uctv_6.4.00_amd64.deb
$ sudo dpkg -i gigamon-gigavue_uctv_6.4.00_amd64.deb
```

- Once the UCT-V package is installed, modify the file `/etc/uctv/uctv.conf` to configure and register the source and destination interfaces. The following examples registers eth0 as the mirror source for both ingress and egress traffic and eth1 as the destination for this traffic:

**NOTE:** Any changes to the UCT-V config file made after the initial setup require an UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. When you have an active, successful monitoring session deployed, modifying the UCT-V config file results in traffic loss until GigaVUE-FM does a periodic sync on its own every 15 minutes.

**Example 1**—Configuration example to monitor ingress and egress traffic at interface eth0 and use the same interface to send out the mirrored packets

```
# eth0 mirror-src-ingress mirror-src-egress mirror-dst
```

**Example 2**—Configuration example to monitor ingress and egress traffic at interface eth0 and use the interface eth1 to send out the mirrored packets

```
# eth0 mirror-src-ingress mirror-src-egress
# eth1 mirror-dst
```

**Example 3**—Configuration example to monitor ingress and egress traffic at interface eth0 and eth 1; use the interface eth1 to send out the mirrored packets

```
# eth0 mirror-src-ingress mirror-src-egress
# eth1 mirror-src-ingress mirror-src-egress mirror-dst
```

- Save the file.
- To enable the third-party orchestration, a configuration file `/etc/gigamon-cloud.conf` needs to be created with the following contents:

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  user: <Username>
  password: <Password>
  remoteIP: <IP address of the UCT-V Controller 1>,
            <IP address of the UCT-V Controller 2>
  remotePort: 8891
```

**NOTE:** User and Password must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the Username and Password created in the **Add Users** Section.

- Reboot the instance.

The UCT-V status will be displayed as running. Check the status using the following command:

```
$ sudo /etc/init.d/uctv status
UCT-V is running
```

### Install UCT-V from RPM package

To install from an RPM (.rpm) package on a Redhat, CentOS, or other RPM-based system:

1. Download the UCT-V 6.4.00 RPM (.rpm) package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Copy this package to your instance. Install the package with root privileges, for example:

```
$ ls gigamon-gigavue_uctv_6.4.00_x86_64.rpm
$ sudo rpm -i gigamon-gigavue_uctv_6.4.00_x86_64.rpm
```

3. Modify the file `/etc/uctv/uctv.conf` to configure and register the source and destination interfaces. The following example registers the eth0 as the mirror source for both ingress and egress traffic and registers eth1 as the destination for this traffic as follows:

**NOTE:** Any changes to the UCT-V config file made after the initial setup require an agent restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. When you have an active, successful monitoring session deployed, modifying the UCT-V config file results in traffic loss until GigaVUE-FM does a periodic sync on its own every 15 minutes.

**Example 1**—Configuration example to monitor ingress and egress traffic at interface eth0 and use the same interface to send out the mirrored packets

```
# eth0 mirror-src-ingress mirror-src-egress mirror-dst
```

**Example 2**—Configuration example to monitor ingress and egress traffic at interface eth0 and use the interface eth1 to send out the mirrored packets

```
# eth0 mirror-src-ingress mirror-src-egress
# eth1 mirror-dst
```

**Example 3**—Configuration example to monitor ingress and egress traffic at interface eth0 and eth 1; use the interface eth1 to send out the mirrored packets

```
# eth0 mirror-src-ingress mirror-src-egress
# eth1 mirror-src-ingress mirror-src-egress mirror-dst
```

4. Save the file.



5. To enable the third-party orchestration, a configuration file **/etc/gigamon-cloud.conf** needs to be created with the following contents:

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  user: <Username>
  password: <Password>
  remoteIP: <IP address of the UCT-V Controller 1>,
            <IP address of the UCT-V Controller 2>
  remotePort: 8891
```

**NOTE:** User and Password must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the UserName and Password created in the **Add Users** Section.

6. Reboot the instance.

Check the status with the following command:

```
$ sudo service uctv status
UCT-V is running
```

### Install UCT-V from Red Hat Enterprise Linux and CentOS with Selinux Enabled

This section provides instructions on how to install UCT-V on Red Hat and CentOS.

Prerequisites:

- For multiple NIC/ENI configuration, you might have to to modify the network configuration files to make sure that the extra NIC/ENI will initialize at boot time.
- Install the packages Python3 and Python modules such as netifaces, urllib3, and requests.
- The packages iproute-tc, tc is required for RHEL and CentOS VMs.
- You must have sudo/root access to edit the UCT-V configuration file.
- You must ensure that the port 9901 is allowed in the Firewall. This port is required for the communication between UCT-V and UCT-V Controller.

To install UCT-V on Redhat, CentOS, or other RPM-based system using the RPM package, perform the following steps:

1. Download the following packages from the [Gigamon Customer Portal](#):
  - gigamon-gigavue\_uctv\_6.4.00\_x86\_64.rpm
2. Copy the downloaded UCT-V package files to UCT-V.

3. Install UCT-V package:

```
sudo rpm -ivh gigamon-gigavue_uctv_6.4.00_x86_64.rpm
```

4. Edit the **uctv.conf** file to configure the required interface as source/destination for mirror:

**NOTE:** If you make any changes to the UCT-V agent config file after the initial setup, you need to restart the UCT-V and refresh or synchronize the inventory from GigaVUE-FM to reflect the changes and start traffic mirroring again. However, if you have an ongoing monitoring session that is active and functioning well, modifying the UCT-V config file can cause traffic to be lost until GigaVUE-FM performs an automatic synchronization every 15 minutes.

```
# eth0 mirror-src-ingress mirror-src-egress mirror-dst  
# sudo systemctl status uctv
```

5. Reboot the instance.

## Windows UCT-V Installation

Windows UCT-V allows you to select the network interfaces by subnet/CIDR and modify the corresponding monitoring permissions in the configuration file. This gives you more granular control over what traffic is monitored and mirrored.

VXLAN is the only supported tunnel type for Windows UCT-V.

### Windows UCT-V Installation Using MSI Package

To install the Windows UCT-V using the MSI file:

1. Download the Windows UCT-V **6.4.00** MSI package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Install the downloaded MSI package as **Administrator** and the UCT-V service starts automatically.

- Once the UCT-V package is installed, modify the file **C:\ProgramData\uctv\gigamon-cloud.conf** to configure and register the source and destination interfaces.

**NOTE:** Any changes to the UCT-V config file made after the initial setup require an UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. When you have an active, successful monitoring session deployed, modifying the UCT-V config file results in traffic loss until GigaVUE-FM does a periodic sync on its own every 15 minutes.



Following are the rules to modify the UCT-V configuration file:

- Interface is selected by matching its CIDR address with config entries.
- For the VMs with single interface (*.conf file modification is optional*):
  - if neither mirror-src permissions is granted to the interface, both mirror-src-ingress and mirror-src-egress are granted to it.
  - mirror-dst is always granted implicitly to the interface.
- For the VMs with multiple interfaces:
  - mirror-dst needs to be granted explicitly in the config file. Only the first matched interface is selected for mirror-dst, all other matched interfaces are ignored.
  - if none interfaces is granted any mirror-src permission, all interfaces will be granted mirror-src-ingress and mirror-src-egress.

**Example 1**—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the same interface to send out the mirrored packets.

```
192.168.1.0/24 mirror-src-ingress mirror-src-egress mirror-dst
```

**Example 2**—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the interface 192.168.2.0/24 to send out the mirrored packets.

```
192.168.1.0/24 mirror-src-ingress mirror-src-egress
192.168.2.0/24 mirror-dst
```

- Save the file.

5. To enable the third-party orchestration, a configuration file **C:\ProgramData\uctv\gigamon-cloud.conf** needs to be created with the following contents:

**Registration:**

```
groupName: <Monitoring Domain Name>
subGroupName: <Connection Name>
user: <Username>
password: <Password>
remoteIP: <<IP address of the UCT-V Controller 1>,
          <IP address of the UCT-V Controller 2>
remotePort: 8891
```

**NOTE:** User and Password must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the UserName and Password created in the **Add Users** Section.

6. To restart the Windows UCT-V, perform one of the following actions:
  - Restart the VM.
  - Run 'sc stop uctv' and 'sc start uctv' from the command prompt.
  - Restart the UCT-V from the Windows Task Manager.

You can check the status of the UCT-V in the Service tab of the Windows Task Manager.

## Windows UCT-V Installation Using ZIP Package

To install the Windows UCT-V using the ZIP package:

1. Download the Windows UCT-V **6.4.00** ZIP package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Extract the contents of the .zip file into a convenient location.
3. Run 'install.bat' as an **Administrator** and the UCT-V service starts automatically.

- Once the UCT-V package is installed, modify the file **C:\ProgramData\Uct-v\uctv.conf** to configure and register the source and destination interfaces.

**NOTE:** Any changes to the UCT-V config file made after the initial setup require an UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. When you have an active, successful monitoring session deployed, modifying the UCT-V config file results in traffic loss until GigaVUE-FM does a periodic sync on its own every 15 minutes.



Following are the rules to modify the UCT-V configuration file:

- Interface is selected by matching its CIDR address with config entries.
- For the VMs with single interface (*.conf file modification is optional*):
  - if neither mirror-src permissions is granted to the interface, both mirror-src-ingress and mirror-src-egress are granted to it.
  - mirror-dst is always granted implicitly to the interface.
- For the VMs with multiple interfaces:
  - mirror-dst needs to be granted explicitly in the config file. Only the first matched interface is selected for mirror-dst, all other matched interfaces are ignored.
  - if none interfaces is granted any mirror-src permission, all interfaces will be granted mirror-src-ingress and mirror-src-egress.

**Example 1**—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the same interface to send out the mirrored packets.

```
192.168.1.0/24 mirror-src-ingress mirror-src-egress mirror-dst
```

**Example 2**—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the interface 192.168.2.0/24 to send out the mirrored packets.

```
192.168.1.0/24 mirror-src-ingress mirror-src-egress
192.168.2.0/24 mirror-dst
```

- Save the file.

6. To enable the third-party orchestration, a configuration file **C:\ProgramData\uctv\gigamon-cloud.conf** needs to be created with the following contents:

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  user: <Username>
  password: <Password>
  remoteIP: <IP address of UCT-V Controller 1, IP address of UCT-V
Controller 2>
  remotePort: 8891
```

**NOTE:** User and Password must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the UserName and Password created in the **Add Users** Section.

7. To restart the Windows UCT-V, perform one of the following actions:
- Restart the VM.
  - Run 'sc stop uctv' and 'sc start uctv' from the command prompt.
  - Restart the UCT-V from the Windows Task Manager.

You can check the status of the UCT-V in the Service tab of the Windows Task Manager.

**NOTE:** You must edit the Windows Firewall settings to grant access to the uctv process. To do this, access the Windows Firewall settings and find “uctvd” in the list of apps and features. Select it to grant access. Be sure to select both Private and Public check boxes. If “uctvd” does not appear in the list, click **Add another app...** Browse your program files for the uctv application (uctvd.exe) and then click **Add**.

**(Disclaimer:** These are general guidelines for changing Windows Firewall settings. See Microsoft Windows help for official instructions on Windows functionality.)

## Create Images with the Agent Installed

If you want to avoid downloading and installing the UCT-Vs every time there is a new VM to be monitored, you can save the UCT-V running on a VM as a private image. When a new VM is launched that contains the UCT-V, GigaVUE-FM automatically detects the new VM and updates the number of monitoring VMs in the monitoring session.

To save the UCT-V as an image, refer to [Capture VM to managed image](#) topic in the Microsoft Azure Documentation.

## Uninstall UCT-V

This section describes how to uninstall UCT-V for Windows UCT-V and Linux UCT-V

## Uninstall Linux UCT-V

The following steps provide instructions on how to uninstall Linux UCT-V

Stop the UCT-V service using the following commands:

For Ubuntu/Debian Package:

```
sudo service uctv stop
```

For RPM package or Red Hat Enterprise Linux and CentOS with Selinux Enabled:

```
sudo systemctl stop uctv
```

Uninstall the UCT-V using the following:

For Ubuntu/Debian Package:

```
sudo dpkg -r uctv
```

For RPM package:

```
sudo rpm -e uctv
```

For Red Hat Enterprise Linux and CentOS with Selinux Enabled:

```
sudo rpm -e uctv
```



## Uninstall Windows UCT-V

To uninstall Windows UCT-V:

1. On your windows, go to **Task Manager > Services**. Search for **uctv**.
2. Right click **uctv** and select **Stop**.
3. Go to **Control Panel** search for uctv and uninstall.

## Upgrade or Reinstall UCT-V

To upgrade UCT-V, delete the existing UCT-V and installing the new version of UCT-V.

**NOTE:** Before deleting the UCT-V, take a back up copy of **/etc/uctv/uctv.conf** configuration file. Follow this step to avoid reconfiguring the source and destination interfaces.

Refer to [Uninstall UCT-V](#) for more detailed information on how to uninstall UCT-V.

Refer to the following topics for more detailed information on how to install new UCT-V:

- [Linux UCT-V Installation](#)
- [Windows UCT-V Installation](#)

## Install Custom Certificate

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

You can upload the custom certificate in two ways:

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

### Upload Custom Certificates using GigaVUE-FM

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

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

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

4. Click **Save**.

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

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

## Upload Custom Certificate using Third Party Orchestration

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

For integrated mode:

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

For generic mode:

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

## Adding Certificate Authority

This section describes how to add Certificate Authority in GigaVUE-FM.

### CA List

The Certificate Authority (CA) List page allows you to add the root CA for the devices.

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

1. Go to **Inventory > Resources > Security > CA List**.
2. Click **Add**, to add a new Custom Authority. The **Add Certificate Authority** page appears.
3. Enter or select the following information.

Field	Action
Alias	Alias name of the CA.
File Upload	Choose the certificate from the desired location.

4. Click **Save**.

## Create Monitoring Domain

You must establish a connection between GigaVUE-FM and your Azure environment before you can perform the configuration steps. Creating a monitoring domain in GigaVUE-FM allows you to establish a connection between your Azure environment and GigaVUE-FM. After establishing a connection, you will be able to use GigaVUE-FM to specify a launch configuration for the UCT-V Controllers, GigaVUE V Series Proxy, and GigaVUE V Series Nodes in the specified VNet and Resource Groups. GigaVUE-FM connects to Azure using either an Application ID with the client secret or the MSI method of authentication. After the connection establishment, GigaVUE-FM launches the UCT-V Controller, GigaVUE V Series Proxy, and GigaVUE V Series 2 Node.

To create an Azure monitoring domain in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > Azure**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. In the Monitoring Domain page, click New. The **Azure Monitoring Domain Configuration** wizard appears.

Monitoring Domain Configuration


Save

Cancel

<b>Monitoring Domain*</b>	<input type="text" value="Enter a monitoring domain name"/>
<b>Use V Series 2</b>	<input checked="" type="checkbox"/> Yes
<b>Traffic Acquisition Method*</b>	<input type="text" value="UCT-V"/>   v
<b>Traffic Acquisition Tunnel MTU*</b>	<input type="text" value="1450"/>
<b>Use FM to Launch Fabric</b> ⓘ	<input checked="" type="checkbox"/> Yes

3. Enter or select the appropriate information for the monitoring domain as described in the following table.

Field	Description
Monitoring Domain	An alias used to identify the monitoring domain.
Use V Series 2	Select <b>Yes</b> for V Series 2 configuration.
Traffic Acquisition Method	<p>Select a Tapping method. The available options are:</p> <ul style="list-style-type: none"> <li>▪ <b>UCT-V:</b> If you select UCT-V as the tapping method, the traffic is acquired from the UCT-Vs installed on your standard VMs in the Resource Group or in the Scale Sets. Then the acquired traffic is forwarded to the GigaVUE V Series nodes. You must configure the UCT-V Controller to monitor the UCT-Vs.</li> <li>▪ <b>Customer Orchestrated Source:</b> If you use select Customer Orchestrated Source as the tapping method, you can select the tunnel as a source where the traffic is directly tunneled to GigaVUE V Series nodes without deploying UCT-Vs or UCT-V Controllers.</li> </ul> <p><b>NOTE:</b> Select the Traffic Acquisition Method as Customer Orchestrated Source if you wish to use Observability Gateway (AMX) application.</p>
Traffic Acquisition Tunnel MTU	<p>The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the UCT-V to the GigaVUE V Series node.</p> <p>For VXLAN, the default value is 1450. The UCT-V tunnel MTU should be 50 bytes less than the agent's destination interface MTU size.</p>
Use FM to Launch Fabric	Select <b>Yes</b> to <a href="#">Configure GigaVUE Fabric Components in GigaVUE-FM</a> or select <b>No</b> to <a href="#">Configure GigaVUE Fabric Components in Azure</a> .
<p><b>Connections</b></p> <p>Connections</p> <div style="border: 1px solid #ccc; padding: 10px;"> <p>Name* <input type="text" value="Enter a connection name"/></p> <p>Credential* <input type="text" value="Credential Name..."/></p> <p>Subscription ID* <input type="text" value="Subscription ID..."/></p> <p>Region* <input type="text" value="Region Name..."/></p> <p>Resource Groups* <input checked="" type="checkbox"/> Discovered <input type="checkbox"/> Regex ⓘ</p> <p><input type="text" value="Resource Groups..."/></p> </div> <p style="text-align: right; margin-right: 20px;">+ -</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>• A Monitoring Domain can have multiple connections, however only one connection can have <b>Managed Service Identity</b> as the <b>Credential</b>.</p> </div>	

Field	Description
	<ul style="list-style-type: none"> <li>The connections in a monitoring domain can be a combination of multiple <b>Application ID with Client Secret</b> (Service Principal) accounts, or one <b>Managed Service Identity</b> and multiple <b>Application ID with Client Secret</b> (Service Principal) accounts.</li> <li>Each connection can have only one <b>Subscription ID</b>.</li> </ul>
Name	An alias used to identify the connection.
Credential	Select an Azure credential. For detailed information, refer to <a href="#">Create Azure Credentials</a> .
Subscription ID	A unique alphanumeric string that identifies your Azure subscription.
Region	Azure region for the monitoring domain. For example, West India.
Resource Groups	Select the Resource Groups of the corresponding VMs to monitor.  <b>NOTE:</b> This field is only available if you select <b>UCT-V</b> as the <b>Traffic Acquisition Method</b> .


4. Click **Save** and the **Azure Fabric Launch Configuration** wizard appears.

## Manage Monitoring Domain

You can view the details of the monitoring domain that are created in the list view. The list view details can be viewed based on:

- [Monitoring Domain](#)
- [Connections Domain](#)
- [Connections Domain](#)
- [UCT-Vs](#)

You can also filter the monitoring domain based on a specified criterion. In the monitoring domain page there are two filter options as follows:

- Right filter - Click the Filter button on the right to filter the monitoring domain based on a specific criterion.
- Left filter - Click the  to filter the monitoring domain based on the domain and connections. You can click **+** to create a new monitoring domain. This filter once applied also works even when the tabs are swapped.

To edit or delete a specific monitoring domain, select the monitoring domain, click the ellipses "...".

When you click a monitoring domain, you can view details of it in a split view of the window. In the split view window, you can view the details such as Configuration, Launch Configuration and V Series configuration.

## Monitoring Domain

The list view shows the following information in the monitoring domain page:

- Monitoring Domain
- Connections
- Tunnel MTU
- Acquisition Method
- Centralized connection
- Management Network

**NOTE:** Click the  to select the columns that should appear in the list view.

Use the following buttons to manage your Monitoring Domain:

Button	Description
New	Use to create new connection
Actions	<p>You can select a monitoring domain and then perform the following options:</p> <ul style="list-style-type: none"> <li>● <b>Edit Monitoring Domain</b>- Select a monitoring domain and then click <b>Edit Monitoring domain</b> to update the configuration.</li> <li>● <b>Delete Domain</b> - You can select a monitoring domain or multiple monitoring domains to delete them.</li> <li>● <b>Edit Fabric</b>-You can select one fabric or multiple fabrics of the same monitoring domain to edit a fabric. You cannot choose different fabrics of multiple monitoring domains at the same time and edit their fabrics</li> <li>● <b>Deploy Fabric</b> - -You can select a monitoring domain to deploy a fabric, you cannot choose multiple monitoring domains at the same time to deploy fabrics. This option is only enabled when there is No FABRIC (launch configuration) for that specific monitoring domain and GigaVUE-FM orchestration is enabled.. You must create a fabric in the monitoring domain, if the option is disabled</li> <li>● <b>Upgrade Fabric</b>-You can select a monitoring domain or multiple monitoring domains to upgrade the fabric. You can upgrade the V-Series nodes using this option.</li> <li>● <b>Delete Fabric</b>- You can delete all the fabrics associated with the monitoring domain of the selected Fabric.</li> <li>● <b>Edit SSL Configuration</b> - You can use this option to add Certificate Authority and the SSL Keys.</li> </ul>
Filter	<p>Filters the monitoring domain based on the list view options that are configured:</p> <ul style="list-style-type: none"> <li>● <b>Tunnel MTU</b></li> <li>● <b>Acquisition Method</b></li> <li>● <b>Centralised Connection</b></li> <li>● <b>Management Subnet</b></li> </ul> <p>You can view the filters applied on the top of the monitoring domain page as a button. You can remove the filters by closing the button.</p>

## Connections Domain

To view the connection related details for a monitoring domain, click the **Connections** tab.

The list view shows the following details:

- Connections
- Monitoring Domain
- Status
- Fabric Nodes
- User Name
- Region

## Fabric

To view the fabric related details for a monitoring domain, click the **Fabric** tab.

The list view shows the following details:

- Connections
- Monitoring Domain
- Fabric Nodes
- Type
- Management IP
- Version
- Status - Click to view the upgrade status for a monitoring domain.
- Security groups

## UCT-Vs

To view all the UCT-Vs associated with the available monitoring domains click the **UCT-Vs** tab.

The list view shows the following details:

- Monitoring Domain
- IP address
- Registration time
- Last heartbeat time
- Agent mode
- Status

Refer to [Configure Azure Settings](#) , for more detailed information on **Settings**



# Configure GigaVUE Fabric Components in GigaVUE-FM

After configuring the Monitoring Domain, you will be navigated to the Azure Fabric Launch Configuration page.

In the same **Azure Fabric Launch Configuration** page, you can configure all the GigaVUE fabric components.

Enter or select the required information as described in the following table.

Fields	Description
Connections	A connection that you created in the monitoring domain page. Refer to <a href="#">Create Monitoring Domain</a> for more information.
Centralized Virtual Network	Alias of the centralized VNet in which the UCT-V Controllers, V Series Proxies, and the GigaVUE V Series nodes are launched.
Authentication Type	Select SSH Public Key as the Authentication Type to connect with the Centralized VNet.
SSH Public Key	The SSH public key for the GigaVUE fabric nodes.
Resource Group	The Resource Groups created in Azure for communication between the controllers, nodes, and GigaVUE-FM.
Security Groups	The security group created for the GigaVUE fabric nodes.
Enable Custom Certificates	Enable this option to validate the custom certificate during SSL Communication. GigaVUE-FM validates the Custom certificate with the trust store. If the certificate is not available in Trust Store, communication does not happen, and an handshake error occurs.  <b>NOTE:</b> If the certificate expires after the successful deployment of the fabric components, then the fabric components moves to failed state.
Certificate	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For more detailed information, refer to <a href="#">Install Custom Certificate</a> .
Prefer IPv6	Enables IPv6 to deploy all the Fabric Controllers, and the tunnel between hypervisor to V Series node using IPv6 address. If the IPv6 address is unavailable, it uses an IPv4 address. This functionality is supported only in OVS Mirroring.
Click <b>Yes</b> to configure V Series Proxy for the monitoring domain. Refer to <a href="#">Configure GigaVUE V Series Proxy</a>	



To deploy GigaVUE fabric images (GigaVUE V Series Nodes, UCT-V Controller, and GigaVUE V Series Proxies) in GigaVUE-FM, you must accept the terms of the GigaVUE



fabric images from the Azure marketplace using the Azure CLI or PowerShell. Refer to [Prerequisites](#) for more detailed information.

Refer to the following topics for details:

- [Configure UCT-V Controllers](#)
- [Configure GigaVUE V Series Proxy](#)
- [Configure GigaVUE V Series Node](#)

## Configure UCT-V Controller

A UCT-V Controller manages multiple UCT-Vs and orchestrates the flow of mirrored traffic to GigaVUE V Series nodes.

**NOTE:** A single UCT-V Controller can manage up to 1000 UCT-Vs. The recommended minimum instance type is Standard\_B1s for UCT-V Controller.

A UCT-V Controller can only manage UCT-Vs that has the same version.

To configure the UCT-V Controllers:

**NOTE:** You cannot configure UCT-V Controller for Customer Orchestrated Source as the traffic acquisition method.

In the **Azure Fabric Launch Configuration** page, Enter or select the appropriate values for the UCT-V Controller as described in the following table.

<b>Controller Version(s)</b>	<input type="button" value="Add"/>
	<div style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span>Image</span> <div style="border: 1px solid #ccc; padding: 2px 10px;">184</div> <span>▼</span> </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 5px;"> <span>Size</span> <div style="border: 1px solid #ccc; padding: 2px 10px;">Standard_B1...</div> <span>▼</span> </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 5px;"> <span>Number of Instances</span> <input style="width: 50px; text-align: center;" type="text" value="1"/> </div> </div>
<b>Management Subnet</b>	<div style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span>IP Address Type</span> <input checked="" type="radio"/> Private           <input type="radio"/> Public         </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 5px;"> <span>Subnet</span> <div style="border: 1px solid #ccc; padding: 2px 10px;">mgmt</div> <span>▼</span> </div> </div>
<b>Additional Subnets</b>	<input type="button" value="Add Subnet"/>
<b>Tags</b>	<input type="button" value="Add"/>

Fields	Description
<b>Controller Version(s)</b>	<p>The UCT-V Controller version you configure must always be the same as the UCT-Vs' version number deployed in the VM machines.</p> <p>If there are multiple versions of UCT-Vs deployed in the VM machines, then you must configure multiple versions of UCT-V Controllers that matches the version numbers of the UCT-Vs.</p> <div data-bbox="391 422 1466 510" style="border: 1px solid #ccc; padding: 5px;"> <p><b>NOTE:</b> If there is a version mismatch between UCT-V Controllers and UCT-Vs, GigaVUE-FM cannot detect the agents in the instances.</p> </div> <p>To add UCT-V Controllers:</p> <ol style="list-style-type: none"> <li>a. Under <b>Controller Versions</b>, click <b>Add</b>.</li> <li>b. From the <b>Image</b> drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances.</li> <li>c. From the <b>Size</b> drop-down list, select a size for the UCT-V Controller. The default size is Standard_B1s.</li> <li>d. In <b>Number of Instances</b>, specify the number of UCT-V Controllers to launch. The minimum number you can specify is 1.</li> </ol>
<b>Management Subnet</b>	<p><b>IP Address Type:</b> Select one of the following IP address types:</p> <ul style="list-style-type: none"> <li>▪ Select <b>Private</b> if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the UCT-V Controller instances and GigaVUE-FM instances in the same network.</li> <li>▪ Select <b>Public</b> if you want the IP address to be assigned from Azure's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. On selecting Public IP address type, you must select all the required Public IPs.</li> </ul> <p><b>Subnet:</b> Select a Subnet for UCT-V Controller. The subnet that is used for communication between the UCT-V Controllers and the UCT-Vs, as well as to communicate with GigaVUE-FM.</p> <p>Every fabric node (both controllers and the nodes) need a way to talk to each other and GigaVUE-FM. So, they should share at least one management plane/subnet.</p> <div data-bbox="391 1287 1466 1375" style="border: 1px solid #ccc; padding: 5px;"> <p><b>NOTE:</b> Some instance types are supported in Azure platform. Refer to Microsoft Azure documentation to learn on supported instance types.</p> </div>
<b>Agent Tunnel Type</b>	<p>The type of tunnel used for sending the traffic from UCT-Vs to GigaVUE V Series Nodes. The options are GRE or VXLAN tunnels. If any Windows agents co-exist with Linux agents, VXLAN must be selected.</p>

Fields	Description
<b>Agent Tunnel CA</b>	The Certificate Authority (CA) that should be used in the UCT-V Controller for connecting the tunnel.
<b>Additional Subnet(s)</b>	<p>(Optional) If there are UCT-Vs on subnets that are not IP routable from the management subnet, additional subnets must be specified so that the UCT-V Controller can communicate with all the UCT-Vs.</p> <p>Click <b>Add</b> to specify additional data subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.</p>
<b>Tag(s)</b>	<p>(Optional) The key name and value that helps to identify the UCT-V Controller instances in your Azure environment. For example, you might have UCT-V Controllers deployed in many regions. To distinguish these UCT-V Controllers based on the regions, you can provide a name that is easy to identify such as us-west-2-uctv-controllers. To add a tag:</p> <ol style="list-style-type: none"> <li data-bbox="435 659 607 688"><b>a.</b> Click <b>Add</b>.</li> <li data-bbox="435 699 1159 728"><b>b.</b> In the <b>Key</b> field, enter the key. For example, enter Name.</li> <li data-bbox="435 739 1425 768"><b>c.</b> In the <b>Value</b> field, enter the key value. For example, us-west-2-uctv-controllers.</li> </ol>

## Configure GigaVUE V Series Proxy

GigaVUE V Series Proxy can manage multiple GigaVUE V Series Nodes and orchestrates the flow of traffic from GigaVUE V Series nodes to the monitoring tools. GigaVUE-FM uses one or more GigaVUE V Series Proxies to communicate with the GigaVUE V Series nodes.

**NOTE:** A single GigaVUE V Series Proxy can manage up to 100 GigaVUE V Series nodes. The recommended minimum instance type is Standard\_B1s for V Series Proxy.

To configure the GigaVUE V Series Proxy:

1. In the **Azure Fabric Launch Configuration** page, Select **Yes** to **Configure a V Series Proxy** and the GigaVUE V Series Proxy fields appears.
2. Enter or select the appropriate values for the V Series Proxy. Refer to the [UCT-V Controller field descriptions](#) for detailed information.

## Configure GigaVUE V Series Node

GigaVUE V Series node is a visibility node that aggregates mirrored traffic from multiple UCT-Vs. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to GigaVUE Cloud Suite for Azure using the standard VXLAN tunnels.

To launch a GigaVUE V Series node:

In the **Azure Fabric Launch Configuration** page, enter or select the appropriate values for the GigaVUE V Series Node.

### V Series Node

<b>Image</b>	<input type="text" value="gigavuev-gigavuev-series-node-2.7.0-31087"/>
<b>Size</b>	<input type="text" value="Standard_D4s_v4   8 vCPUs"/>
<b>Disk Size (GB)</b>	<input type="text" value="&gt;= 30"/>
<b>IP Address Type</b>	<input checked="" type="radio"/> Private <input type="radio"/> Public
<b>Management Subnet</b>	<b>Subnet</b> <input type="text" value="mgmt"/>
<b>Data Subnets</b>	<input type="button" value="Add Subnet"/>
<b>Tags</b>	<input type="button" value="Add"/>

**Tool Subnet**  Tool Subnet ⓘ

**Subnet 1**

**Security Groups**

Fields	Description
<b>Image</b>	From the <b>Image</b> drop-down list, select a GigaVUE V Series Node image.
<b>Size</b>	From the <b>Size</b> down-down list, select a size for the GigaVUE V Series Node. The default size for GigaVUE V Series Node configuration is <b>Standard_D4s_v4</b> .
<b>Disk Size (GB)</b>	<p>The size of the storage disk. The default disk size is 30GB.</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #e6f2ff;"> <p><b>NOTE:</b> When using Application Metadata Exporter, the minimum recommended Disk Size is 80GB.</p> </div>
<b>IP Address Type</b>	Select one of the following IP address types:

Fields	Description
	<ul style="list-style-type: none"> <li>▪ Select <b>Private</b> if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the GigaVUE V Series Node instances and GigaVUE-FM instances in the same network.</li> <li>▪ Select <b>Public</b> if you want the IP address to be assigned from Azure's pool of public IP address. On selecting Public IP address type, you must select the number of Public IPs defined in the Maximum Instance.</li> </ul>
<b>Management Subnet</b>	<p><b>Subnet:</b> Select a management subnet for GigaVUE V Series. The subnet that is used for communication between the UCT-Vs and the GigaVUE V Series Nodes, as well as to communicate with GigaVUE-FM.</p> <p>Every fabric node (both controllers and the nodes) need a way to talk to each other and GigaVUE-FM. So, they should share at least one management plane/subnet.</p>
<b>Data Subnet(s)</b>	<p>The subnet that receives the mirrored VXLAN tunnel traffic from the UCT-Vs. Select a <b>Subnet</b> and the respective <b>Security Groups</b>. Click <b>Add</b> to add additional data subnets.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> Using the <b>Tool Subnet</b> checkbox you can indicate the subnets to be used by the GigaVUE V Series Node to egress the aggregated/manipulated traffic to the tools.</p> </div>
<b>Tag(s)</b>	<p>(Optional) The key name and value that helps to identify the GigaVUE V Series Node instances in your Azure environment. For example, you might have GigaVUE V Series Nodes deployed in many regions. To distinguish these GigaVUE V Series Nodes based on the regions, you can provide a name that is easy to identify. To add a tag:</p> <ol style="list-style-type: none"> <li>a. Click <b>Add</b>.</li> <li>b. In the <b>Key</b> field, enter the key. For example, enter Name.</li> <li>c. In the <b>Value</b> field, enter the key value.</li> </ol>
<b>Min Instances</b>	<p>The minimum number of GigaVUE V Series Nodes to be launched in the Azure connection.</p> <p>The minimum number of instances that can be entered is 1.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> Nodes will be launched when a monitoring session is deployed if GigaVUE-FM discovers some targets to monitor. The minimum amount will be launched at that time. The GigaVUE-FM will delete the nodes if they are idle for over 15 minutes.</p> </div>
<b>Max Instances</b>	<p>The maximum number of GigaVUE V Series Nodes that can be launched in the Azure connection. When the number of instances per V Series node exceeds the max instances specified in this field, increase the number in the Max Instances to Launch. When additional V Series nodes are launched, GigaVUE-FM re-balances the instances assigned to the nodes. This can result in a brief interruption of traffic.</p>

Click **Save** to complete the Azure Fabric Launch Configuration.

A monitoring domain is created, and you can view the monitoring domain and fabric component details by clicking on a monitoring domain name in the **Monitoring Domain** page.



## Configure Role-Based Access for Third Party Orchestration

Before deploying the fabric components using a third party orchestrator, we must create users, roles and the respective user groups in GigaVUE-FM. The Username and the Password provided in the User Management page will be used in the registration data that can be used to deploy the fabric components in your orchestrator.

## Users

The Users page lets you manage the GigaVUE-FM and GigaVUE-OS FM users. You can also configure user's role and user groups to control the access privileges of the user in GigaVUE-FM.

## Add Users

This section provides the steps for adding users. You can add users only if you are a user with **fm\_super\_admin role** or a user with either read/write access to the FM security Management category.


**IMPORTANT:** It is recommended to create users through GigaVUE-FM:

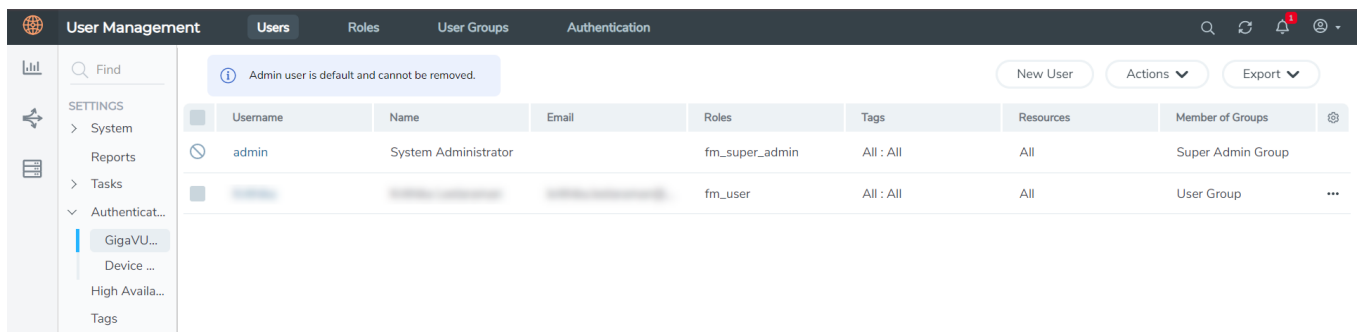
- You cannot view or manage users created in GigaVUE-FM CLI using GigaVUE-FM.
- You cannot view changes made to the users in GigaVUE-FM CLI in GigaVUE-FM.

**NOTE:** Monitor and operator users are not available in GigaVUE-FM. However, if you upgrade from a previous version in which monitor/operator users have been mapped in map default user, then after upgrade:

- **In AAA:** Users authenticated through the external servers will be assigned the fm\_user role.
- **In LDAP:** Remote group based DN entry will not be migrated.

To add users perform the following steps:

1. On the left navigation pane, click  and select **Authentication > GigaVUE-FM User Management > Users**. The **User** page is displayed.



**Figure 1** FM Users Page

2. Click **New User**. In the Add User wizard that appears perform the following steps.

**Add User** ✕

i All form elements are required unless indicated as optional. ✕

**Name**

**Username**

**Password**

**Confirm password**

**Email**

**User Group**  
 ?

**i** Your new password must contain:

- ✓ At least 8 characters and up to a maximum of 64 characters in length
- ✓ At least one numerical character
- ✓ At least one uppercase character
- ✓ At least one lowercase character
- ✓ At least one special character from -!@#S%^&\*()+

Cancel Ok

**Figure 2** *Create User*

- a. In the Add User pop-up box, enter the following details:
  - o **Name:** Actual name of the user
  - o **Username:** User name configured in GigaVUE-FM
  - o **Email:** Email ID of the user
  - o **Password/Confirm Password:** Password for the user. Refer to the [Change Your Password](#) section.
  - o **User Group:** User group

**NOTE:** GigaVUE-FM will prompt for your password.

- b. Click **Ok** to save the configuration.

The new user is added to the summary list view.

You can also assign users to roles and user groups that set the access permissions. Refer to the following sections for details:

- [Create Roles](#)
- [Create Groups.](#)

**NOTE:** If you have logged in as a user with **fm\_super\_admin** role or a user with either read/write access on FM security Management category, then click on the ellipsis to:

- **Assign User Group:** Assign user group to users.
- **Edit:** Edit the user details.
- **Delete:** Delete a user.
- **Unlock:** Unlock a locked user.

## How to Unlock User Account

To unlock a locked user, you must be a user with **fm\_super\_admin** role or a user with either read/write access on FM security Management category.

To unlock:

1. Select the required user whose account you want to lock.
2. Click on the ellipses and select **Unlock**. You can also click the **Actions** drop-down button and select **Unlock**.
3. A notification message prompts up. Click **Unlock** to unlock the user.

The user account is unlocked. An event is triggered in the Events page, and an email will be sent if Email Notification settings are configured.

The User name and password provided in this section will be used as the User and Password in the registration data.

After adding User, you must configure roles for third party orchestration.

## Create Roles

You can associate a role with user. Under the **Select Permissions** tab select **Third Party Orchestration** and provide read/write permissions.

## Create Roles

This section describes the steps for creating roles and assigning user(s) to those roles.

GigaVUE-FM has the following default roles:

- **fm\_super\_admin** — Allows a user to do everything in Fabric Manager, including adding or modifying users and configuring all AAA settings in the RADIUS, TACACS+, and LDAP tabs. Can change password for all users.
- **fm\_admin** — Allows a user to do everything in Fabric Manager except add or modify users and change AAA settings. Can only change own password.
- **fm\_user** — Allows a user to view everything in Fabric Manager, including AAA settings, but cannot make any changes.

**NOTE:** If you are a user with read-only access you will be restricted from performing any configurations on the screen. The menus and action buttons in the UI pages will be disabled appropriately.

Starting in software version 5.7, you can create custom user roles in addition to the default user roles in GigaVUE-FM. Access control for the default roles and the custom roles is based on the categories defined in GigaVUE-FM. These categories provide the ability to limit user access to a set of managed inventories such as ports, maps, cluster, forward list and so on.

Refer to the following table for the various categories and the associated resources. Hover your mouse over the resource categories in the Roles page to view the description of the resources in detail.

Category	Associated Resources
<b>All</b>	Manages all resources <ul style="list-style-type: none"> <li>● A user with fm_super_admin role has both read and write access to all the resource categories.</li> <li>● A user with fm_user role has only read access to all the resource categories.</li> </ul>
<b>Infrastructure Management</b>	Manages resources such as devices, cards, ports and cloud resources. You can add or delete a device in GigaVUE-FM, enable or disable cards, modify port parameters, set leaf-spine topology. The following resources belong to this category: <ul style="list-style-type: none"> <li>● <b>Physical resources:</b> Chassis, slots, cards ports, port groups, port</li> </ul>


Category	Associated Resources
	<p>pairs, cluster config, nodes and so on</p> <ul style="list-style-type: none"> <li>● <b>GigaVUE-FM inventory resources:</b> Nodes, node credentials</li> <li>● <b>Device backup/restore:</b> Device and cluster configuration</li> <li>● <b>Device license configuration:</b> Device/cluster licensing</li> <li>● <b>Statistics:</b> Device, port</li> <li>● <b>Tags:</b> Events, historical trending</li> <li>● <b>Device security:</b> SystemTime, System EventNotification, SystemLocalUser, System Security Policy Settings, AAA Authentication Settings, Device User Roles, LDAP Servers, RADIUS Servers, TACACS+ Servers</li> <li>● <b>Device maintenance:</b> Sys Dump, Syslog</li> <li>● <b>Cloud Infrastructure resources:</b> Cloud Connections, Cloud Proxy Server, Cloud Fabric Deployment, Cloud Configurations, Sys Dump, Syslog, Cloud licenses, Cloud Inventory.</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> Cloud APIs are also RBAC enabled.</p> </div>
<b>Traffic Control Management</b>	<p>Manages inline resources, flow maps, GigaSMART applications, second level maps, map chains, map groups. The following resources belong to this category:</p> <ul style="list-style-type: none"> <li>● <b>Infrastructure resources:</b> IP interfaces, circuit tunnels, tunnel endpoints, tunnel load balancing endpoints, ARP entries</li> <li>● Intent Based Orchestration resources: Policies, rules</li> <li>● <b>GigaSMART resources:</b> GigaSMART, GSgroups, vPorts, Netflow exporters</li> <li>● <b>Map resources:</b> Fabric, fabric resources, flow maps, maps, map chains, map groups, map templates</li> <li>● <b>Application intelligence resources:</b> Application visibility, Metadata, application filter resources</li> <li>● <b>Tag:</b> Flow manipulation - Netflow operations, Statistics - device port</li> <li>● Active visibility</li> <li>● <b>Inline resources:</b> Inline networks, Inline network groups, Inline tools, Inline tool groups, Inline serial tools, Inline heartbeat profile</li> <li>● <b>Cloud operation resources:</b> Monitoring session, stats, map library, tunnel library, tools library, inclusion/exclusion maps.</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> Cloud APIs are also RBAC enabled.</p> </div>
<b>FM Security Management</b>	<p>Ensures secure GigaVUE-FM environment. Users in this category can manage user and roles, AAA services and other security operations.</p>
<b>System Management</b>	<p>Controls system administration activities of GigaVUE-FM. User in this category are allowed to perform operations such as backup/restore of GigaVUE-FM and devices, and upgrade of GigaVUE-FM. The following GigaVUE-FM resources belong to this category:</p>

Category	Associated Resources
	<ul style="list-style-type: none"> <li>● Backup/restore</li> <li>● Archive server</li> <li>● License</li> <li>● Storage management</li> <li>● Image repo config</li> <li>● Notification target/email</li> </ul>
<b>Forward list/CUPS Management</b>	Manages the forward list configuration. The following resources belong to this category: <ul style="list-style-type: none"> <li>● GTP forward list</li> <li>● SIP forward list</li> </ul>
<b>Third Party Orchestration</b>	Used to deploy fabric components using external orchestrator.
<b>Device Certificate Management</b>	Manages device certificates.
Other Resource Management	Manages virtual and cloud resources

You can associate the custom user roles either to a single category or to a combination of categories based on which the users will have access to the resources. For example, you can create a 'Physical Devices Technician' role such that the user associated with this role can only access the resources that are part of the **Physical Device Infrastructure Management**.

**NOTE:** A user with **fm\_admin** role has both read and write access to all of the categories, but has read only access to the FM Security Management category.

To create a role

1. On the left navigation pane, click  and select **Authentication > GigaVUE-FM User Management > Roles**.
2. Click **New Role**.



**New Role**

All form elements are mandatory unless indicated as optional. x

Cancel Apply

**Role Name** Enter Role Name

**Description** Enter Description

**Select Permission**

Resources	Permissions	Description
> Infrastructure Management	Select a permission	Manage physical and cloud infrastr...
> Traffic Control Management	Select a permission	Manage inline resources, Define an...
> FM Security Management	Select a permission	Secure FM environment. User can ...
> System Management	Select a permission	Control system administration activ...
> Forwardlist Management	Select a permission	Manage the forwardlist configurati...

FM Instance: GigaVUE-FM Last Updated At: May 9, 2023 15:03:36

- In the New Role page, select or enter the following details:
  - Role Name:** Name of the role.
  - Description:** Description of the role.
  - Select Permission:** In the **Select Permission** table, select the required permission for the various resource categories.
- Click **Apply** to save the configuration.

## Create User Groups

You can use the user group option to associate the users with Roles and Tags. A user group consists of a set of roles and set of tags associated with that group. When a user is created they can be associated with one or more user groups.

## Create User Groups

Starting in software version 5.8.00, you can use the user group option to associate the users with Roles and Tags. A user group consists of a set of roles and set of tags associated with that group. When a user is created they can be associated with one or more user groups.

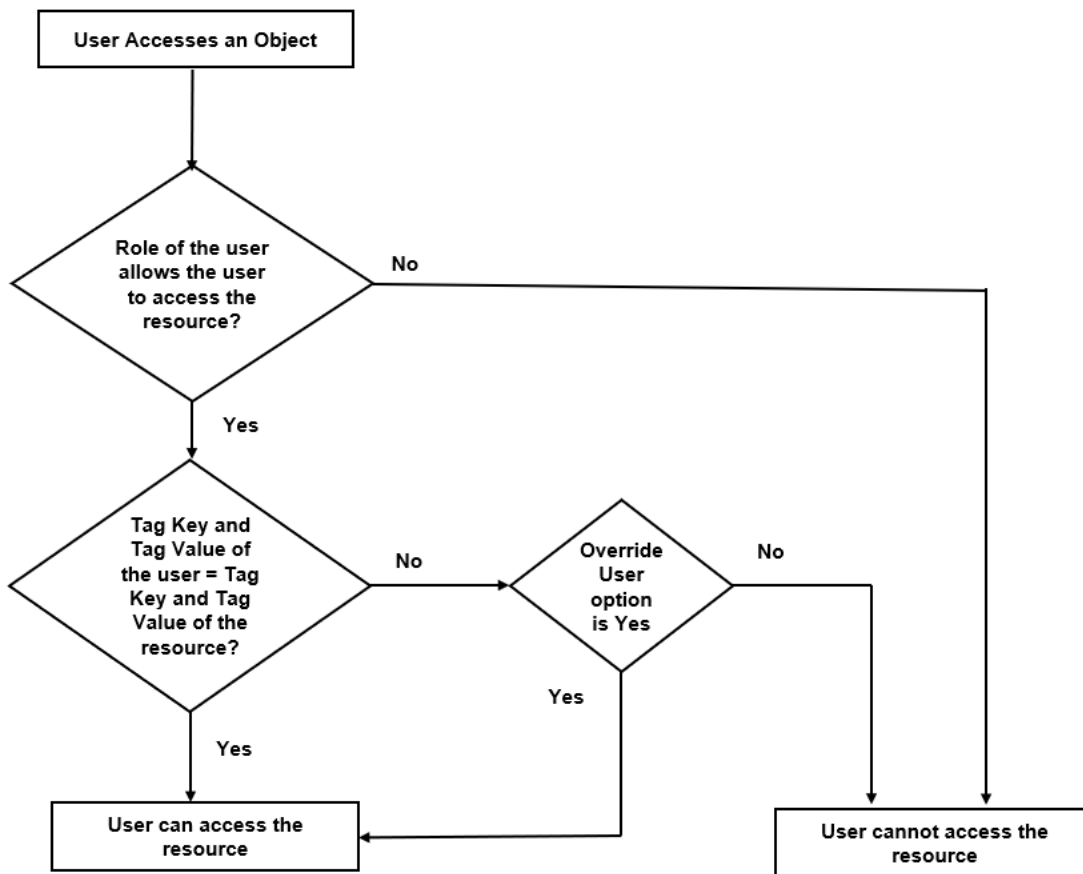
The following user groups are available by default in GigaVUE-FM. You will not be able to edit or change these groups in the system.

User Group	Tag Key and Tag Value	Permission
Super Admin Group	Tag Key = All Tag Value = All	Group with privileges of fm_super_adminrole.
Admin Group	Tag Key= All Tag Value = All	Group with privileges of fm_admin role.
View only user	Tag Key = All Tag Value = All	Group with privileges of fm_user role.


By creating groups and associating to tags and roles, you can control the users of the following:

- The category of resources which the user can access, such as the clusters, ports, maps and so on. This is defined using the **Roles** option. Refer to the Roles section for more details.
- The physical and logical resources that the user can access, such as the ports in a cluster that belong to a specific department in a location. This is defined using the **Tags** option.

Refer to the following flow chart to see how access control operation occurs when the user accesses a resource:



To create a user group:

1. On the left navigation pane, click , and then select **Authentication > GigaVUE-FM User Management > User Groups**.
2. Click **New Group**. In the Wizard that appears, perform the following steps. Click **Next** to progress forward and click **Back** to navigate backward and change the details.

The screenshot shows the 'New User Group' configuration wizard in the 'Assign Roles' step. The wizard has four steps: 1. Group Info, 2. Assign Roles (current), 3. Assign Tags, and 4. Assign Users. The 'Roles' table is as follows:

Roles	Description	Resources
<input type="checkbox"/> fm_super_admin	Allows a user to do everything in GigaVUE-FM, including add...	All
<input checked="" type="checkbox"/> fm_admin	Allows a user to do everything in GigaVUE-FM except adding...	Infrastructure Management+ 6 more
<input type="checkbox"/> fm_user	Allows a user to view everything in GigaVUE-FM, including A...	All

At the bottom of the table, there is a pagination control: 'Go to page: 1 of 1' and '3 roles total'.

3. In the **Group Info** tab, enter the following details:
  - **Group Name**
  - **Description**
4. In the **Assign Roles** tab, select the required role.
5. In the **Assign Tags** tab, select the required tag key and tag value.
6. In the **Assign Users** tab, select the required users. Click **Apply** to save the configuration. Click **Skip and Apply** to skip this step and proceed without adding users.

The new user group is added to the summary list view.

Click on the ellipses to perform the following operations:

- **Modify Users:** Edit the details of the users.
- **Edit:** Edit an existing group.

## Configure GigaVUE Fabric Components in Azure

This section provides step-by-step information on how to register GigaVUE fabric components using Azure Portal or a configuration file.

### Overview of Third-Party Orchestration

You can use your own Azure Orchestrator to deploy the GigaVUE fabric nodes instead of using GigaVUE-FM to deploy your fabric components.

The third-party orchestration feature allows you to deploy GigaVUE fabric components using your own Azure orchestration system. These fabric components register themselves with GigaVUE-FM using the information provided by the user. Once the nodes are registered with GigaVUE-FM, you can configure monitoring sessions and related services in GigaVUE-FM.

You can either manually deploy the fabric nodes using a configuration file, or you can use the Azure portal to launch the instances and deploy the fabric nodes using Custom data. Using the Custom data provided by you, the fabric nodes register themselves with the GigaVUE-FM. Based on the group name and the subgroup name details provided in the Custom data, GigaVUE-FM groups these fabric nodes under their respective monitoring domain and connection name. The health status of the registered nodes is determined by the heartbeat messages sent from the respective nodes.

You can also upload custom certificates to GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controller using your own cloud platform when deploying the fabric components. Refer to [Install Custom Certificate](#) for more detailed information.

Refer to the following for more detailed information and step-by-step instructions on how to deploy GigaVUE Fabric Components using Azure:

- [Prerequisites](#)
- [Disable GigaVUE-FM Orchestration in Monitoring Domain](#)
- [Configure UCT-V Controller in Azure](#)
- [Configure UCT-V in Azure](#)
- [Configure GigaVUE V Series Node and GigaVUE V Series Proxy in Azure](#)
- [Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure](#)

## Prerequisites

GigaVUE V Series Node must have a minimum of two Networks Interfaces (NIC) attached to it, a management NIC and a data NIC with Accelerated Networking enabled.

When creating a virtual machine for GigaVUE V Series Node using CLI, Management NIC and Data NIC can be attached at the time of the virtual machine creation. However, if you are using Azure GUI to create the virtual machine for GigaVUE V Series Node, then the data NIC can only be attached after creating the virtual machine. Refer to the following topics for more detailed information on how to create GigaVUE V Series Node with Management and Data NIC Attached using CLI or Azure GUI:

- [Create GigaVUE V Series Node with Management and Data NIC Attached using CLI](#)
- [Create GigaVUE V Series Node with Management and Data NIC Attached using Azure GUI](#)

## Create GigaVUE V Series Node with Management and Data NIC Attached using CLI

Create management NIC:

```
az network nic create -g <resource group> --vnet-name <VNet Name> --subnet <Subnet name> -n <Mangement NIC Name>
```

Create data NIC with Accelerated Networking enabled:

```
az network nic create <resource group> --vnet-name <VNet> --subnet <Subnet> -n <Data NIC> --accelerated-networking true
```

Create GigaVUE V Series Node virtual machine using the above NICs:

```
az vm create --resource-group <Resource group> --size <Standard_D4s_v4/Standard_D8S_V4> --name <GigaVUE V Series Node> --admin-username gigamon --generate-ssh-keys --image gigamon-inc:gigamon-gigavue-cloud-suite:vseries-node:6.4 --plan-name vseries-node --plan-product gigamon-gigavue-cloud-suite --plan-publisher gigamon-inc --nics <Management NIC and Data NIC>
```

## Create GigaVUE V Series Node with Management and Data NIC Attached using Azure GUI

Enable Management NIC when creating the GigaVUE V Series Node virtual machine. Refer to [Create virtual machine](#) topic in Azure Documentation for more detailed information on how to create a virtual machine. Follow the steps given below to attach the data NIC:

1. Select the GigaVUE V Series Node virtual machine from the Resources Page.
2. Stop the Virtual Machine using the **Stop** button.
3. Navigate to **Setting > Networking** from the left navigation pane. The **Networking** page appears.
4. In the **Networking** page, click **Attach network interface**. Select an existing network interface for Data NIC and click **OK**.
5. To enable accelerated networking, refer to [Manage Accelerated Networking through the portal](#).
6. Start the Virtual Machine.

Keep in mind the following when deploying the fabric components using third party orchestration in integrated mode:

- Create Roles and Users in GigaVUE-FM. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information on how to create users and assign roles to the users.
- When configuring UCT-V Controller, select **UCT-V** as the Traffic Acquisition Method.
- When you select Customer Orchestrated Source as your Traffic Acquisition Method, UCT-V and UCT-V Controller registration are not applicable.

- When you deploy the fabric components using third party orchestration, you cannot delete the monitoring domain without unregistering the GigaVUE V Series Nodes or UCT-V Controllers.
- Deployment of UCT-V Controller, GigaVUE V Series Node, and GigaVUE V Series Proxy through a third-party orchestrator is supported only on Linux platform.
- Deployment of UCT-V through a third-party orchestrator is supported on Linux and Windows platforms. Refer to [Linux Agent Installation](#) and [Windows UCT-V Installation](#) for detailed information.

### Keep in mind the following when upgrading the GigaVUE-FM to 6.1.00 or higher version (when using third party orchestration to deploy fabric components):

When upgrading GigaVUE-FM to any version higher than 6.0.00 and if the GigaVUE V Series Nodes version deployed in that GigaVUE-FM are lower than or equal to 6.0.00, then for the seamless flow of traffic, GigaVUE-FM automatically creates **Users** and **Roles** in GigaVUE-FM with the required permission. The username would be **orchestration** and the password would be **orchestration123A!** for the user created in GigaVUE-FM. Ensure there is no existing user in GigaVUE-FM, with the username **orchestration**.

It is recommended to change the password in the Users page, once the upgrade is complete. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for detailed steps on how to change password in the user page.

## Disable GigaVUE-FM Orchestration in Monitoring Domain

To register fabric nodes under Azure monitoring domain:

1. Create a monitoring domain in GigaVUE-FM. Refer to [Create a Monitoring Domain](#) for detailed instructions.
2. In the **Monitoring Domain Configuration** page, select **No** for the **Use FM to Launch Fabric** field as you are going to configure the fabric components in Azure Orchestrator.

The screenshot shows the 'Azure > Monitoring Domain' configuration page. The title is 'Azure Monitoring Domain Configuration'. The page contains several configuration items:

- Use V Series 2:** Yes (checked)
- Configure HTTP Proxy:** No (unchecked)
- Monitoring Domain:** Enter a monitoring domain name (text input)
- Authentication Type:** Managed Identities (dropdown)
- Region Name:** Region Name... (dropdown)
- Traffic Acquisition Method:** UCT-V (dropdown)
- Virtual Networks:** Virtual Networks... (dropdown)
- Resource Groups:** Resource Groups... (dropdown)
- Traffic Acquisition Tunnel MTU:** 1450 (text input)
- Use FM to Launch Fabric:** No (unchecked)

3. After creating your monitoring domain, you can deploy your fabric components through Azure Portal.

In your Azure Portal, you can configure the following GigaVUE fabric components:

- [Configure UCT-V Controller in Azure](#)
- [Configure UCT-V in Azure](#)
- [Configure GigaVUE V Series Node and GigaVUE V Series Proxy in Azure](#)

Refer [Deploying GigaVUE Cloud Suite for Azure using Customer Orchestration](#) for more detailed information.

## Configure UCT-V Controller in Azure

You can configure more than one UCT-V Controller in a monitoring domain.

To register UCT-V Controller in Azure Portal, use any one of the following methods.

- [Register UCT-V Controller during Virtual Machine Launch](#)
- [Register UCT-V Controller after Virtual Machine Launch](#)

### **Register UCT-V Controller during Virtual Machine Launch**

In your Azure portal, to launch the UCT-V Controller init virtual machine and register UCT-V Controller using custom data, follow the steps given below:



- In the Virtual machines page of the Azure Portal, select **Create** then **Virtual machine**. Then **Create a Virtual Machine** Page appears. For detailed information, refer to [Create virtual machine](#) topic in Azure Documentation.

On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. Enter the monitoring domain name and the connection name of the monitoring domain created earlier as the groupName and the subGroupName in the Custom Data. The UCT-V Controller uses this custom data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM. You can also install custom certificates to GigaVUE V Series Node or Proxy, refer to the below table for details:

Field	User Data
User data without custom certificate	<pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf   owner: root:root   permissions: '0644'   content:       Registration:       groupName: &lt;Monitoring Domain Name&gt;       subGroupName: &lt;Connection Name&gt;       user: &lt;Username&gt;       password: &lt;Password&gt;       remoteIP: &lt;IP address of the GigaVUE-FM&gt;       remotePort: 443</pre>
User data with custom certificate	<pre>#cloud-config write_files: - path: /etc/cntlr-cert.conf   owner: root:root   permissions: "0644"   content:       -----BEGIN CERTIFICATE-----     &lt;certificate content&gt;     -----END CERTIFICATE----- - path: /etc/cntlr-key.conf   owner: root:root   permissions: "400"   content:       -----BEGIN PRIVATE KEY-----     &lt;private key content&gt;     -----END PRIVATE KEY----- - path: /etc/gigamon-cloud.conf   owner: root:root   permissions: '0644'   content:       Registration:       groupName: &lt;Monitoring Domain Name&gt;</pre>

Field	User Data
	<pre> subGroupName: &lt;Connection Name&gt; user: &lt;Username&gt; password: &lt;Password&gt; remoteIP: &lt;IP address of the GigaVUE-FM&gt; remotePort: 443 </pre>

**NOTE:** User and Password must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the Username and Password created in the **Add Users** Section.

The UCT-V Controller deployed in your Azure portal appears on the Monitoring Domain page of GigaVUE-FM.

Monitoring Domain	Connection	Fabric	Management IP	Fabric Version	Status
<input type="checkbox"/> MD1					
	pubtrngj-vpc				✔ Connected
		G-vTapController	34.219.250.141	1.7-304	✔ Ok
		Gigamon-VSeriesProxy-1	34.211.211.49	2.1.0	✔ Ok
		Gigamon-VSeriesNode-1	172.16.24.188	2.2.0	✔ Ok

## Register UCT-V Controller after Virtual Machine Launch

To register UCT-V Controller after launching a Virtual Machine using a configuration file, follow the steps given below:

1. Log in to the UCT-V Controller.
2. Create a local configuration file (`/etc/gigamon-cloud.conf`) and enter the following custom data.

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  user: <Username>
  password: <Password>
  remoteIP: <IP address of the GigaVUE-FM>
  remotePort: 443
```

**NOTE:** User and Password must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the UserName and Password created in the **Add Users** Section.

3. Restart the UCT-V Controller service.  
`$ sudo service uctv-cntl restart`

The deployed UCT-V Controller registers with the GigaVUE-FM. After successful registration, the UCT-V Controller sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the fabric node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the UCT-V Controller and if that fails as well then GigaVUE-FM unregisters the UCT-V Controller and it will be removed from GigaVUE-FM.

## Configure UCT-V in Azure

UCT-V should be registered via the registered UCT-V Controller and communicates through PORT 8891.

**NOTE:** Deployment of UCT-Vs through third-party orchestrator is supported on both Linux and Windows platforms. Refer to [Linux Agent Installation](#) and [Windows Agent Installation](#) for detailed information.

To register UCT-V in Azure Portal, use any one of the following methods.

- [Register UCT-V during Virtual Machine Launch](#)
- [Register UCT-V after Virtual Machine Launch](#)

### Register UCT-V during Virtual Machine Launch

**NOTE:** Registering UCT-V during Virtual Machine Launch is not applicable for Windows Agents. You can register your Windows Agents after launching the Virtual machine, using a configuration file.

In your Azure portal, to launch the UCT-V init virtual machine and register the UCT-V using custom data, follow the steps given below:

1. In the Virtual machines page of the Azure Portal, select **Create** then **Virtual machine**. Then **Create a Virtual Machine** Page appears. For detailed information, refer to [Create virtual machine](#) topic in Azure Documentation.
2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. The UCT-V uses this custom data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
write_files:
- path: /etc/gigamon-cloud.conf
  owner: root:root
  permissions: '0644'
  content: |
    Registration:
      groupName: <Monitoring Domain Name>
      subGroupName: <Connection Name>
      user: <Username>
      password: <Password>
      remoteIP: <IP address of the UCT-V Controller 1, <IP address of the UCT-V Controller
2>
      remotePort: 8891
```

**NOTE:** User and Password must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the UserName and Password created in the **Add Users** Section.

### Register UCT-V after Virtual Machine Launch

**NOTE:** You can configure more than one UCT-V Controller for a UCT-V, so that if one UCT-V Controller goes down, the UCT-V registration will happen through another Controller that is active.

To register UCT-V after launching a Virtual Machine using a configuration file, follow the steps given below:

1. Install the UCT-V in the Linux or Windows platform. For detailed instructions, refer to [Linux UCT-V Installation](#) and [Windows UCT-V Installation](#).
2. Log in to the UCT-V. Refer to [Default Login Credentials](#) for UCT-V Controller default login credentials.

3. Edit the local configuration file and enter the following custom data.



- **/etc/gigamon-cloud.conf** is the local configuration file in Linux platform.
- **C:\ProgramData\uctv\gigamon-cloud.conf** is the local configuration file in Windows platform.

Registration:

```

groupName: <Monitoring Domain Name>
subGroupName: <Connection Name>
user: <Username>
password: <Password>
remoteIP: <IP address of the UCT-V Controller 1>,
          <IP address of the UCT-V Controller 2>
remotePort: 8891

```

**NOTE:** User and Password must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the UserName and Password created in the **Add Users** Section.

4. Restart the UCT-V service.

- Linux platform:  
`$ sudo service uctv restart`
- Windows platform: Restart from the Task Manager.

The deployed UCT-V registers with the GigaVUE-FM through the UCT-V Controller. After successful registration, the UCT-V sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, UCT-V status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the UCT-V and if that fails as well then GigaVUE-FM unregisters the UCT-V and it will be removed from GigaVUE-FM.

## Configure GigaVUE V Series Node and GigaVUE V Series Proxy in Azure



- It is not mandatory to register GigaVUE V Series Nodes via GigaVUE V Series however, if there is a large number of nodes connected to GigaVUE-FM or if the user does not wish to reveal the IP addresses of the nodes, then you can register your nodes using GigaVUE V Series Proxy. In this case, GigaVUE-FM communicates with GigaVUE V Series Proxy to manage the GigaVUE V Series Nodes.
- When deploying GigaVUE V Series Node using GigaVUE V Series Proxy, deploy the GigaVUE V Series Proxy first and provide the IP address of the proxy as the Remote IP of the GigaVUE V Series Node.

To register GigaVUE V Series Node and GigaVUE V Series Proxy in Azure Portal, use any one of the following methods.

- [Register GigaVUE V Series Node and GigaVUE V Series Proxy during Virtual Machine Launch](#)
- [Register GigaVUE V Series Node and GigaVUE V Series Proxy after Virtual Machine Launch](#)

### **Register GigaVUE V Series Node and GigaVUE V Series Proxy during Virtual Machine Launch**

To register GigaVUE V Series Node and GigaVUE V Series Proxy using the custom data in Azure Portal, follow the steps given below:

1. In the Virtual machines page of the Azure Portal, select **Create** then **Virtual machine**. Then **Create a Virtual Machine** Page appears. For detailed information, refer to [Create virtual machine](#) topic in Azure Documentation.

2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. Enter the monitoring domain name and the connection name of the monitoring domain created earlier as the groupName and the subGroupName in the Custom Data. The GigaVUE V Series Node and GigaVUE V Series Proxy uses this custom data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM. You can also install custom certificates to GigaVUE V Series Node or Proxy, refer to the below table for details:

Field	User Data
User data without custom certificate	<pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf   owner: root:root   permissions: '0644'   content:       Registration:       groupName: &lt;Monitoring Domain Name&gt;       subGroupName: &lt;Connection Name&gt;       user: &lt;Username&gt;       password: &lt;Password&gt;       remoteIP: &lt;IP address of the GigaVUE-FM&gt; or &lt;IP address of the Proxy&gt;       remotePort: 443</pre>
User data with custom certificate	<pre>#cloud-config write_files: - path: /etc/cntlr-cert.conf   owner: root:root   permissions: "0644"   content:       -----BEGIN CERTIFICATE-----     &lt;certificate content&gt;     -----END CERTIFICATE----- - path: /etc/cntlr-key.conf   owner: root:root   permissions: "400"   content:       -----BEGIN PRIVATE KEY-----     &lt;private key content&gt;     -----END PRIVATE KEY----- - path: /etc/gigamon-cloud.conf   owner: root:root   permissions: '0644'   content:       Registration:       groupName: &lt;Monitoring Domain Name&gt;       subGroupName: &lt;Connection Name&gt;       user: &lt;Username&gt;       password: &lt;Password&gt;       remoteIP: &lt;IP address of the GigaVUE-FM&gt; or &lt;IP address of the Proxy&gt;       remotePort: 443</pre>



- You can register your GigaVUE V Series Node directly with GigaVUE-FM or you can use GigaVUE V Series Proxy to register your GigaVUE V Series Node with GigaVUE-FM. If you wish to register GigaVUE V Series Node directly, enter the `remotePort` value as 443 and the `remoteIP` as <IP address of the GigaVUE-FM> or if you wish to deploy GigaVUE V Series Node using GigaVUE V Series Proxy then, enter the `remotePort` value as 8891 and `remoteIP` as <IP address of the Proxy>.
- User and Password must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the Username and Password created in the **Add Users** Section.

## Register GigaVUE V Series Node and GigaVUE V Series Proxy after Virtual Machine Launch

To register GigaVUE V Series Proxy after launching the virtual machine using a configuration file, follow the steps given below:

1. Log in to the GigaVUE V Series Node or Proxy. Refer to [Default Login Credentials](#) for UCT-V Controller default login credentials.
2. Create a local configuration file (`/etc/gigamon-cloud.conf`) and enter the following custom data.

### Registration:

```
groupName: <Monitoring Domain Name>
subGroupName: <Connection Name>
user: <Username>
password: <Password>
remoteIP: <IP address of the GigaVUE-FM> or <IP address of the Proxy>
remotePort: 443
```



- You can register your GigaVUE V Series Node directly with GigaVUE-FM or you can use V Series proxy to register your GigaVUE V Series with GigaVUE-FM. If you wish to register GigaVUE V Series Node directly, enter the `remotePort` value as 443 and the `remoteIP` as <IP address of the GigaVUE-FM> or if you wish to deploy GigaVUE V Series Node using GigaVUE V Series Proxy then, enter the `remotePort` value as 8891 and `remoteIP` as <IP address of the Proxy>.
- User and Password must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the Username and Password created in the **Add Users** Section.



3. Restart the GigaVUE V Series Proxy service.
  - GigaVUE V Series Node:  
`$ sudo service vseries-node restart`
  - GigaVUE V Series Proxy:  
`$ sudo service vps restart`

The deployed GigaVUE V Series Node or Proxy registers with the GigaVUE-FM. After successful registration, the GigaVUE V Series Node or Proxy sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the fabric node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the GigaVUE V Series Node or Proxy and if that fails as well then GigaVUE-FM unregisters the GigaVUE V Series Node or Proxy and it will be removed from GigaVUE-FM.

If you are using Azure GUI to create the virtual machine for GigaVUE V Series Node then data NIC must be attached to GigaVUE V Series Node after creating the virtual machine. Refer to [Create GigaVUE V Series Node with Management and Data NIC Attached using Azure GUI](#) for more detailed information.

## Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure

This chapter describes how to upgrade GigaVUE V Series Proxy and GigaVUE V Series Node. For more detailed information about UCT-V Controller, GigaVUE V Series Proxy and Node Version refer [GigaVUE-FM Version Compatibility Matrix](#).

Refer to the following topic for more information:

- [Prerequisite](#)
- [Upgrade UCT-V Controller](#)
- [Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy](#)

### Prerequisite

Before you upgrade the GigaVUE V Series Proxy and GigaVUE V Series Node, you must upgrade GigaVUE-FM to software version 5.13.01 or above.

### Upgrade UCT-V Controller

**NOTE:** UCT-V Controllers cannot be upgraded. Only a new version that is compatible with the UCT-V's version can be added or removed in the **Azure Fabric Launch Configuration** page.

To change the UCT-V Controller version follow the steps given below:

## To change UCT-V Controller version between different major versions

**NOTE:** You can only add UCT-V Controllers which has different major versions. For example, you can only add UCT-V Controller version 1.8-x if your existing version is 1.7-X.

- In the **Azure Fabric Launch Configuration** page, under **Controller Versions**, click **Add**.
- From the **Image** drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances.
- From the **Size** drop-down list, select a size for the UCT-V Controller. The default size is Standard\_B1s.
- In **Number of Instances**, specify the number of UCT-V Controllers to launch. The minimum number you can specify is 1.

The screenshot shows the 'Controller Version(s)' configuration area. It features an 'Add' button at the top. Below it, there are three main configuration blocks:

- Image Configuration:** Includes a dropdown for 'Image' (currently 'Select image...'), a dropdown for 'Size' (currently 'Standard\_B1s'), and a text input for 'Number of Instances' (currently '1').
- Management Subnet:** Includes radio buttons for 'IP Address Type' (Private and Public, with Public selected) and a dropdown for 'Subnet' (currently 'mgmt').
- Additional Subnets:** Includes an 'Add Subnet' button and a 'Subnet 1' dropdown (currently 'traffic1').

At the bottom, there is a 'Tags' section with an 'Add' button.

You cannot change the IP Address Type and the Additional Subnets details, provided at the time of UCT-V Controller configuration.

After installing the new version of UCT-V Controller, follow the steps given below:

1. Install UCT-V with the version same as the UCT-V Controller.
2. Delete the UCT-V Controller with older version.

## To change UCT-V Controller version with in the same major version:

**NOTE:** This is only applicable, if you wish to change your UCT-V Controller version from one minor version to another with in the same major version. For example, from 1.8-2 to 1.8-3.

- From the **Image** drop-down list, select a UCT-V Controller image with in the same major version.
- Specify the **Number of Instances**. The minimum number you can specify is 1.

- c. Select the **Subnet** from the drop-down.



- You cannot modify the rest of the fields.
- After installing the new version of UCT-V Controller, install the UCT-V with the same version.

## Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy

GigaVUE-FM lets you upgrade GigaVUE V Series Proxy and GigaVUE V Series Node at a time.

There are multiple ways to upgrade the GigaVUE V Series Proxy and Node. You can:

- Launch and replace the complete set of nodes and proxys at a time.

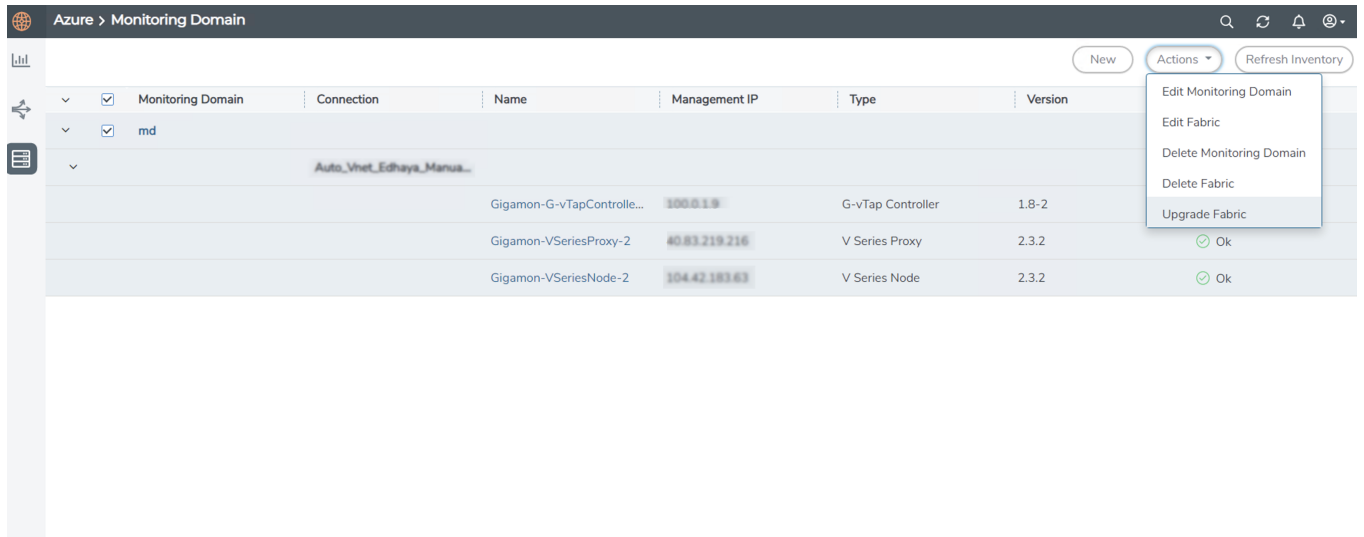
For example, if you have 1 GigaVUE V Series Proxy and 10 GigaVUE V Series Nodes in your VNet, you can upgrade all of them at once. First, the new version of GigaVUE V Series controller is launched. Next, the new version of GigaVUE V Series nodes are launched. Then, the old version of V Series controller and nodes are deleted from the VNet.

### NOTES:

- When the new version of node and proxy is launched, the old version still exists in the VNet until they are deleted. Make sure the instance type determined during the configuration can accommodate the total number of new and old instances present in the VNet. If the instance type cannot support so many instances, you can choose to upgrade in multiple batches.
- If there is an error while upgrading the complete set of proxys and nodes present in the VNet, the new version of the fabric is immediately deleted and the old version of the fabric is retained as before.
- If you have deployed your nodes using Public IP address while creating the monitoring domain, then select the same number of Public IP addresses defined in your Max Instances when upgrading your nodes. Refer to [Create Monitoring Domain](#) for more detailed information.
- Launch and replace the nodes and proxy in multiple batches.  
For example, if there are 18 GigaVUE V Series Nodes to be upgraded, you can specify how many you want to upgrade per batch.

To upgrade the GigaVUE V Series Proxy and GigaVUE V Series Node:

1. Go to **Inventory > VIRTUAL > Azure**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. On the Monitoring Domain page, select the connection name check box and click **Actions**



3. Select **Upgrade Fabric** from the drop-down list. The Fabric Nodes Upgrade page is displayed.

### Fabric Nodes Upgrade

#### V Series Proxy

Upgrade	<input checked="" type="checkbox"/>
Current Version	2.3.0
Image	gigamon-gigavue-vseries-proxy-2.3.2-284364
Change Size	<input type="checkbox"/>
Batch Size	1

#### V Series Node

Upgrade	<input checked="" type="checkbox"/>
Current Version	2.3.0
Image	gigamon-gigavue-vseries-node-2.3.2-284421
Change Size	<input type="checkbox"/>
Batch Size	1
Public IPs	104.42.183.63 104.42.183.63 x

Upgrade Cancel

4. To upgrade the GigaVUE V Series Node/Proxy, select the **Upgrade** checkbox.
5. From the **Image** drop-down list, select the latest version of the GigaVUE V Series Proxy/Nodes.
6. Select the **Change Size** checkbox to change the flavor of the node/proxy, only if required.
7. To upgrade the GigaVUE V Series Node/Proxy, specify the batch size in the **Batch Size** box.

For example, if there are 7 GigaVUE V Series Nodes, you can specify 7 as the batch size and upgrade all of them at once. Alternatively, you can specify 3 as the batch size, and launch and replace 3 V Series nodes in each batch. In the last batch, the remaining 1 V Series node is launched.

8. From the Public IPs drop-down list, select the IP addresses equal to the Max Instances defined when creating a monitoring domain.

**NOTE:** This is only applicable for nodes deployed using Public IP, when creating a monitoring domain.

9. Click **Upgrade**.

The upgrade process takes a while depending on the number of GigaVUE V Series Proxies and Nodes upgrading in your Azure environment. First, the new version of the GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes is launched. Then, the older version of both is deleted from the project. The monitoring session is deployed automatically.

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

**Fabric Nodes Upgrade Status**

---

**Monitoring Domain:** md

**Start Time** 2021-10-11 20:58:56

**End Time** 2021-10-11 21:04:03

**Status** Fabric upgrade completed successfully

---

	Proxies	Nodes
<b>Total</b>	1	1
<b>Upgraded</b>	1	1
<b>Upgrading</b>	0	0
<b>Remaining</b>	0	0
<b>Failures</b>	0	0

---

[Clear](#) [Close](#)

- Click **Clear** to delete the monitoring domain upgrade status history of successfully upgraded nodes.

# Configure Monitoring Session

This chapter describes how to setup ingress and egress tunnel, maps, applications in a monitoring session to receive and send traffic to the GigaVUE Cloud Suite V Series node. It also describes how to filter, manipulate, and send the traffic from the V Series node to monitoring tools.

Refer to the following sections for details:

- [Create a Monitoring Session](#)
- [Interface Mapping](#)
- [Create Ingress and Egress Tunnels](#)
- [Create Raw Endpoint](#)
- [Create a New Map](#)
- [Add Applications to Monitoring Session](#)
- [Deploy Monitoring Session](#)
- [View Monitoring Session Statistics](#)
- [View Health Status on the Monitoring Session Page](#)
- [Visualize the Network Topology](#)

## Create a Monitoring Session

You must create a monitoring domain before creating a monitoring session. Refer to [Create Monitoring Domain](#) for more detailed information on how to create a monitoring domain.

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. You can filter the traffic and, use a suite of GigaSMART applications as well.

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

You can create multiple monitoring sessions per monitoring domain.

To create a new monitoring session:

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

### Create A New Monitoring Session

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

Field	Description
<b>Alias</b>	The name of the monitoring session.
<b>Monitoring Domain</b>	The name of the monitoring domain that you want to select.
<b>Connection</b>	The connection(s) that are to be included as part of the monitoring domain. You can select the required connections that need to be part of the monitoring domain.

4. Click **Create**. The **Edit Monitoring Session** Canvas page appears.

The Monitoring Session page **Actions** button also has the following options:

Button	Description
<b>Edit</b>	Opens the Edit page for the selected monitoring session.  <b>NOTE:</b> In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again.
<b>Delete</b>	Deletes the selected monitoring session.
<b>Clone</b>	Duplicates the selected monitoring session.
<b>Deploy</b>	Deploys the selected monitoring session.



Button	Description
<b>Undeploy</b>	Undeploys the selected monitoring session.
<b>Apply Threshold</b>	You can use this button to apply the threshold template created for monitoring cloud traffic health. Refer to <a href="#">Monitor Cloud Health</a> for more detailed information on cloud traffic health, how to create threshold templates, and how to apply threshold templates.
<b>Apply Policy</b>	You can use this button to enable precryption, prefiltering, or Secure Tunnel. Refer to <a href="#">Enable Prefiltering, Precryption, and Secure Tunnel</a> for more details.

## Edit Monitoring Session

In the edit monitoring session canvas page, you can add and configure applications, tunnel endpoints, raw endpoints, and maps.

Refer to the following topics for detailed information:

- [Create Ingress and Egress Tunnels](#)
- [Add Applications to Monitoring Session](#)
- [Create Raw Endpoint](#)
- [Create a New Map](#)

The **Edit Monitoring Session** page has the following buttons:

Button	Description
<b>Options</b>	You can enable or disable Prefiltering, Precryption, and Secure Tunnel here. You can also create prefiltering template and apply it to the monitoring session. Refer to <a href="#">Enable Prefiltering, Precryption, and Secure Tunnel</a> for more detailed information.
<b>Show Targets</b>	Use to refresh the subnets and monitored instances details that appear in the <b>Instances</b> dialog box.
<b>Interface mapping</b>	Use to change the interfaces mapped to an individual GigaVUE V Series Node. Refer to <a href="#">Interface Mapping</a> topic for more details.
<b>Deploy</b>	Deploys the selected monitoring session. Refer to <a href="#">Deploy Monitoring Session</a> topic for more details.

## Enable Prefiltering, Precryption, and Secure Tunnel

Prefiltering, Precryption, and Secure tunnel can be enabled for the monitoring session from the Edit Monitoring Session canvas page.

### Enable Prefiltering

To enable Prefiltering, follow the steps given below:

1. In the Edit Monitoring Session page, click **Options**. The **Monitoring Session Options** page appears.
2. Enable the **Mirroring** toggle button. Then, enable the **Prefiltering** toggle button.
3. You can select an existing Prefiltering template from the **Template** drop-down menu, or you can create a new template and apply it. Refer to [Prefiltering](#) for more details on how to create a new template.
4. Click Save to apply the template to the monitoring session.

You can save the newly created template by using the **Save as Template** button.

### Enable Precryption

To enable Precryption, follow the steps given below:

1. In the Edit Monitoring Session page, click **Options**. The **Monitoring Session Options** page appears.
2. Enable the **Precryption** toggle button. Refer to topic for more details on precryption.

### Enable Secure Tunnel

To enable Secure Tunnel, follow these steps:

1. In the Edit Monitoring Session page, click **Options**. The **Monitoring Session Options** page appears.
2. Enable the **Secure Tunnel** button. You can enable secure tunnel for both mirrored and precrypted traffic. For more information about Secure Tunnel, refer to

## Prefiltering

Prefiltering allows you to filter the traffic at UCT-Vs before sending it to the GigaVUE V Series Nodes. For prefiltering the traffic, GigaVUE-FM allows you to create a prefiltering policy template, and the policy template can be applied to a monitoring session.

You can define a policy template with rules and filter values. A policy template once created can be applied to multiple monitoring sessions. However, a monitoring session can use only one template.

Each monitoring session can have a maximum of 16 rules.

You can also edit a specific policy template with required rules and filter values for a particular monitoring session while editing a monitoring session. However, the customized changes are not saved in the template.

Some of the points that must be remembered for prefiltering in Next Generation UCT-Vs are:

- Prefiltering is supported only in Next Generation UCT-Vs. It is not supported for classic mirroring mechanism.
- Prefiltering is supported for both Linux and Windows UCT-Vs.
- For a single monitoring session, only one prefiltering policy can be applied. All the agents in that monitoring session are configured with respective prefiltering policy.
- For multiple monitoring sessions, if the same agent is selected by two or more monitoring sessions, then prefiltering policy cannot be applied. It is default to PassAll.

### Create Prefiltering Policy Template

GigaVUE-FM allows you to create a prefiltering policy template with a single rule or multiple rules. You can configure a rule with a single filter or multiple filters. Each monitoring session can have a maximum of 16 rules.

To create a prefiltering policy template, do the following steps:

1. Go to **Resources > Prefiltering**, and then click **UCT-V**.
2. Click **New**.
3. Enter the name of the template in the **Template Name** field.
4. Enter the name of a rule in the **Rule Name** field.
5. Click any one of the following options:
  - Pass — Passes the traffic.
  - Drop — Drops the traffic.
6. Click any one of the following options as per the requirement:
  - Bi-Directional — Allows the traffic in both directions of the flow. A single Bi-direction rule should consist of 1 Ingress and 1 Egress rule.
  - Ingress — Filters the traffic that flows in.
  - Egress — Filters the traffic that flows out.

7. Select the value of the priority based on which the rules must be prioritized for filtering. Select the value as 1 to pass or drop a rule in top priority. Similarly, you can select the value as 2, 3, 4 to 8, where 8 can be used for setting a rule with the least priority. Drop rules are added based on the priority and, then pass rules are added.

8. Select the **Filter Type** from the following options:

- L3
- L4

9. Select the **Filter Name** from the following options:

- ip4Src
- ip4Dst
- ip6Src
- ip6Dst
- Proto - It is common for both ipv4 and ipv6.

10. Select the **Filter Relation** from any one of the following options:

- Not Equal to
- Equal to

11. Enter the value for the given filter.

12. Click **Save**.

**NOTE:** Click + to add more rules or filters. Click - to remove a rule or a filter.

## Interface Mapping

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

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Select a Monitoring session from the list view and click **Actions > Edit**. The Edit Monitoring session page appears.
3. In the Edit Monitoring session canvas page, click on the **Interface Mapping** button.
4. The **Select nodes to deploy the Monitoring Session dialog box** appears. Select the GigaVUE V Series Nodes for which you wish to map the interface.

5. After selecting the GigaVUE V Series Node, select the interfaces for each of the REPs and the TEPs deployed in the monitoring session from the drop-down menu for the selected individual GigaVUE V Series Nodes. Then, click **Deploy**.

## Create Ingress and Egress Tunnels

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 VXLAN and TLS-PCAPNG tunnel.

To create a new tunnel endpoint:

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

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

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

Field	Description	
<b>Alias</b>	The name of the tunnel endpoint. <b>NOTE:</b> Do not enter spaces in the alias name.	
<b>Description</b>	The description of the tunnel endpoint.	
<b>Type</b>	VXLAN and TLS-PCAPNG are the only supported tunnel types for Azure.	
<b>Traffic Direction</b>		
The direction of the traffic flowing through the GigaVUE V Series Node.		
<b>In</b>	Choose <b>In</b> (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node.	
	<b>IP Version</b>	The version of the Internet Protocol. Select IPv4 or IPv6.
	<b>Remote Tunnel IP</b>	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	<b>VXLAN Network Identifier</b>	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	<b>Source L4 Port</b>	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.
	<b>Destination L4 Port</b>	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.
<b>Out</b>	Choose <b>Out</b> (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint.	
	<b>Remote Tunnel IP</b>	For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	<b>MTU</b>	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	<b>Time to Live</b>	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.
	<b>DSCP</b>	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.

Field	Description	
	<b>Flow Label</b>	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575
	<b>VXLAN Network Identifier</b>	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	<b>Source L4 Port</b>	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.
	<b>Destination L4 Port</b>	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.
<b>TLS-PCAPNG</b>		
<b>Traffic Direction</b>		
The direction of the traffic flowing through the GigaVUE V Series Node.		
<b>In</b>	<b>IP Version</b>	The version of the Internet Protocol. only IPv4 is supported.
	<b>Remote Tunnel IP</b>	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	<b>MTU</b>	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	<b>Source L4 Port</b>	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.
	<b>Destination L4 Port</b>	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.
	<b>Key Alias</b>	Select the Key Alias from the drop-down.
	<b>Cipher</b>	Only SHA 256 is supported.
	<b>TLS Version</b>	Only TLS Version1.3.
	<b>Selective Acknowledgments</b>	Enable to receive the acknowledgments.
	<b>Sync Retries</b>	Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6.
	<b>Delay</b>	Enable to receive the acknowledgments when there is a



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

4. Click **Save**.

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

To apply threshold template to Tunnel End Points, select the required tunnel end point on the canvas and click **Details**. The quick view appears, click on the Threshold tab. For more details on how to create or apply threshold template, refer to [Monitor Cloud Health](#).

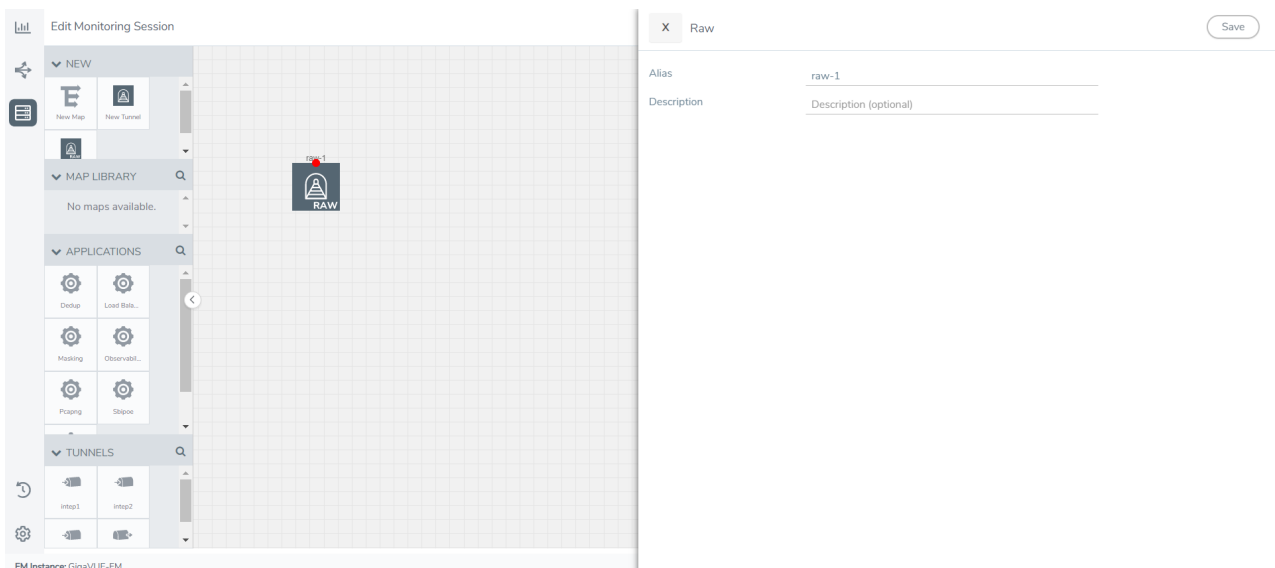
After configuring the tunnels and deploying the monitoring session, you can view the names of egress tunnels configured for a monitoring session, on the Monitoring Session details page. The Egress Tunnel column displays the name of the egress tunnel configured for a particular monitoring session. When multiple egress tunnels are configured for a monitoring session, then the Egress Tunnel column displays the number of egress tunnels configured in that monitoring session. Hover over the number of egress tunnels to display the names of the egress tunnels used in that particular monitoring session.

## Create Raw Endpoint

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** from **NEW** to the graphical workspace.
2. Click the **New RAW** icon and select **Details**. The **RAW** quick view page appears.
3. Enter the alias and description. In the **Alias** field, enter a name for the Raw End Point and click **Save**.



4. To deploy the monitoring session after adding the Raw Endpoint click the **Deploy** button on the edit monitoring session page.
5. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the V Series Nodes for which you wish to deploy the monitoring session.

- After selecting the 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 V Series Nodes. Then, click **Deploy**.

## Create a New Map

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

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

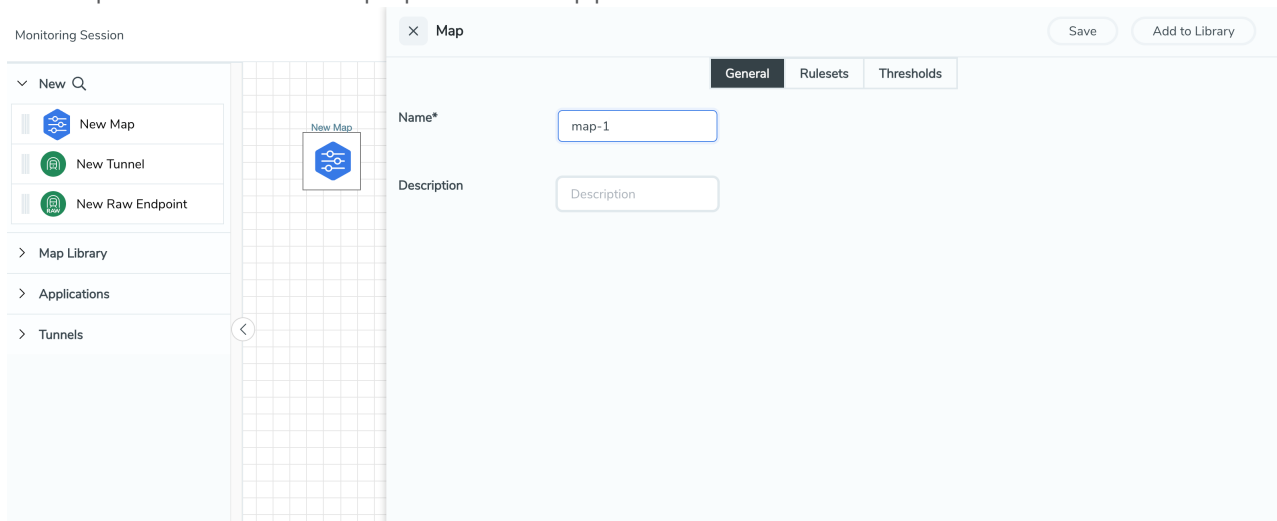
Keep in mind the following when creating a map:

Parameter	Description
<b>Rules</b>	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.
<b>Priority</b>	A priority determines the order in which the rules are executed. The priority value can range from 1 to 5, with 1 being the highest and 5 is the lowest priority.
<b>Pass</b>	The traffic from the virtual machine will be passed to the destination.
<b>Drop</b>	The traffic from the virtual machine is dropped when passing through the map.
<b>Traffic Filter Maps</b>	A set of maps that are used to match traffic and perform various actions on the matched traffic.
<b>Inclusion Map</b>	An inclusion map determines the instances to be included for monitoring. This map is used only for target selection.

<b>Exclusion Map</b>	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
<b>Automatic Target Selection (ATS)</b>	<p>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.</p> <p>The below formula describes how ATS works:</p> <p><b>Selected Targets = Traffic Filter Maps <math>\cap</math> Inclusion Maps - Exclusion Maps</b></p> <p>Below are the filter rule types that work in ATS:</p> <ul style="list-style-type: none"> <li>● mac Source</li> <li>● mac Destination</li> <li>● ipv4 Source</li> <li>● ipv4 Destination</li> <li>● ipv6 Source</li> <li>● ipv6 Destination</li> <li>● VM Name Destination</li> <li>● VM Name Source</li> <li>● VM Tag Destination - Not applicable to Nutanix.</li> <li>● VM Tag Source - Not applicable to Nutanix.</li> <li>● VM Category Source - Applicable only to Nutanix</li> <li>● VM Category Destination - Applicable only to Nutanix.</li> <li>● Host Name -Applicable only to Nutanix and VMware.</li> </ul> <p>The traffic direction is as follow:</p> <ul style="list-style-type: none"> <li>● For any rule type as Source - the traffic direction is egress.</li> <li>● For Destination rule type - the traffic direction is ingress.</li> <li>● For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> 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.</p> </div>
<b>Group</b>	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

To create a new map:


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



3. On the New Map quick view, click on **General** tab and enter the required information as described in the following table:

Field	Description
<b>Name</b>	Name of the new map
<b>Description</b>	Description of the map

- Pass and Drop rule selection with Automatic Target Selection (ATS) differ with the Map type as follows:
  - Traffic Map—Only Pass rules for ATS
  - Inclusion Map—Only Pass rules for ATS
  - Exclusion Map—Only Drop rules for ATS

4. Click on **Rule Sets** tab. Through the map, packets can be dropped or passed based on the highest to lowest rule priority. You can add 5 rule sets on a map. 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.
  - a. **To create a new rule set:**
    - i. Click **Actions > New Rule Set**.
    - 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.
5. To reuse the map, click **Add to Library**. Save the map using one of the following ways:
  - a. Select an existing group from the **Select Group** list or create a **New Group** with a name.
  - b. Enter a description in the **Description** field, and click **Save**.
6. Click **Save**.

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



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

To apply threshold template to maps, select the required map on the canvas and click **Details**. The quick view appears, click on the Threshold tab. For more details on how to create or apply threshold templates, refer to [Monitor Cloud Health](#).

### Rules and Notes:

- Directional rules do not work on single NIC VMs that are running a Windows UCT-V.

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

- Click a map and select **Details** to edit the map
- Click a map and select **Delete** to delete the map.
- Click the **Show Targets** button to refresh the subnets and monitored instances details that appear in the **Instances** dialog box.
- Click  to expand the **Targets** dialog box. To view details about a GigaVUE V Series Node, click the arrow next to the VM.
- In the Instances window, click  to filter the list of instances.

## 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 **Rule sets** 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 **Rule Sets**, 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 **Rule Sets** 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.

## Add Applications to Monitoring Session

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

- Slicing
- Masking
- De-duplication
- Load Balancing
- PCAPng Application
- Header Stripping
- Application Metadata Exporter
- SSL Decrypt

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

You can also configure the following GigaSMART operations from the **Traffic > Solutions > Application Intelligence**:

- Application Metadata Intelligence
- Application Filtering Intelligence

For more information, refer to these GigaSMART Operations in the *GigaVUE Fabric Management Guide*.

## Deploy Monitoring Session

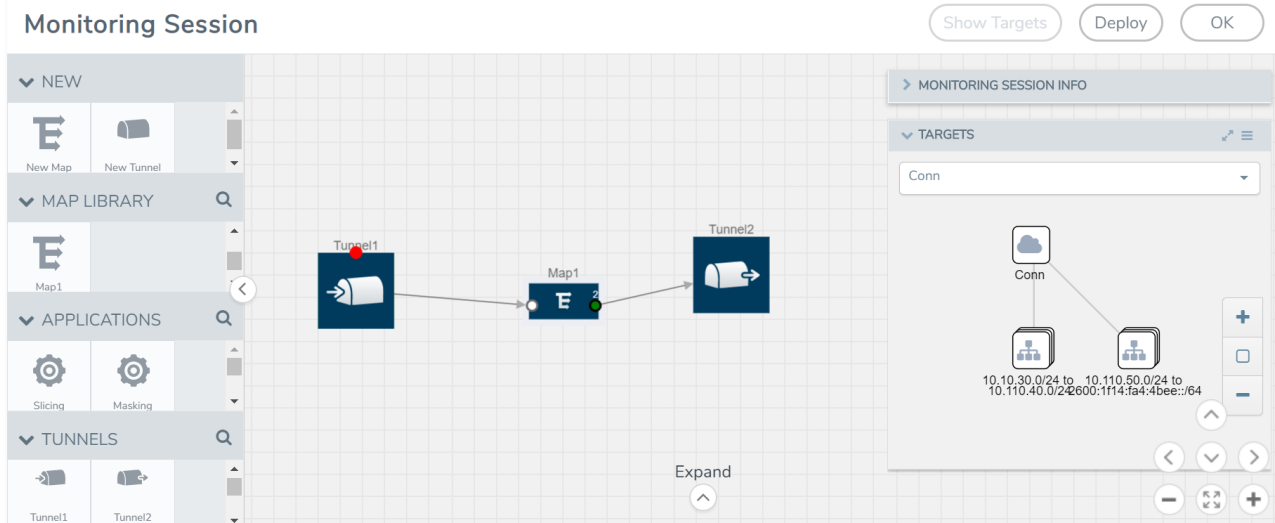
To deploy the monitoring session:

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



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

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



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

The Monitoring Session page also has the following options under the **Actions** button:

Button	Description
<b>Undeploy</b>	Undeploys the selected monitoring session.
<b>Clone</b>	Duplicates the selected monitoring session.
<b>Edit</b>	Opens the Edit page for the selected monitoring session. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> In case of an error while editing a monitoring session, undeploy and deploy the monitoring session</p> </div>

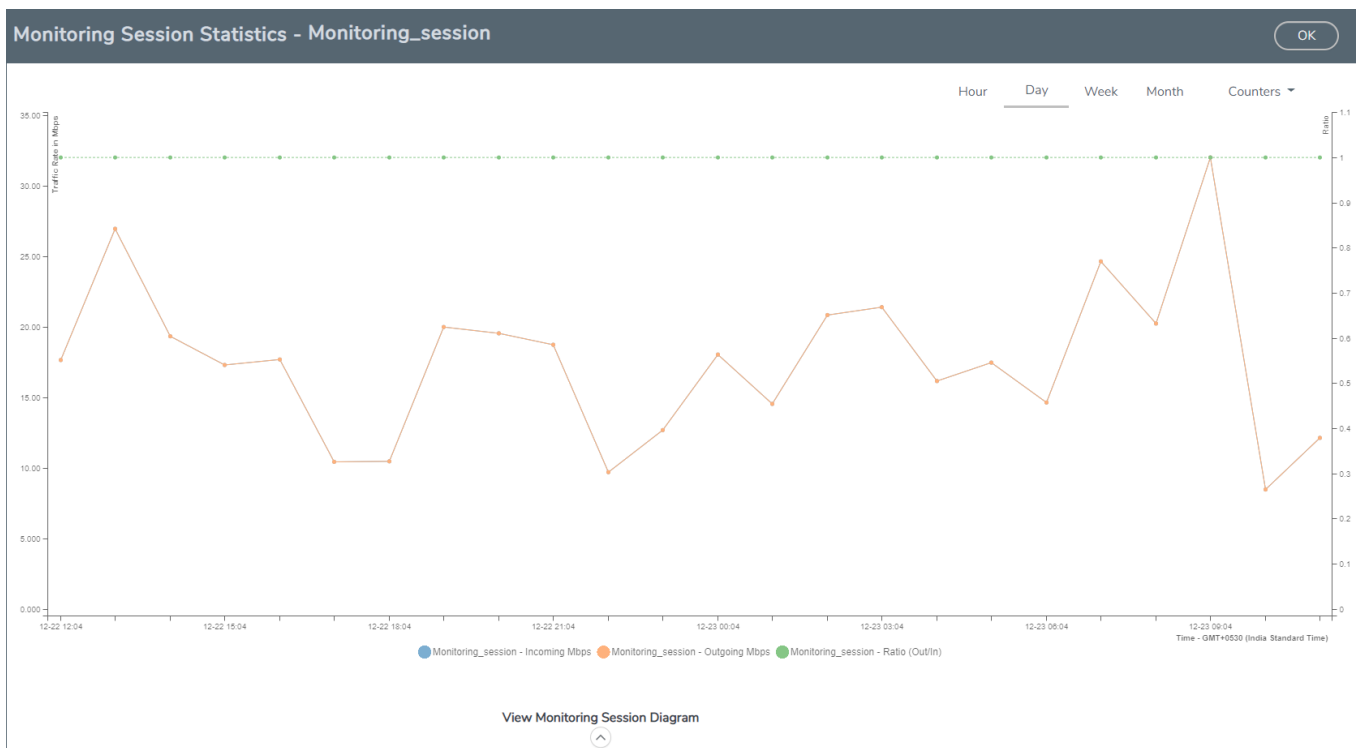
Button	Description
	again..
Delete	Deletes the selected monitoring session.

## View Monitoring Session Statistics

The Monitoring Session Statistics page lets you analyze the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. The traffic can be viewed based on kilobits/second, megabits/second or gigabits/second.

On the Monitoring Sessions page, click **View** in the Statistics column to view the Monitoring Session Statistics page. The **Monitoring Session Statistics** page appears where you can analyze incoming and outgoing traffic.

**NOTE:** If there are multiple monitoring sessions with different target selection, then the incoming maps will not show true statistics and it shows the aggregate traffic from all the targets.



You can also perform the following actions on the Monitoring Session Statistics page:

- Directly below the graph, you can click on **IncomingMbps**, **Outgoing Mbps**, or **Ratio (Out/In) (Mbps)** to view the statistics individually.
- At the bottom of the Monitoring Session Statistics page, you can click on **View Monitoring Session Diagram**. The Monitoring Session Diagram quick view appears.
- On the **Monitoring Session Diagram** page, you can expand any map, or tunnel to open a **Details** quick view of that item to see more details about the incoming and outgoing traffic for that item.
- You can also scroll down the Map **Details** quick view to view the Map Rules, Action Sets, and Map Info for this map. You can select Map Rules or Action Sets to view the traffic matching the selected rule on the graph in the quick view.
- You can also view the statistics of the monitoring session deployed in the individual V Series Nodes. To view the statistics of the individual V Series Node, select the name of the V Series Node for which you want to view the statistics from the V Series Node drop-down menu on the top left-corner of the Monitoring Session Statistics page.
- Hover over the V Series Node drop-down to view the number of the applications, end points, and other application environments configured for a particular V Series Node. It also displays the error message related to configuration for the particular V Series Node.

## View Health Status on the Monitoring Session Page

You can view the health status of the monitoring session and the components deployed, in the monitoring session page. Refer to [Monitor Cloud Health](#) for more detailed information on how to configure cloud health and view health status.

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

### Health

This column displays the health status (both traffic and configuration) of the entire monitoring session. The status is marked healthy only if both the traffic and configuration health status is healthy, even if either of them is unhealthy then the health status is moved to unhealthy.

### V Series Node Health

This column displays the configuration and traffic health status of the monitoring session deployed in V Series Nodes. This column provides information on the number of GigaVUE V Series Nodes that have healthy traffic flow and monitoring session successfully deployed to the total number of V Series Nodes that have monitoring session deployed.

You can view the health status of the individual V Series Nodes by clicking on the V Series Node Health column.

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

## Target Source Health

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

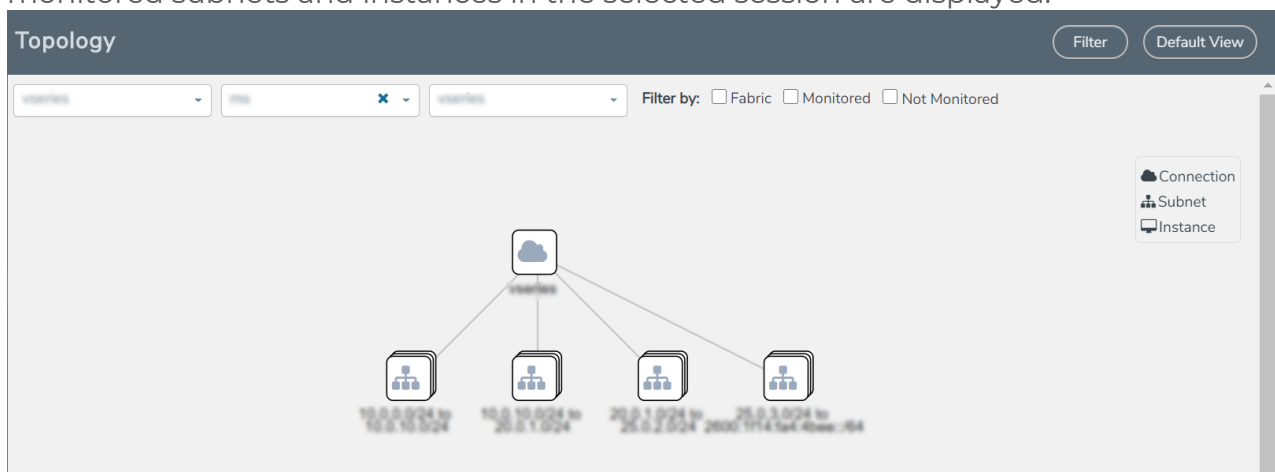
You can view the health status of the individual targets and also the error message associated with them, by clicking on the Target Source Health column.

## Visualize the Network Topology

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

To view the topology diagram in GigaVUE-FM:

1. On the Monitoring Session page, select **Topology** tab. The Topology page appears.
2. Select a monitoring domain from the **Select monitoring domain...** list.
3. Select a connection from the **Select monitoring session...**list.
4. Select a monitoring session from the **Select connection...** list. The topology view of the monitored subnets and instances in the selected session are displayed.



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

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

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

# Configure Application Intelligence Solutions on GigaVUE V Series Nodes for Azure

To configure the Application Intelligence solution on the GigaVUE V Series Nodes, create a virtual environment with the required connections. After creating the connections, configure the sources and the required destinations for the traffic flow. Refer the following topics for step by step instructions on how to configure Application Intelligence solution for GigaVUE V Series Nodes:

- [Configure Environment](#)
- [Create Credentials](#)
- [Connect to Azure](#)
- [Create Source Selectors](#)
- [Create Tunnel Specifications](#)
- [User Defined Application](#)
- [Configure Application Intelligence Session](#)
- [Slicing and Masking in Application Filtering Intelligence](#)
- [Application Metadata Intelligence](#)
- [Create NetFlow Session for Virtual Environment](#)



## Important Notes:

- You can deploy multiple GigaVUE V Series Nodes in a connection.
- When upgrading from any previous version to 6.4.00, you cannot enable secure tunnels. You will have to delete the Application Intelligence solution and deploy it again with secure tunnels.
- You cannot enable secure tunnels for an existing Application Intelligence Session, you must delete the Application Intelligence solution and deploy it again with secure tunnels.



- You can use tool templates while creating an Application Metadata Intelligence session. To create a custom tool template for GigaVUE V Series Node, signature is required from the node. Refer to the Tool Templates section in the *GigaVUE Fabric Management Guide* for more detailed information.
- Prior to configuring the Application Intelligence solution, refer to the [Before You Begin](#) topic for the minimum requirements.
- 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 [Configuration Settings](#) section in the *GigaVUE Administration Guide* for configuration details.
- To delete a GigaVUE V Series Node deployed in a Application Intelligence solution, you must delete the resources in the following order:
  1. Delete the Application Intelligence solution.
  2. Delete the GigaVUE V Series Node and Connection.
  3. Delete the Environment.

## Configure Environment

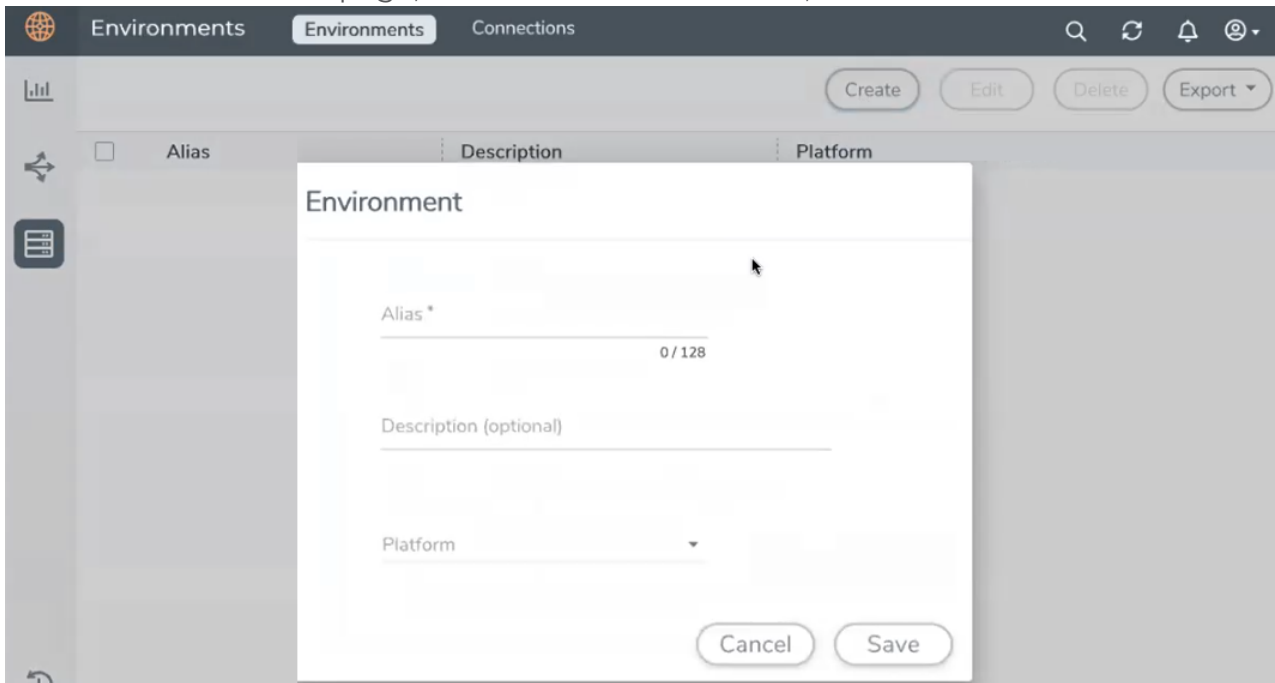
The Environments page allows you to create the following:

- **Environments:** The physical or the virtual environment in which the Application Intelligence solution is to be deployed.
- **Connections:** Connection between GigaVUE-FM and the cloud platform.

### Create Environment

To configure the Environment:

1. Select **Inventory > Resources > Environments**.
2. On the **Environments** page, on the **Environments** tab, click **Create**.



3. Select or enter the following details:

Field	Description
<b>Alias</b>	Alias name used to identify the Environment.
<b>Description</b>	Brief description about the Environment.
<b>Platform</b>	Select the cloud platform.

4. Click **Save**. The environment is added to the list view.

Use the following buttons to manage your environment:

Button	Description
Delete	Use to delete an Environment.
Edit	Use to edit the details in an Environment.
Export	Export the details from the Environment page in an XLS or CSV file.

## Create Credentials

You must configure your Azure Credentials for configuring the Application Intelligence solution.

## Create Azure Credentials

To create Azure credentials:

1. From the left navigation pane, click **Inventory** > **Resources** > **Environment**.
2. On the **Environments** page, on the **Credentials** tab, select **Azure** from the drop-down menu.
3. In the Azure Credential page, click **Add**. The **Configure Credential** wizard appears.

4. Enter or select the appropriate information for the Azure credential as described in the following table.

Field	Description
Name	An alias used to identify the Azure credential.
Authentication Type	<p><b>Application ID with Client Secret:</b> Connection with Azure with a service principal. Enter the values for the following fields.</p> <ul style="list-style-type: none"> <li>o <b>Tenant ID</b>—a unique identifier of the Azure Active Directory instance.</li> <li>o <b>Application ID</b>—a unique identifier of an application in Azure platform.</li> <li>o <b>Application Secret</b>—a password or key to request tokens.</li> </ul> <p>Refer to <a href="#">Application ID with client secret</a> for detailed information.</p>
Azure Environment	Select an Azure environment where your workloads are located. For example, Azure_US_Government.

5. Click **Save**.

## Connect to Azure

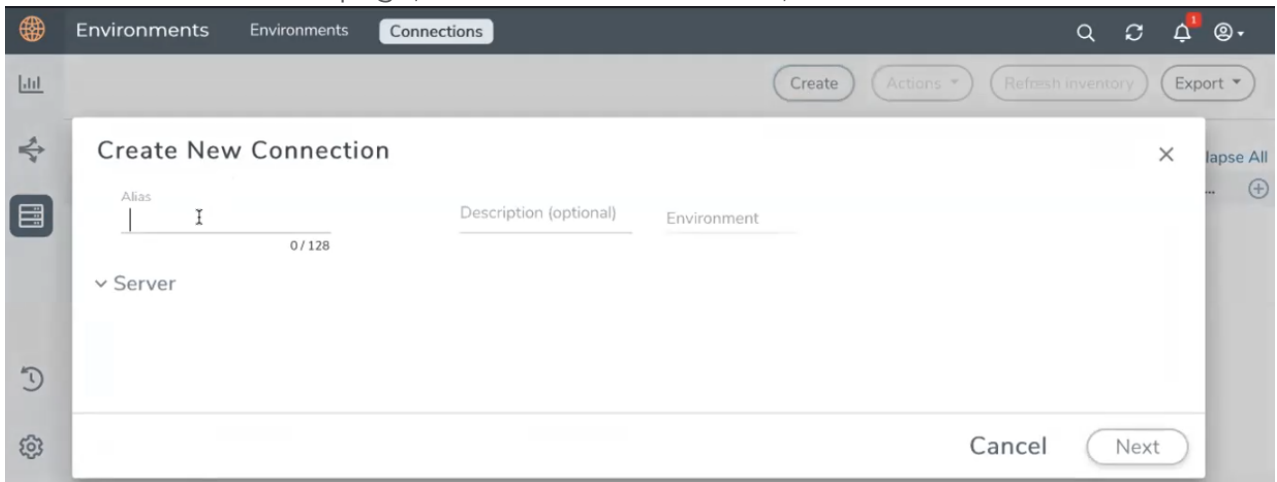
After creating an environment create a connection between the Azure and GigaVUE-FM. Refer to the following step given below for detailed information on how to create a new connection.



## Create Connection

To create a new Connection:

1. Select **Inventory > Resources > Environment**.
2. On the **Environments** page, on the **Connections** tab, click **Create**.



3. The **Create New Connection** dialog box opens. Enter the details as mentioned in the below section.

**NOTE:** When creating a connection in the connections page, the corresponding monitoring domain created for internal use in GigaVUE-FM will not be displayed in the Monitoring Domain list page.

To connect to Azure, select or enter the following details:

Field	Description
<b>Name</b>	Name used to identify the connection.
<b>Credential</b>	Select your credentials from the drop-down menu. Refer <a href="#">Create Credentials</a> for detailed information on how to create credentials.
<b>Subscription ID</b>	Select the subscription ID.
<b>Region Name</b>	The Azure region for the connection. For example, East Asia.

Field	Description
<b>Resource Groups</b>	The Resource Groups created in Azure for communication between the controllers, nodes, and GigaVUE-FM. A Resource Group must contain the VMs that needs to be monitored.
<b>Traffic Acquisition Method</b>	Select a Tapping method. The available options are: <ul style="list-style-type: none"> <li>● <b>UCT-V:</b> If you select UCT-V as the tapping method, you must configure the UCT-V Controller to monitor the UCT-Vs.</li> <li>● <b>Tunnel:</b> If you use select Tunnel as the tapping method, you can select the tunnel as a source where the traffic is directly tunneled to V Series nodes without deploying UCT-Vs or UCT-V Controllers.</li> </ul>
<b>MTU</b>	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> The default MTU is 1450. You can edit the MTU value according to your requirements. The valid range is between 1450 to 9000.</p> </div>

In the Azure Virtual Node Deployment page, select or enter the following details and click **Save**:

Field	Description
Centralized Virtual Network	Alias of the centralized VNet in which the UCT-V Controllers, V Series Proxies, and the GigaVUE V Series nodes are launched.
Authentication Type	Select SSH Public Key as the Authentication Type to connect with the Centralized VNet.
SSH Public Key	The SSH public key for the GigaVUE fabric nodes.
Security Groups	The security group created for the GigaVUE fabric nodes.

Field	Description
Configure a V Series Proxy (optional)	Enable the <b>Configure a V Series Proxy</b> toggle button if you wish to deploy V Series nodes using a proxy.
Enable Custom Certificates	<p>Enable this option to validate the custom certificate during SSL Communication. GigaVUE-FM validates the Custom certificate with the trust store. If the certificate is not available in Trust Store, communication does not happen, and an handshake error occurs.</p> <div style="border: 1px solid black; padding: 5px;"> <p><b>NOTE:</b> If the certificate expires after the successful deployment of the fabric components, then the fabric components moves to failed state.</p> </div>
Certificate	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For more detailed information, refer to <a href="#">Install Custom Certificate</a> .

In the UCT-V Controller section, select or enter the following details:

Field	Description
<b>Controller Version(s)</b>	<p>The UCT-V Controller version you configure must always be the same as the UCT-Vs' version number deployed in the VM machines.</p> <p>If there are multiple versions of UCT-Vs deployed in the VM machines, then you must configure multiple versions of UCT-V Controllers that matches the version numbers of the UCT-Vs.</p> <div style="border: 1px solid black; padding: 5px;"> <p><b>NOTE:</b> If there is a version mismatch between UCT-V Controllers and UCT-Vs, GigaVUE-FM cannot detect the agents in the instances.</p> </div> <p>To add UCT-V Controllers:</p> <ol style="list-style-type: none"> <li>a. Under <b>Controller Versions</b>, click <b>Add</b>.</li> <li>b. From the <b>Image</b> drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances.</li> <li>c. From the <b>Size</b> drop-down list, select a size for the UCT-V Controller. The default size is <b>Standard_B1s</b>.</li> <li>d. In <b>Number of Instances</b>, specify the number of UCT-V Controllers to launch. The minimum number you can specify is 1.</li> </ol>
<b>Management Subnet</b>	<p><b>IP Address Type:</b> Select one of the following IP address types:</p> <ul style="list-style-type: none"> <li>▪ Select <b>Private</b> if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the</li> </ul>

Field	Description
	<p>UCT-V Controller instances and GigaVUE-FM instances in the same network.</p> <ul style="list-style-type: none"> <li>Select <b>Public</b> if you want the IP address to be assigned from Azure's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. On selecting Public IP address type, you must select all the required Public IPs.</li> </ul> <p><b>Subnet:</b> Select a management subnet for UCT-V Controller. The subnet that is used for communication between the UCT-V Controllers and the UCT-Vs, as well as to communicate with GigaVUE-FM.</p> <p>Every fabric node (both controllers and the nodes) need a way to talk to each other and GigaVUE-FM. So, they should share at least one management subnet.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> Some instance types are supported in Azure platform. Refer to Microsoft Azure documentation to learn on supported instance types.</p> </div>
<b>Additional Subnets</b>	<p>(Optional) If there are UCT-Vs on subnets that are not IP routable from the management subnet, additional subnets must be specified so that the UCT-V Controller can communicate with all the UCT-Vs.</p> <p>Click <b>Add</b> to specify additional data subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.</p>
<b>Tags</b>	<p>(Optional) The key name and value that helps to identify the UCT-V Controller instances in your Azure environment. For example, you might have UCT-V Controllers deployed in many regions. To distinguish these UCT-V Controllers based on the regions, you can provide a name that is easy to identify such as us-west-2-uctv-controllers. To add a tag:</p> <ol style="list-style-type: none"> <li>Click <b>Add</b>.</li> <li>In the <b>Key</b> field, enter the key. For example, enter Name.</li> <li>In the <b>Value</b> field, enter the key value. For example, us-west-2-uctv-controllers.</li> </ol>
<b>Agent Tunnel Type</b>	The type of tunnel used for sending the traffic from UCT-Vs to GigaVUE V Series nodes. The options are GRE, VXLAN, and Secure tunnels (TLS-PCAPNG).
<b>Agent Tunnel CA</b>	The Certificate Authority (CA) that should be used in the UCT-V Controller for connecting the tunnel.

**NOTE:** In a connection, you can configure multiple versions of a UCT-V Controller and you can only configure one version of a V Series Proxy.

In the V Series Proxy section, select or enter the values for the fields as described in the previous UCT-V Controller configuration table. The fields of the V Series Proxy configuration are similar to UCT-V Controller configuration.

In the V Series Node section, select or enter the following details:

Fields	Description
<b>Image</b>	From the <b>Image</b> drop-down list, select a V Series node image.
<b>Size</b>	From the <b>Size</b> down-down list, select a size for the V Series node. The default size for V Series configuration is <b>Standard_D4s_v4</b> .
<b>IP Address Type</b>	Select one of the following IP address types: <ul style="list-style-type: none"> <li>▪ Select <b>Private</b> if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the V Series node instances and GigaVUE-FM instances in the same network.</li> <li>▪ Select <b>Public</b> if you want the IP address to be assigned from Azure's pool of public IP address. On selecting Public IP address type, you must select the number of Public IPs defined in the Maximum Instance.</li> </ul>
<b>Management Subnet</b>	<b>Subnet:</b> Select a management subnet for V Series node. The subnet that is used for communication between the UCT-Vs and the V Series nodes, as well as to communicate with GigaVUE-FM.  Every fabric node (both controllers and the nodes) needs a way to talk to each other and GigaVUE-FM. So, they should share at least one management subnet.
<b>Data Subnets</b>	The subnet that receives the mirrored VXLAN tunnel traffic from the UCT-Vs. Select a <b>Subnet</b> and the respective <b>Security Groups</b> . Click <b>Add</b> to add additional data subnets.  <b>NOTE:</b> Using the <b>Tool Subnet</b> checkbox you can indicate the subnets to be used by the V Series node to egress the aggregated/manipulated traffic to the tools.
<b>Tag(s)</b>	(Optional) The key name and value that helps to identify the V Series node instances in your Azure environment. For example, you might have V Series node deployed in many regions. To distinguish these V Series node based on the regions, you can provide a name that is easy to identify. To add a tag: <ol style="list-style-type: none"> <li>Click <b>Add</b>.</li> <li>In the <b>Key</b> field, enter the key. For example, enter Name.</li> <li>In the <b>Value</b> field, enter the key value.</li> </ol>

Use the following buttons to manage your Azure connections :

Button	Description
<b>Create</b>	Use to create new connection.
<b>Actions</b>	Provides the following options: <ul style="list-style-type: none"> <li>• <b>Edit Connection</b> - Use to edit a connection. You can also use this option to deploy your node after creating the connection.</li> <li>• <b>Edit Node</b> - If you have already deployed your node, then use this option to edit your node. You can also use this option to add more nodes into your existing connection.</li> <li>• <b>Delete Connection</b> - Use to delete a connection.</li> <li>• <b>Delete Node</b> - Use to delete a node.</li> </ul>

Button	Description
	<ul style="list-style-type: none"> <li>• <b>Force Delete</b> - This option is enabled when an upgrade fails due to infrastructure issues. Use this option to force delete the connection.</li> <li>• <b>Upgrade Fabric</b> - Use to upgrade your fabric components.</li> </ul>
<b>Refresh Inventory</b>	Use to refresh the selected connection.
<b>Export</b>	Use to export the details from the Connections page into an XLS or a CSV file.

To create Application Intelligence sessions, refer to [Create an Application Intelligence Session in Virtual Environment](#).

Refer the following Gigamon Validated Design for more detailed information on how to achieve deep observability in Azure

- [Supplementing the Existing Tools to Gain Deep Observability in Azure \(5.15\)](#)

## Create Source Selectors

When setting up a traffic flow, it is important to define the selection criteria for the source of traffic. Use the Source Selectors page for configuring the source of traffic to the GigaVUE V Series nodes.

**NOTE:** When deploying the Application Intelligence using Source Selector, if the GigaVUE V Series Node is down, you will not be able to view the Selected Targets and UCT-Vs.

To configure the Source Selectors:

1. Select **Inventory > Resources > Source Selectors**.
2. On the **Source Selectors** page, on the **VM** tab, click **Create**. The **Create Source Selector** wizard appears.

### Create Source Selector ✕

Alias 0 / 128

---

Description 0 / 128

---

**Filters**

Criteria 1 ⊖

Filter

Operator

+ -

+ New Criteria

Cancel
Save

3. Enter or select the required information:

Field	Description
<b>Alias</b>	Name of the source
<b>Description</b>	Description of the source
<b>Filters</b>	You can create a filter template from the Filters option
<b>Criteria 1</b>	Criteria to filter the traffic source. <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;"><b>NOTE:</b> You can create multiple criteria.</div>
<b>Filter</b>	The criteria based on which the traffic is filtered. Select from the list of available filters. <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;"><b>NOTE:</b> Ensure that the registered traffic agents match the filter criteria.</div>
<b>Operator</b>	Select the required operator based on the filter selected. Options are: <ul style="list-style-type: none"> <li>Starts with</li> <li>Ends with</li> <li>excludes</li> <li>equals</li> <li>between</li> </ul>
<b>Values</b>	The values for the filter.

4. Click Save to save the source selector.



**Note:** You can create multiple filter criteria. Within each criterion, you can configure multiple filters.

- If you have configured multiple filters in a criterion, then the traffic will be filtered only if all the filter rules are true.
- If you have configured multiple criteria, then the traffic will be filtered even if one of the criteria is true.
- A maximum of 25 inclusion rulesets and 25 exclusion rulesets can be added.

## Create Tunnel Specifications

A tunnel endpoint can be created using a standard L2GRE, VXLAN, or ERSPAN tunnel. The tunnel can be an ingress tunnel or an egress tunnel.

**NOTE:** VXLAN is the only supported tunnel type for Azure.

To configure the tunnels:

1. Select **Inventory > Resources > Tunnel Specifications**.
2. On the **Tunnel Specifications** page, navigate to **VM** tab and click **Create**. The Create Tunnel Specification wizard appears.



## Create tunnel specification




Alias	Description	
Alias *	Description (optional)	Tunnel type

Cancel

Save

3. Enter or select the following information:

Field	Description
<b>Alias</b>	<p>The name of the tunnel endpoint.</p> <p><b>NOTE:</b> Do not enter spaces in the alias name.</p>
<b>Description</b>	The description of the tunnel endpoint.
<b>Tunnel Type</b>	<p>The type of the tunnel.</p> <p>Select ERSPAN, or L2GRE, or VXLAN to create a tunnel.</p> <p>Do not select UDPGRE tunnel type.</p> <p><b>NOTE:</b> VXLAN is the only supported tunnel type for Azure.</p>
<b>Traffic Direction</b>	<p>The direction of the traffic flowing through the V Series node.</p> <ul style="list-style-type: none"> <li>Choose <b>In</b> (Decapsulation) for creating an Ingress tunnel, Tunnel Spec for the Source should always have the Traffic Direction as IN, signifying an ingress tunnel. Enter values for the Key.</li> <li>Choose <b>Out</b> (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint. Select or enter values for MTU, Time to Live, DSCP, PREC, Flow Label, and Key.</li> </ul> <p> ERSPAN, L2GRE, and VXLAN are the supported <b>Ingress tunnel</b> types. You can configure Tunnel Endpoint as your first level entity in Monitoring Session.</p> <ul style="list-style-type: none"> <li>L2GRE and VXLAN are the supported <b>Egress tunnel</b> types.</li> <li>For Azure connection, VXLAN is the supported Ingress and Egress tunnel type.</li> </ul>
<b>IP Version</b>	The version of the Internet Protocol. Select IPv4 or IPv6.
<b>Remote Tunnel IP</b>	<p>For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.</p> <p>For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.</p>

4. Click **Save** to save the configuration.

## User Defined Application

This feature gives you the ability to classify the applications by the DPI engine. This allows unclassified TCP, UDP, HTTP, and HTTPS applications to be identified and named with the help of user defined application signatures.

To configure User Defined Application signatures :

Step Number	Task	Refer the following
1	Create rules under User Defined Application Section	Create rules under User Defined Application
2	Configure Application Intelligence Session	For Physical: <a href="#">Application Intelligence Session</a> For Virtual: <a href="#">Configure Application Intelligence Session</a>
3	Monitor User Defined Application	<a href="#">View the Application Intelligence Dashboard</a>

### Create Rules under User Defined Application

1. Click **Inventory**.
2. Click **User Defined Applications** to create rules based on a set of **Supported Protocols and Attributes**. For information on **Supported protocols and Attributes** refer **User Defined Application** topic. This helps the physical or virtual node to classify the traffic based on the protocols and attributes selected in the created rule.
3. Click **New** in the **User Defined Applications** screen to create a new rule.
4. Enter **Application Name**.
5. Enter **Priority**. The value must be between 1 and 120.  
**Note:** The least value will have the highest priority.
6. In the created rule:
  - a. Choose the **Protocol** from the list of protocols.
  - b. Choose the **Attributes** from the list of attributes.
  - c. Choose the **Values** from the list of values.

7. Click **Apply**. The rule is now created. For information on the limitations for creating rules refer Configuration Limitations section.
8. Click the application listed under the **Applications** column.
9. Click the **Rule** tab.
10. Select a rule to view its protocol details.

## Supported Protocols and Attributes

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

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

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

	referer	URI	address where client got the URI	to Server Only		
	stc-server_agent	Server Agent	Software used for the server	Server to Client Only	REGEXP	NWS_TCloud_PX
	stc-location	Redirect Location	Destination address where the client is redirected to	Server to Client Only	REGEXP	.*\Vfootball\ .*
	cts-cookie	Cookie (Raw)	Raw value of the HTTP Cookie header line	Client to Server Only	REGEXP	.*tEstCoOkie.*
	content	Content	Message body content	Both, Client to Server or Server to Client	REGEXP	.*GIGAMON.* mindata = 206 Refer <a href="#">Mindata</a>
ssl	common_name	Domain Name	Domain name from Client Hello message or the certificate		REGEXP	(.*\.)?gigamon\.com
	stc-	Subject	List of	Server	REGEXP	(.*\.)?gigamon\.com

	subject_ alt_ name	t Alt Name (s)	host names which belong to the same certificat e	to Client Only		
rtmp	cts- page_ url	Page URL	URL of the webpage where the audio/vid eo content is streame d	Client to Server Only	REGEXP	http:\\\\www.music.tv\\recode d\\1234567
tcp	stream	Payloa d Data	Data payload for a packet, excludin g the header.		REGEXP	.*GIGAMON.*  mindata = 70  Refer <a href="#">Mindata</a>
	port	Server Port	Server (listen) port number		UINT16 RANGE as REGEXP String	80-4350
udp	stream	Payloa d Data	Data payload for a packet, excludin g the header		REGEXP	.*GIGAMON.*  mindata = 100  Refer <a href="#">Mindata</a>
	port	Server Port	Server (listen)		UINT16 RANGE	80-4350

			port number		as REGEXP String	
sip	user_agent	User Agent	Software used	Both, Client to Server or Server to Client	REGEXP	GVUE-release 6.2.0
icmp	code	Message Code	Code of the ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	200
	typeval	Message Type	Type of ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	10
ip	address	Server IP Addresses	IP address of the server		IPV4 as REGEXP String	62.132.12.30/24
	dscp	DSCP Value	DSCP from Differentiated Service (DS) Field in IP header		UINT8 as REGEXP String	33

	resolv_name	DNS Name	Server's DNS name		REGEXP	gigamon.com
ipv6	address	Server IP Address	IP address of the server		IPV6 as REGEXP String	2001:0:9d38:6ab8:307b:16a4:9c66:5f4 2001:0:9d38::9c66:5f4/64
	dscp	DSCP Value	DSCP from Differentiated Service (DS) Field in IP header		UINT8 as REGEXP String	43

## Mindata

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

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

## Supported RegExp Syntax

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

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

## Limitations

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

## Configure Application Intelligence Session

Application Intelligence provides a comprehensive solution that:

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

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

- **Application Visualization (earlier known as Application Monitoring)** - Identifies and monitors all applications contributing to the network traffic, and reports on the total applications and the total bandwidth they consume over a select period. Able to identify more than 3,200 applications. It displays the traffic statistics in bytes, packet and flows.



- **Application Filtering Intelligence**- Enables traffic filtering by layer 7 applications, which means you can filter out high-volume, low-risk traffic from reaching the tools and distribute high-risk network traffic of interest to the right tool at the right time.
- **Application Metadata Intelligence** - Supports exporting over 5000 attributes of metadata that provide relevant usage context on over 3,200 applications, thus enabling you to rapidly identify indicators of compromise (IoC) for security analytics and forensics tools.

## Prerequisites

- The environment on which the Application Intelligence solution is to be deployed must already be created and the nodes must be deployed on it.
- In virtual environment, the destination tunnels for the Application Filtering Intelligence Map must already be created.

**NOTE:** For Application Visualization and Application Metadata Intelligence, the destination(s) are defined internally by the solution.

## Create an Application Intelligence Session in Virtual Environment

To create an Application Intelligence Session:

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

3. In the **Basic Info** section, enter the name and description, and in the Environment select **Virtual** for the session to be created:
  - Virtual- connects to the specific environment.
4. In the Environment section, select the **Environment Name**, and the **Connection Name**. To create an Environment and connection, refer to *Configure Environment* section in the respective cloud guides..

5. In the **Configurations** section, complete the following:
- Select an **Export Interval** during which you want the Application Intelligence session to generate the reports for application visualization. The valid range is 60–900 seconds.
  - Select the required interface. By default, **Management Interface** is enabled. To export the data through tunnel interface, uncheck the Management Interface check box.
  - Enter a value for the **Scale Unit**. The scale unit represents the number of flows supported by the application. If the scale unit value is 1, the maximum active flow limit will be 100k.  
Refer to the following table for the maximum scale unit supported for VMware, AWS Nutanix, and Azure platforms.

Cloud Platform	Instance Size	Maximum Scale Unit	
		Secure Tunnel Disabled	Secure Tunnel Enabled
VMware	Large (8 vCPU and 16 GB RAM)	3	2
AWS	Large (c5n.2xlarge)	4	3
	Medium (t3a.xlarge)	3	1
Azure	Large (Standard_D8s_V4)	9	5
	Medium (Standard_D4s_v4)	3	1
Nutanix	Large (8 vCPU and 16 GB RAM)	3	2

**NOTE:** If the Application Intelligence Session deployment fails, due to using a scale unit other than the recommended scale unit, then reload the GigaVUE V Series Node.

6. In the **Source Traffic** section, select anyone of the following:
- **Source Selector**- Select the source from the drop-down list box. To create new source, select **New Source Selector** and add the filters. For more information on creating a New Source Selector, refer to [Create Source Selectors](#).
    - **Prefilter** - Enable the mirroring option, select the prefilter checkbox and then select the policy. If you want to enable Secure tunnel, then select the secure tunnel checkbox.
    - **Precryption**: Select the Precryption checkbox and then select the policy. If you want to enable Secure tunnel, then select the secure tunnel checkbox.

**NOTE:** You cannot configure Source Selectors when you deploy the GigaVUE V Series Nodes using the Third Party Orchestration in VMware ESXi host.

- **Tunnel Specification-** Select the tunnel from the drop-down list box. To create new tunnel, select **New Source Tunnel Spec** and add the details for the tunnel. For more information on creating a new tunnel, refer to [Create Tunnel Specifications](#).

**NOTE:** Select the ens192 interface for the Tunnel Specifications from the drop-down menu when using third party orchestration.

- **Raw End Point-** Select the Raw End Point Interface from the drop-down menu which will trap the traffic for application monitoring.

**NOTE:** This field is applicable only when you deploy your GigaVUE V Series Nodes using third party orchestration in VMware ESXi Host, Nutanix and Google Cloud Platform.



- Tunnel Specification for the source must always be configured with Traffic Direction as IN, to indicate that it is an ingress tunnel.
- For Azure Connection, VXLAN is the only supported Tunnel Type.

7. Click **Save**. The session created is added in the list view.
8. In the **User Defined Applications** section, select the template from the list. For information on **Supported protocols and Attributes** and **Limitations** refer **User Defined Application** topic.

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

Select the session from the Application Intelligence Sessions pane and click on the icon and select **View Details** from the drop-down menu, to view the deployed UCT-V, their status and more information about source selectors, selected target.

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

**NOTE:** GigaVUE-FM takes few minutes to display the application statistics.

**NOTE:** The option **Reapply all pending solutions** is applicable for physical solution only.

When the Application Intelligence solution is in suspended state, you cannot delete the session. You can click on the icon and select **View Details** from the drop-down menu, to view the details.

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

## Slicing and Masking in Application Filtering Intelligence

When the traffic passes through the Application Filtering Intelligence, application metadata is created. With the addition of slicing and masking parameters to the existing application filtering functionality, you will be able to slice, mask, or slice and mask the filtered packets before sending them to the destination tunnel endpoint.

For step-by-step instructions on how to configure Application Filtering Intelligence refer to [Create Application Filtering Intelligence by Editing Monitoring Session from Dashboard](#) topic from *GigaVUE Fabric Management Guide*.

### Configuring Application Filtering Intelligence with Slicing

You can enable the slicing configuration and provide inputs for each **Application Filtering** rule set:

1. From the **Select a Protocol** drop-down list, choose a protocol.
2. In the **Offset** field, specify the length of the packet that must be sliced.

The filtered traffic will be sliced before forwarding it to the destination tunnel endpoint.

Refer to Slicing section in the *GigaVUE V Series Applications Guide* for more detailed information on Slicing.

### Configuring Application Filtering Intelligence with Masking

You can enable the masking configuration and provide inputs for each **Application Filtering** rule set:

1. From the **Select a Protocol** drop-down list, choose a protocol.
2. In the **Offset** field, specify the length of the packet that must be masked.
3. In the Pattern field, enter the pattern for masking the packet.
4. In the Length field, enter the length of the packet that must be masked.

The filtered traffic will be masked before forwarding it to the destination tunnel endpoint.

Refer to Masking section in the *GigaVUE V Series Applications Guide* for more detailed information on Masking.

## Configuring Application Filtering Intelligence with Slicing and Masking

You can enable both slicing and masking configurations, and provide inputs for each **Application Filtering** rule set.

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

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

## Application Metadata Intelligence

Application Metadata Intelligence generates more than 5000 attributes for more than 3200 applications without impacting the users, devices, applications, or the network appliances. The feature identifies applications even when the traffic is encrypted.

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

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

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


Application Metadata Intelligence generates metadata only if the application is allowed to be passed in Application Filtering Intelligence. For example, Application Metadata Intelligence has the capability to generate metadata for HTTP traffic only if Application Filtering Intelligence filters in the HTTP traffic.

Refer to [Create Application Metadata Intelligence Session for Virtual Environment](#) topic for step-by-step instructions on how to configure Application Metadata Intelligence on Virtual Environment.

## Create Application Metadata Intelligence Session for Virtual Environment

You can create an Application Metadata Intelligence session for virtual environment.

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

1. Go to **Traffic > Solutions > Application Intelligence**.
2. From the Sessions pane, click  and select **Edit**. The **Edit Application Intelligence Session** window appears.
3. In the **Edit Application Intelligence Session** window, click **Application Metadata**.

**NOTE:** If Application Filtering Intelligence License is available, you must create Application Filtering to create Application Metadata Intelligence. For more information, refer to [Create Application Filtering Intelligence by Editing Monitoring Session from Dashboard](#)


4. In the **Destination Traffic** section, click **+ Add New** to create an exporter to receive application-specific traffic. You can also create multiple exporters.
- a. Enter the following details:

Field	Description
<b>Tool Name</b>	Enter the tool Name
<b>Tool IP Address</b>	Enter the tool IP address
<b>Template</b>	Select the tool template. Refer to <a href="#">Tool Templates</a> for more details on what are tool templates and to create custom tool templates.
<b>L4 Source Port</b>	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.
<b>L4 Destination Port</b>	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.
<b>APPLICATION ID</b>	Enable to export the data with Application Id.
<b>Format</b>	Select NetFlow or CEF
<b>NetFlow:</b> Select this option to use Netflow	
Record / Template type	<ul style="list-style-type: none"> <li>● Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool.</li> <li>● Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.</li> </ul>
Active Timeout	Enter the active timeout value in seconds.
Inactive Timeout	Enter the inactive timeout in seconds.
Version	Select the NetFlow version.
Template Refresh Interval	Enter the time interval at which the template must be refreshed in seconds
<b>CEF:</b> Select this option to use CEF	
Record / Template type	<ul style="list-style-type: none"> <li>● Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool.</li> <li>● Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.</li> </ul>
Active Timeout	Enter the active timeout value in seconds.
Inactive Timeout	Enter the inactive timeout in seconds.

- b. Click **App Editor**, to select the applications and its attributes. You can select a maximum of 64 attributes for each of the application. (Not applicable when using NetFlow V5 Template in the above **Template** drop-down menu.) The Application Editor screen appears as shown:

- c. Select an **Application Family** and the **Applications** that needs to be filtered from the traffic. You can also select **Add All Applications in Family** or **Delete All Applications in Family**. The selected applications and their families appear in the **Selected Applications** section.

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

5. In the **Advanced Settings > Collects** section, you can select the following packet attributes:
  - Counter - Select the Bytes, and Packets.
  - IPv4 - Select the required attributes. By default, Source Address, Destination Address, and Protocol are enabled.
  - IPv6 - Select the required attributes. By default, Source Address, Destination Address, and Next Header are enabled.
  - Transport -Select the required attributes. By default, Source Port, Destination Port are enabled.
- a. By default, the above collect types are displayed. Click  to add the following collect types:
  - Data Link - Select any one of the parameters such as Source Mac, Destination Mac and VLAN.
  - Timestamp - Select the required timestamp such as System Uptime First, Flow Start, System Uptime Last, and Flow End.
  - Flow - Select the parameter as End Reason if required.
  - Interface - Select any one of the parameter such as Input Physical, Output Physical and Input Name.



6. In the **Application Metadata Settings** section:
  - a. Select the Flow Behavior as any one of the following:
    - Uni-Directional
    - Bi-Directional. The default value is Bi-Directional.
  - b. Enter the Timeout and Cache Size.
  - c. You can enable or disable the **Multi-Collect** option to perform the following:
    - **Enable** — Enables the multi-collect of attributes within a given Metadata Store cache which means that if a configured attributes is seen in multiple packets within the same flow, each of these information is collected. By default, when a new cache is created, multi-collect is enabled. When upgraded from an older release, the multi-collect option is enabled.
    - **Disable** — Disables the multi-collect of attributes within a given Metadata Store cache.
  - d. You can use the toggle button to enable or disable the **Aggregate Mode**, which is disabled by default. You need to delete the existing solution and recreate the solution to enable the **Aggregate Mode**. The **Aggregate Mode** option is applicable only for Gen 3 devices. Only one exporter is supported with the **Aggregate Mode** enabled.

Protocol Name	Attribute
http	rtt
icmp	rtt
icmp6	rtt
ssh	rtt
tcp	rtt
tcp	rtt_app
telnet	rtt
wsp	connect_rtt
wsp	query_rtt

**NOTE:** You need to enable the **Aggregate Mode** option to export the minimum, maximum, and mean of RTT values for the following list of supported protocols and attributes and also the aggregate of TCP Lost byte values collected per export time interval.

- e. You can enable or disable the **Advance Hash** option to perform the following:
    - **Enable** — Configures metadata cache advance-hash for encapsulated flows . This feature improves the efficiency of scheduling the distribution of encapsulated flows. It also improves the distribution of flows in service provider deployment cases. By default, when a new cache is created, advance hash is enabled. When upgraded from an older release, the advance hash is enabled.
    - **Disable** — Disables the metadata cache advance-hash for flows.
  - f. If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the **Data Link** and enable the **VLAN** option.
  - g. In the **Observation Domain ID** field, enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is **00 01 02 05**, and in Decimal is **66053**.
7. Click **Save**.

The metrics of the Application Metadata traffic appear on the dashboard.

## Create NetFlow Session for Virtual Environment

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

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

To create an NetFlow session, follow these steps:

1. On the left navigation pane, select **Traffic > Solutions >Application Intelligence**.
2. Click **Create** . The **Create Application Intelligence Session** page appears.
3. In the **Basic Info** section, enter the name and description, and in the Environment select **Virtual** for the session to be created.
4. In the Environment section, select the **Environment Name**, and the **Connection Name**. To create an Environment and connection, refer to *Configure Environment* section in the respective cloud guides.
5. In the **Configurations** section, complete the following:
  - a. The **Export Interval** during which you want the Application Intelligence session to generate the reports for application visualization is 5 seconds
  - b. By default, **Management Interface** is enabled.

6. In the **Source Traffic** section, select anyone of the following:
  - a. **Source Selector**- Select the source from the drop-down list box. To create new source, select **New Source Selector** and add the filters. For more information on creating a New Source Selector, refer to [Create Source Selectors](#)

**NOTE:** You cannot configure Source Selectors when you deploy the GigaVUE V Series Nodes using Third Party Orchestration in VMware ESXi Host

- b. **Tunnel Specification**- Select the tunnel from the drop-down list box. To create new tunnel, select **New Source Tunnel Spec** and add the details for the tunnel. For more information on creating a new tunnel, refer to [Create Tunnel Specifications](#).

**NOTE:** Select the ens192 interface for the Tunnel Specifications from the drop-down menu when using third party orchestration. Tunnel Specification for the source must always be configured with Traffic Direction as IN, to indicate that it is an ingress tunnel. For Azure Connection, VXLAN is the only supported Tunnel Type.

- c. **Raw End Point**- Select the Raw End Point Interface from the drop-down menu which will tap the traffic for application monitoring.

**NOTE:** This field is applicable only when you deploy your GigaVUE V Series Nodes using third party orchestration in VMware ESXi Host, Nutanix and Google Cloud Platform.

7. Click on the **Application Metadata** tab.

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

Field	Description
<b>Tool Name</b>	Enter the tool name.
<b>Tool IP Address</b>	Enter the tool IP address.
<b>Template</b>	Select the tool template. Refer to <a href="#">Tool Templates</a> for more details on what tool templates are and to create custom tool templates.
<b>L4 Source Port</b>	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.
<b>L4 Destination Port</b>	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.
<b>APPLICATION ID</b>	Enable to export the data with Application Id.
<b>Format</b>	NetFlow
<b>Record / Template type</b>	<ul style="list-style-type: none"> <li>● Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool.</li> <li>● Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.</li> </ul>
<b>Active Timeout</b>	Enter the active timeout value in seconds.
<b>Inactive Timeout</b>	Enter the inactive timeout in seconds.
<b>Version</b>	Select the NetFlow version.
<b>Template Refresh Interval</b>	Enter the time interval at which the template must be refreshed in seconds.

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

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

- TimeStamp
- Counter
- Interface
- IPv4
- Transport

10. In the **Application Metadata Settings** section:
- Select the Flow Behavior as any one of the following:
    - Uni-Directional
    - Bi-Directional. The default value is Bi-Directional.
  - Enter the Timeout and Cache Size.
  - You can enable or disable the **Multi-Collect** option to perform the following:
    - **Enable** — Enables the multi-collect of attributes within a given Metadata Store cache which means that if a configured attributes is seen in multiple packets within the same flow, each of these information is collected. By default, when a new cache is created, multi-collect is enabled. When upgraded from an older release, the multi-collect option is enabled.
    - **Disable** — Disables the multi-collect of attributes within a given Metadata Store cache.
  - You can use the toggle button to enable or disable the **Aggregate Mode**, which is disabled by default. You need to delete the existing solution and recreate the solution to enable the **Aggregate Mode**. The **Aggregate Mode** option is applicable only for Gen 3 devices. Only one exporter is supported with the **Aggregate Mode** enabled.

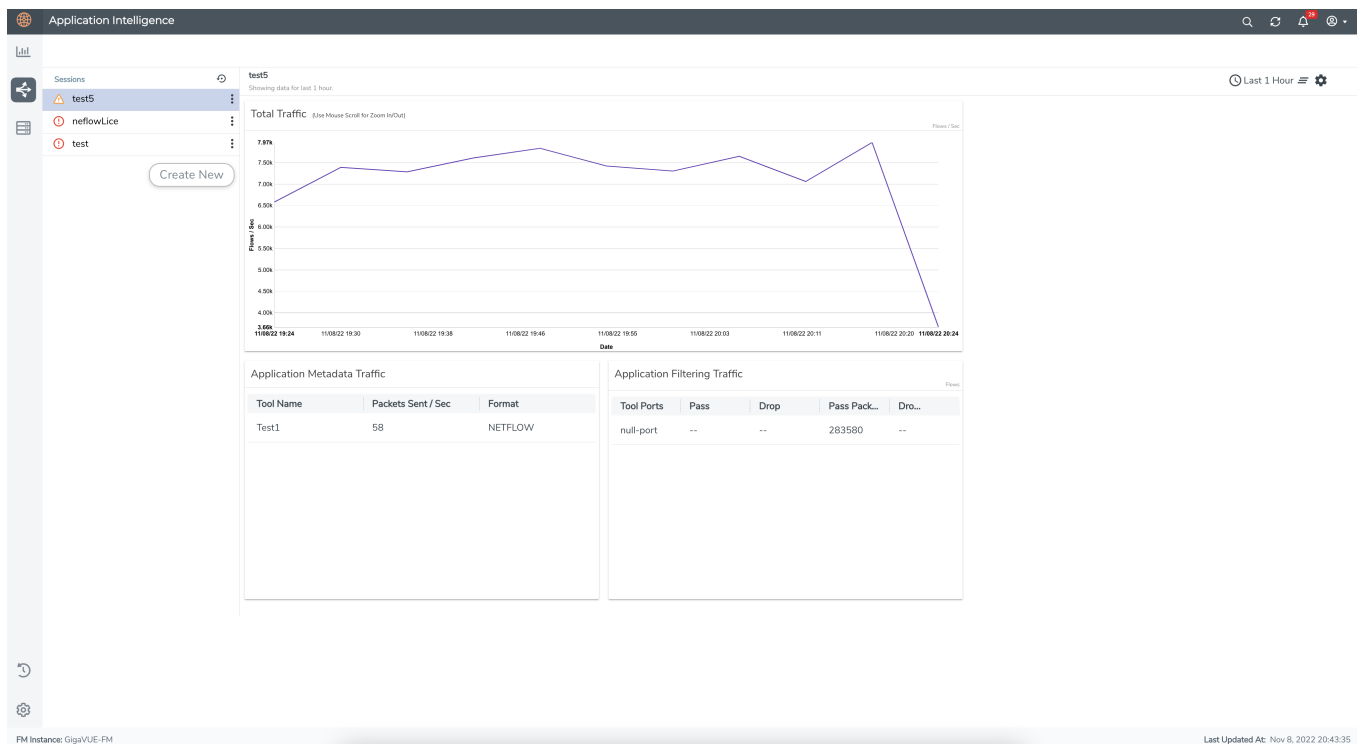
Protocol Name	Attribute
http	rtt
icmp	rtt
icmp6	rtt
ssh	rtt
tcp	rtt
tcp	rtt_app
telnet	rtt
wsp	connect_rtt
wsp	query_rtt

**NOTE:** You need to enable the **Aggregate Mode** option to export the minimum, maximum, and mean of RTT values for the following list of supported protocols and attributes and also the aggregate of TCP Lost byte values collected per export time interval.

- e. You can enable or disable the **Advance Hash** option to perform the following:
- **Enable** — Configures metadata cache advance-hash for encapsulated flows . This feature improves the efficiency of scheduling the distribution of encapsulated flows. It also improves the distribution of flows in service provider deployment cases. By default, when a new cache is created, advance hash is enabled. When upgraded from an older release, the advance hash is enabled.
  - **Disable** — Disables the metadata cache advance-hash for flows.
- f. If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the **Data Link** and enable the **VLAN** option.
- g. In the **Observation Domain ID** field, enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is **00 01 02 05**, and in Decimal is **66053**.
11. Click **Save**.

## NetFlow Dashboard

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



# Secure Tunnels

Secure Tunnel securely transfers the cloud captured packets on UCT-V and UCT-C to a GigaVUE V Series Node or Tool (only in case of UCT-C). The data from UCT-V and UCT-C are encapsulated in PCAPng format, and the encrypted data is sent over a TLS connection to a GigaVUE V Series Node.

Secure Tunnel can also transfer the cloud captured packets from a GigaVUE V Series Node to another GigaVUE V Series Node.

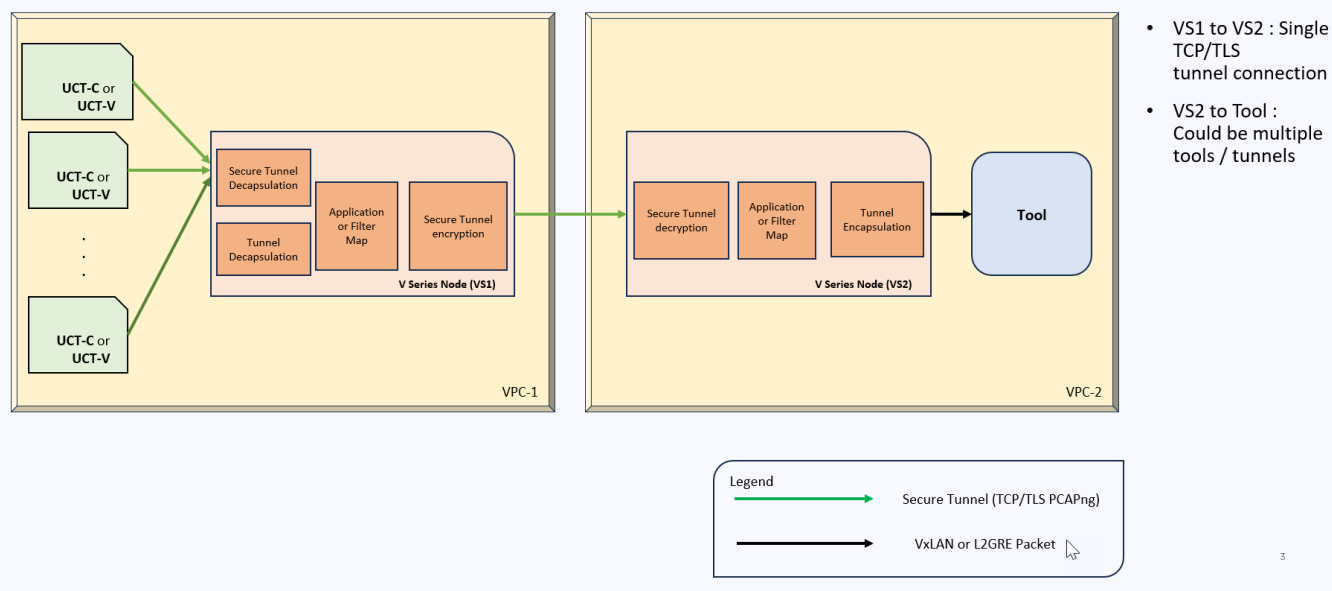
In case of GigaVUE V Series Node to GigaVUE V Series node, the traffic from the GigaVUE V Series Node 1 is encapped using PCAPNG format and transported to GigaVUE V Series Node 2 where the traffic is decapped. The secure tunnels between V Series Node to V Series Node have multiple uses cases.

The GigaVUE V Series Node decapsulates and processes the packet per the configuration. The decapsulated packet can be sent to the application such as De-duplication, Application Intelligence, Load balancer and to the tool. The Load Balancer on this node can send the packets to multiple V series Nodes, in this case the packets can be encapsulated again and sent over a secure tunnel.

For more information about PCAPng, refer to [PCAPng Application](#).

## Secure Tunnel Use Case

Tool in remote Virtual Private Cloud (VPC) – Single V Series Node



## Supported Platforms

Secure tunnel is supported on:

- OpenStack
- Azure
- AWS
- VMware NSX-T (only for Third Party Orchestration)
- VMware ESXi (only for Third Party Orchestration)
- Nutanix (only for Third Party Orchestration)
- Google Cloud Platform (only for Third Party Orchestration)

For information about how to configure secure tunnels, refer to the section [Configure Secure Tunnel](#).

## Configure Secure Tunnel

Secure tunnel can be configured on:

- [Precrypted Traffic](#)
- [Mirrored Traffic](#)

### Precrypted Traffic

You can send the precrypted traffic through secure tunnel. When secure tunnel for precryption is enabled, packets are framed and sent to the TLS socket. PCAPng format is used to send the packet.

When you enable the secure tunnel option for both regular and precryption packets two TLS secure tunnel sessions are created.

It is recommended to always enable secure tunnels for precrypted traffic to securely transfer the sensitive information.

For more information about PCAPng, refer to [PCAPng Application](#).

### Mirrored Traffic

You can enable the Secure Tunnel for mirrored traffic. By default, Secure Tunnel is disabled.

Refer to the following sections for Secure Tunnel Configuration:

- [Configure Secure Tunnel from UCT-V to GigaVUE V Series Node in UCT-V](#)
- [Configure Secure Tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2](#)



## Prerequisites

While creating Secure Tunnel, you must provide the following details:

- SSH key pair
- CA certificate

## Configure Secure Tunnel from UCT-V to GigaVUE V Series Node

To configure a secure tunnel in UCT-V, you must configure one end of the tunnel to the UCT-V and the other end to GigaVUE V Series Node. You must configure the CA certificates in UCT-V and the private keys and SSL certificates in GigaVUE V Series Node. Refer to the following steps for configuration:

S. No	Task	Refer to						
1.	Upload a Custom Authority Certificate (CA)	<p>You must upload a Custom Certificate to UCT-V Controller for establishing a connection with the GigaVUE V Series Node.</p> <p>To upload the CA using GigaVUE-FM follow the steps given below:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Inventory &gt; Resources &gt; Security &gt; CA List</b>.</li> <li>2. Click <b>New</b>, to add a new Custom Authority. The <b>Add Custom Authority</b> page appears.</li> <li>3. Enter or select the following information. <table border="1" data-bbox="706 1119 1474 1283"> <thead> <tr> <th>Field</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Alias</td> <td>Alias name of the CA.</td> </tr> <tr> <td>File Upload</td> <td>Choose the certificate from the desired location.</td> </tr> </tbody> </table> </li> <li>4. Click <b>Save</b>.</li> </ol> <p>For more information, refer to the section <a href="#">Adding Certificate Authority</a></p>	Field	Action	Alias	Alias name of the CA.	File Upload	Choose the certificate from the desired location.
Field	Action							
Alias	Alias name of the CA.							
File Upload	Choose the certificate from the desired location.							
2.	Upload a SSL Key	<p>You must add a SSL key to GigaVUE V Series Node. To add SSL Key, follow the steps in the section <a href="#">SSL Decrypt</a>.</p>						

S. No	Task	Refer to
3	Enable the secure tunnel	<p>You should enable the secure tunnel feature to establish a connection between the UCT-V and GigaVUE V Series Node. To enable the secure tunnel feature follow these steps:</p> <ol style="list-style-type: none"> <li>1. In the Edit Monitoring Session page, click <b>Options</b>. The <b>Apply template</b> page appears.</li> <li>2. Enable the <b>Secure Tunnel</b> button. You can enable secure tunnel for both mirrored and precrypted traffic.</li> </ol>
4.	Select the SSL Key while creating a monitoring domain and configuring the fabric components in GigaVUE-FM.	<p>You must select the added SSL Key in GigaVUE V Series Node while creating a monitoring domain configuring the fabric components in GigaVUE-FM. To select the SSL key, follow the steps in the section <a href="#">Configure GigaVUE Fabric Components in GigaVUE-FM</a></p> <p>If the existing monitoring domain does not have a SSL key, you can add it by following the given steps:</p> <ol style="list-style-type: none"> <li>1. Select the monitoring domain for which you want to add the SSL key.</li> <li>2. Click the <b>Actions</b> drop down list and select <b>Edit SSL Configuration</b>. An <b>Edit SSL Configuration</b> window appears.</li> <li>3. Select the CA in the <b>UCT-V Agent Tunnel CA</b> drop down list.</li> <li>4. Select the SSL key in the <b>V Series Node SSL key</b> drop down list.</li> <li>5. Click <b>Save</b>.</li> </ol>
5.	Select the CA certificate while creating the monitoring domain configuring the fabric components in GigaVUE-FM.	<p>You should select the added Certificate Authority (CA) in UCT-V Controller. To select the CA certificate, follow the steps in the section <a href="#">Configure GigaVUE Fabric Components in GigaVUE-FM</a></p>

## Configure Secure Tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2

You can create secure tunnel in the following ways:

- Between GigaVUE V Series Node 1 to GigaVUE V Series Node 2
- From GigaVUE V Series Node 1 to multiple GigaVUE V Series nodes.

You must have the following details before you start the configuration of secure tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2:

- IP address of the tunnel destination endpoint (GigaVUE V Series Node 2).
- SSH key pair (pem file).

To configure secure tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2, refer to the following steps:

S. No	Task	Refer to						
1.	Upload a Certificate Authority (CA) Certificate	<p>You must upload a Custom Certificate to UCT-V Controller for establishing a connection between the GigaVUE V Series Node.</p> <p>To upload the CA using GigaVUE-FM follow the steps given below:</p> <ol style="list-style-type: none"> <li>Go to <b>Inventory &gt; Resources &gt; Security &gt; CA List</b>.</li> <li>Click <b>Add</b>, to add a new Certificate Authority. The <b>Add Certificate Authority</b> page appears.</li> <li>Enter or select the following information. <table border="1" data-bbox="388 611 1474 774"> <thead> <tr> <th>Field</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Alias</td> <td>Alias name of the CA.</td> </tr> <tr> <td>File Upload</td> <td>Choose the certificate from the desired location.</td> </tr> </tbody> </table> </li> <li>Click <b>Save</b>.</li> <li>Click <b>Deploy All</b>.</li> </ol> <p>For more information, refer to the section <a href="#">Adding Certificate Authority</a></p>	Field	Action	Alias	Alias name of the CA.	File Upload	Choose the certificate from the desired location.
Field	Action							
Alias	Alias name of the CA.							
File Upload	Choose the certificate from the desired location.							
2.	Upload a SSL Key	<p>You must add a SSL key to GigaVUE V Series node. To add SSL Key, follow the steps in the section <a href="#">Upload SSL Keys</a>.</p>						
3	Create a secure tunnel between UCT-V and GigaVUE V Series Node 1.	<p>You should enable the secure tunnel feature to establish a connection between the UCT-V and GigaVUE V Series node 1. To enable the secure tunnel feature follow these steps:</p> <ol style="list-style-type: none"> <li>In the Edit Monitoring Session page, click <b>Options</b>. The <b>Apply template</b> page appears.</li> <li>Enable the <b>Secure Tunnel</b> button. You can enable secure tunnel for both mirrored and preencrypted traffic.</li> </ol>						
4.	Select the added SSL Key while creating a monitoring domain.	<p>Select the added SSL Key while creating a monitoring domain and configuring the fabric components in GigaVUE-FM in GigaVUE V Series Node 1.</p> <p>You must select the added SSL Key in GigaVUE V Series Node 1.</p> <p>To select the SSL key, follow the steps in the section <a href="#">Configure GigaVUE Fabric Components in GigaVUE-FM</a></p>						

S. No	Task	Refer to										
5.	Select the added CA certificate while creating the monitoring domain	You should select the added Certificate Authority (CA) in UCT-V Controller. To select the CA certificate, follow the steps in the section <a href="#">Configure GigaVUE Fabric Components in GigaVUE-FM</a>										
6	Create an Egress tunnel from GigaVUE V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session.	<p>You must create a tunnel for traffic to flow out from GigaVUE V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session. Refer to <a href="#">Create Ingress and Egress Tunnels</a> for more detailed information on how to create tunnels.</p> <p>To create the egress tunnel, follow these steps:</p> <ol style="list-style-type: none"> <li>1. After creating a new monitoring session, or click <b>Actions &gt; Edit</b> on an existing monitoring session, the GigaVUE-FM canvas appears.</li> <li>2. In the canvas, select <b>New &gt; New Tunnel</b>, drag and drop a new tunnel template to the workspace. The <b>Add Tunnel Spec</b> quick view appears.</li> <li>3. On the New Tunnel quick view, enter or select the required information as described in the following table:</li> </ol> <table border="1"> <thead> <tr> <th>Field</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Alias</td> <td>The name of the tunnel endpoint.</td> </tr> <tr> <td>Description</td> <td>The description of the tunnel endpoint.</td> </tr> <tr> <td>Type</td> <td>Select TLS-PCAPNG for creating egress secure tunnel</td> </tr> <tr> <td>Traffic Direction</td> <td> <p>Choose <b>Out</b> (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values:</p> <ul style="list-style-type: none"> <li>o MTU- The default value is 1500.</li> <li>o Time to Live - Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64.</li> <li>o DSCP - Enter the Differentiated Services Code Point (DSCP) value.</li> <li>o Flow Label - Enter the Flow Label value.</li> <li>o Source L4 Port- Enter the Souce L4 Port value</li> <li>o Destination L4 Port - Enter the Destination L4 Port value.</li> <li>o Flow Label</li> <li>o Cipher- Only SHA 256 is supported.</li> <li>o TLS Version - Select TLS Version1.3.</li> <li>o Selective Acknowledgments - Choose <b>Enable</b> to turn on the</li> </ul> </td> </tr> </tbody> </table>	Field	Action	Alias	The name of the tunnel endpoint.	Description	The description of the tunnel endpoint.	Type	Select TLS-PCAPNG for creating egress secure tunnel	Traffic Direction	<p>Choose <b>Out</b> (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values:</p> <ul style="list-style-type: none"> <li>o MTU- The default value is 1500.</li> <li>o Time to Live - Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64.</li> <li>o DSCP - Enter the Differentiated Services Code Point (DSCP) value.</li> <li>o Flow Label - Enter the Flow Label value.</li> <li>o Source L4 Port- Enter the Souce L4 Port value</li> <li>o Destination L4 Port - Enter the Destination L4 Port value.</li> <li>o Flow Label</li> <li>o Cipher- Only SHA 256 is supported.</li> <li>o TLS Version - Select TLS Version1.3.</li> <li>o Selective Acknowledgments - Choose <b>Enable</b> to turn on the</li> </ul>
Field	Action											
Alias	The name of the tunnel endpoint.											
Description	The description of the tunnel endpoint.											
Type	Select TLS-PCAPNG for creating egress secure tunnel											
Traffic Direction	<p>Choose <b>Out</b> (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values:</p> <ul style="list-style-type: none"> <li>o MTU- The default value is 1500.</li> <li>o Time to Live - Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64.</li> <li>o DSCP - Enter the Differentiated Services Code Point (DSCP) value.</li> <li>o Flow Label - Enter the Flow Label value.</li> <li>o Source L4 Port- Enter the Souce L4 Port value</li> <li>o Destination L4 Port - Enter the Destination L4 Port value.</li> <li>o Flow Label</li> <li>o Cipher- Only SHA 256 is supported.</li> <li>o TLS Version - Select TLS Version1.3.</li> <li>o Selective Acknowledgments - Choose <b>Enable</b> to turn on the</li> </ul>											

S. N o	Task	Refer to								
		<table border="1"> <thead> <tr> <th data-bbox="310 304 500 380">Field</th> <th data-bbox="500 304 1471 380">Action</th> </tr> </thead> <tbody> <tr> <td data-bbox="310 380 500 562"></td> <td data-bbox="500 380 1471 562">           TCP selective acknowledgments.           <ul style="list-style-type: none"> <li>o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6.</li> <li>o Delay Acknowledgments - Choose <b>Enable</b> to turn on delayed acknowledgments.</li> </ul> </td> </tr> <tr> <td data-bbox="310 562 500 611">IP Version</td> <td data-bbox="500 562 1471 611">The version of the Internet Protocol. Only IPv4 is supported.</td> </tr> <tr> <td data-bbox="310 611 500 686">Remote Tunnel IP</td> <td data-bbox="500 611 1471 686">Enter the interface IP address of the GigaVUE V Series Node 2 (Destination IP).</td> </tr> </tbody> </table> <p data-bbox="310 699 1471 737"><b>4.</b> Click <b>Save</b>.</p>	Field	Action		TCP selective acknowledgments. <ul style="list-style-type: none"> <li>o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6.</li> <li>o Delay Acknowledgments - Choose <b>Enable</b> to turn on delayed acknowledgments.</li> </ul>	IP Version	The version of the Internet Protocol. Only IPv4 is supported.	Remote Tunnel IP	Enter the interface IP address of the GigaVUE V Series Node 2 (Destination IP).
Field	Action									
	TCP selective acknowledgments. <ul style="list-style-type: none"> <li>o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6.</li> <li>o Delay Acknowledgments - Choose <b>Enable</b> to turn on delayed acknowledgments.</li> </ul>									
IP Version	The version of the Internet Protocol. Only IPv4 is supported.									
Remote Tunnel IP	Enter the interface IP address of the GigaVUE V Series Node 2 (Destination IP).									
7.	Select the added SSL Key while creating a monitoring domain and configuring the fabric components in GigaVUE-FM in GigaVUE V Series Node 2	You must select the added SSL Key in GigaVUE V Series Node 2. To select the SSL key, follow the steps in the section <a href="#">Configure GigaVUE Fabric Components in GigaVUE-FM</a>								
8	Create an ingress tunnel in the GigaVUE V	<p>You must create an ingress tunnel for traffic to flow in from GigaVUE V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session. Refer to <a href="#">Create a Monitoring Session</a> to know about monitoring session.</p> <p>To create the ingress tunnel, follow these steps:</p> <ol style="list-style-type: none"> <li><b>1.</b> After creating a new monitoring session, or click <b>Actions &gt; Edit</b> on an existing monitoring session, the GigaVUE-FM canvas appears.</li> </ol>								

S. No	Task	Refer to														
	Series Node 2 with tunnel type as TLS-PCAPNG while creating the monitoring session for GigaVUE Node 2.	<p><b>2.</b> In the canvas, select <b>New &gt; New Tunnel</b>, drag and drop a new tunnel template to the workspace. The <b>Add Tunnel Spec</b> quick view appears.</p> <p><b>3.</b> On the New Tunnel quick view, enter or select the required information as described in the following table:</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Alias</td> <td>The name of the tunnel endpoint.</td> </tr> <tr> <td>Description</td> <td>The description of the tunnel endpoint.</td> </tr> <tr> <td>Type</td> <td>Select TLS-PCAPNG for creating egress secure tunnel</td> </tr> <tr> <td>Traffic Direction</td> <td>Choose <b>In</b> (Decapsulation) for creating an ingress tunnel that receives traffic from V Series node 1. Select or enter the values as described in Step 6.</td> </tr> <tr> <td>IP Version</td> <td>The version of the Internet Protocol. Only IPv4 is supported.</td> </tr> <tr> <td>Remote Tunnel IP</td> <td>Enter the interface IP address of the GigaVUE Cloud Suite V Series Node 1 (Destination IP).</td> </tr> </tbody> </table> <p><b>4.</b> Click <b>Save</b>.</p>	Field	Action	Alias	The name of the tunnel endpoint.	Description	The description of the tunnel endpoint.	Type	Select TLS-PCAPNG for creating egress secure tunnel	Traffic Direction	Choose <b>In</b> (Decapsulation) for creating an ingress tunnel that receives traffic from V Series node 1. Select or enter the values as described in Step 6.	IP Version	The version of the Internet Protocol. Only IPv4 is supported.	Remote Tunnel IP	Enter the interface IP address of the GigaVUE Cloud Suite V Series Node 1 (Destination IP).
Field	Action															
Alias	The name of the tunnel endpoint.															
Description	The description of the tunnel endpoint.															
Type	Select TLS-PCAPNG for creating egress secure tunnel															
Traffic Direction	Choose <b>In</b> (Decapsulation) for creating an ingress tunnel that receives traffic from V Series node 1. Select or enter the values as described in Step 6.															
IP Version	The version of the Internet Protocol. Only IPv4 is supported.															
Remote Tunnel IP	Enter the interface IP address of the GigaVUE Cloud Suite V Series Node 1 (Destination IP).															

You can also configure Secure Tunnels when using Application Intelligence Session. Refer to [Configure Application Intelligence Solutions on GigaVUE V Series Nodes for Azure](#) for more detailed information on how to enable secure tunnels when using Application Intelligence.

## Viewing Status of Secure Tunnel

GigavUE-FM allows you to view the status of secure tunnel connection in UCT-C. You can verify whether the tunnel is connected to the tool or V Series node through the status.

To verify the status of secure tunnel, go to **UCT-C > Monitoring Domain**. In the monitoring domain page, **Tunnel status** column shows the status of the tunnel. The green color represents that the tunnel is connected and the red represents that the tunnel is not connected.

For configuring secure tunnel, refer to **Configure Secure Tunnel** section.

## Preryption™

**License:** Requires **SecureVUE Plus** license.

Gigamon Precryption™ technology<sup>1</sup> redefines security for virtual, cloud, and containerized applications, delivering plaintext visibility of encrypted communications to the full security stack, without the traditional cost and complexity of decryption.

This section explains about:

- [How Gigamon Precryption Technology Works](#)
- [Why Gigamon Precryption](#)
- [Key Features](#)
- [Key Benefits](#)
- [Precryption Technology on Single Node](#)
- [Precryption Technology on Multi-Node](#)
- [Supported Platforms](#)
- [Prerequisites](#)

## How Gigamon Precryption Technology Works

Precryption technology leverages native Linux functionality to tap, or copy, communications between the application and the encryption library, such as OpenSSL.



In this way, Precryption captures network traffic in plaintext, either before it has been encrypted, or after it has been decrypted. Precryption functionality doesn't interfere with the actual encryption of the message nor its transmission across the network. There's no proxy,

---

**Disclaimer:** The Precryption feature allows users to acquire traffic after it has been decrypted. This traffic can be acquired from both virtual machine (VM) and container-based solutions, and is then sent to the V Series product for further processing. The Precryption feature provides an option to use encrypted tunnels for communication between the acquisition (via UCT or G-vTAP) of unencrypted traffic and the traffic processing (at the V Series) which will better safeguard the traffic while in transit. However, if a user does not use the option for encrypted tunnels for communication, decrypted traffic will remain unencrypted while in transit between the point of acquisition and processing.

Please note that this information is subject to change, and we encourage you to stay updated on any modifications or improvements made to this feature.

By using this feature, you acknowledge and accept the current limitations and potential risks associated with the transmission of decrypted traffic.

no retransmissions, no break-and-inspect. Instead, this plaintext copy is forwarded to the Gigamon Deep Observability Pipeline for further optimization, transformation, replication, and delivery to tools.

Preryption technology is built on GigaVUE® Universal Cloud Tap (UCT) and works across hybrid and multi-cloud environments, including on-prem and virtual platforms. As a bonus, UCT with Preryption technology runs independent of the application, and doesn't have to be baked into the application development lifecycle.

## Why Gigamon Preryption

GigaVUE Universal Cloud Tap with Preryption technology is a lightweight, friction-free solution that eliminates blind spots present in modern hybrid cloud infrastructure, providing East-West visibility into virtual, cloud, and container platforms. It delivers unobscured visibility into all encryption types including TLS 1.3, without managing and maintaining decryption keys. IT organizations can now manage compliance, keep private communications private, architect the necessary foundation for Zero Trust, and boost security tool effectiveness by a factor of 5x or more.

## Key Features

The following are the key features of this technology:

- Plaintext visibility into communications with modern encryption (TLS 1.3, mTLS, and TLS 1.2 with Perfect Forward Secrecy).
- Plaintext visibility into communications with legacy encryption (TLS 1.2 and earlier).
- Nonintrusive traffic access without agents running inside container workloads.
- Elimination of expensive resource consumption associated with traditional traffic decryption.
- Elimination of key management required by traditional traffic decryption.
- Zero performance impact based on cipher type, strength, or version.
- Support across hybrid and multi-cloud environments, including on-prem, virtual, and container platforms.
- Keep private communications private across the network with plaintext threat activity delivered to security tools.
- Integration with Gigamon Deep Observability Pipeline for the full suite of optimization, transformation, and brokering capabilities.

## Key Benefits

The following are the key benefits of this technology:



- Eliminate blind spots for encrypted East-West (lateral) and North-South communications, including traffic that may not cross firewalls.
- Monitor application communications with an independent approach that enhances development team velocity.
- Extend security tools' visibility to all communications, regardless of encryption type.
- Achieve maximum traffic tapping efficiency across virtual environments.
- Leverage a 5–7x performance boost for security tools by consuming unencrypted data.
- Support a Zero Trust architecture founded on deep observability.
- Maintain privacy and compliance adherence associated with decrypted traffic management.

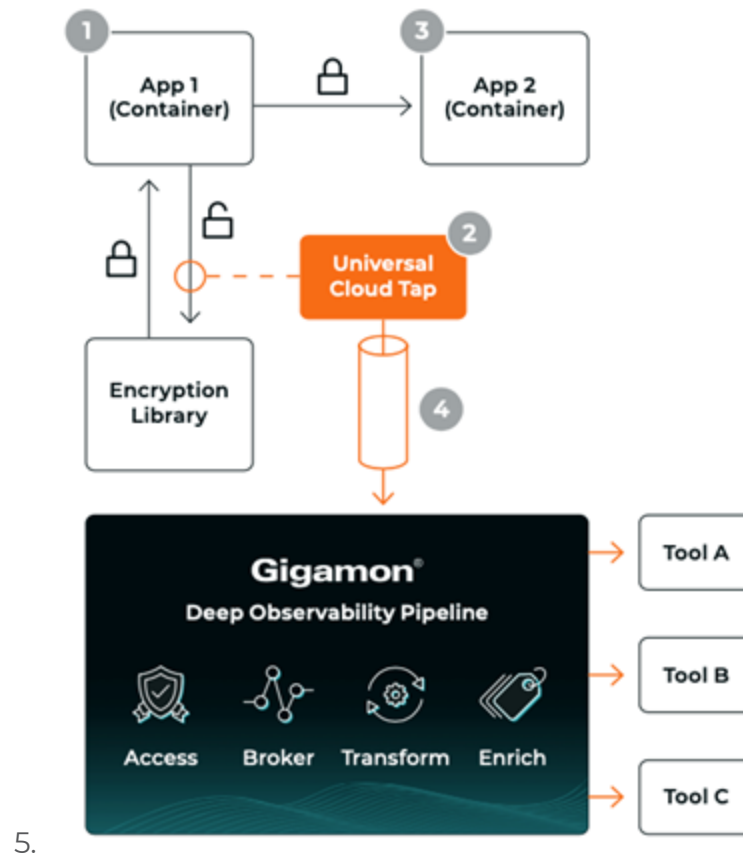
## How Gigamon Precryption Technology Works

This section explains about how Precryption technology works on single node and multiple node in the following sections:

- [Precryption Technology on Single Node](#)
- [Precryption Technology on Multi-Node](#)

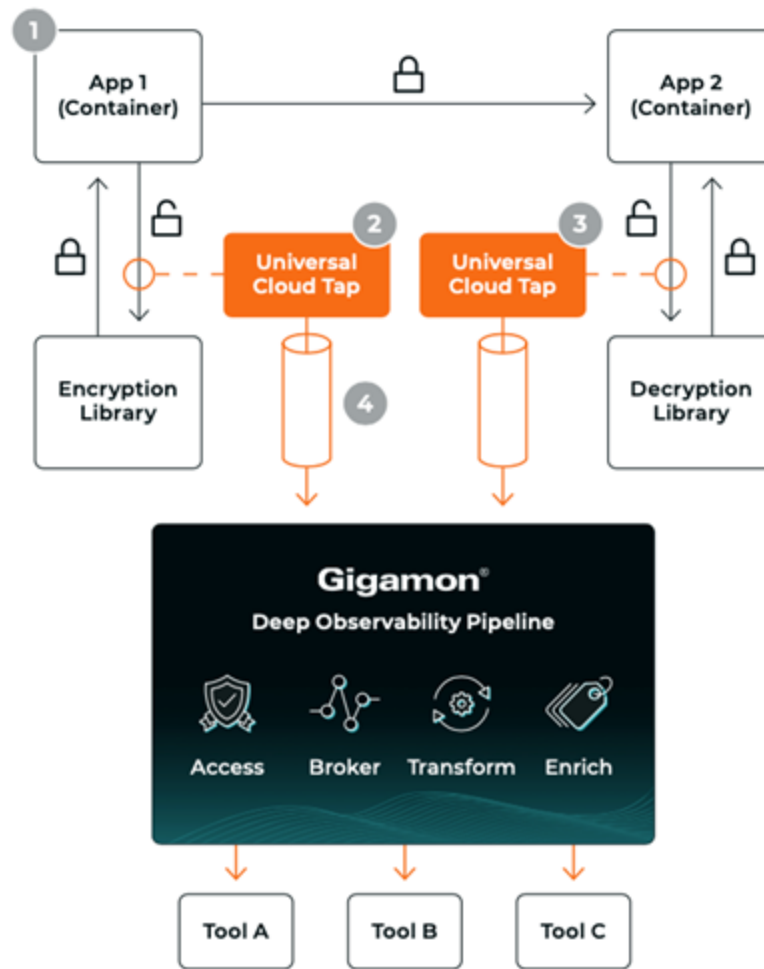
### Precryption Technology on Single Node

1. When any application needs to encrypt a message, it uses an encryption library, such as OpenSSL, to perform the actual encryption.
2. GigaVUE Universal Cloud Tap (UCT), enabled with Precryption technology, gets a copy of this message before it's encrypted on the network.
3. The encrypted message is sent to the receiving application, with unmodified encryption. No proxy, no re- encryption, no retransmissions.
4. GigaVUE UCT creates packet headers as needed, encapsulates in a tunnel, and forwards to GigaVUE V Series in the deep observability pipeline. Gigamon further optimizes, transforms, and delivers data to tools, without need for further decryption



## Pre-encryption Technology on Multi-Node

1. When any application needs to encrypt a message, it uses an encryption library, such as OpenSSL, to perform the actual encryption.
2. GigaVUE Universal Cloud Tap (UCT), enabled with Pre-encryption, gets a copy of this message before it's encrypted on the network.
3. Optionally, GigaVUE UCT enabled with Pre-encryption can also acquire a copy of the message from the server end, after the decryption.
4. GigaVUE UCT creates packet headers as needed, encapsulates in a tunnel, and forwards to V Series in the deep observability pipeline where it is further enriched, transformed, and delivered to tools, without further decryption.



5.

## Supported Platforms

**VM environments:** Precryption™ is supported on the following VM platforms where UCT-V is supported:

Platform Type	Platform
Public Cloud	<ul style="list-style-type: none"> <li>● AWS</li> <li>● Azure</li> <li>● GCP (via Third Party Orchestration)</li> </ul>
Private Cloud	<ul style="list-style-type: none"> <li>● OpenStack</li> <li>● VMware ESXi (via Third Party Orchestration only)</li> <li>● VMware NSX-T (via Third Party Orchestration only)</li> </ul>

**Container environments:** Precryption™ is supported on the following container platforms where UCT-C is supported:

Platform Type	Platform
Public Cloud	<ul style="list-style-type: none"> <li>● EKS</li> <li>● AKS</li> </ul>
Private Cloud	<ul style="list-style-type: none"> <li>● OpenShift</li> <li>● Native Kubernetes (VMware)</li> </ul>

## Prerequisites

### Deployment Prerequisites

- Linux Kernel version 5.4 and above
- OpenSSL version 1.0.2, version 1.1.0, version 1.1.1, and version 3.x
- Protocol version IPv4
- For GigaVUE-FM, to capture the statistics, you must add the port 5671 in the security group
- Port 9900 should be enabled in security group settings on the UCT-V controller to receive the statistics information from UCT-V agent
- For UCT-C, you must add the port 42042 and port 5671 in the security group

### License Prerequisite

- Precryption™ requires SecureVUE Plus license.

### Note

- See the [Configure Precryption in UCT-V](#) section for details on how to enable Precryption™ in VM environments.
- See the [Configure in UCT-C](#) section for details on how to enable Precryption™ in container environments.
- See how [Secure Tunnels](#) feature can enable secure delivery of precrypted data.

## Configure Precryption in UCT-V

GigaVUE-FM allows you to enable or disable the Precryption feature for a monitoring session.

To enable or disable the Precryption feature in UCT-V, refer to Create monitoring session.

To create a new monitoring session with Precryption, follow these steps:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Click **New** to open the **Create a New Monitoring Session** page.
3. Enter the appropriate information for the monitoring session as described in the following table:

Field	Description
<b>Alias</b>	The name of the monitoring session.
<b>Monitoring Domain</b>	The name of the monitoring domain that you want to select.
<b>Connection</b>	The connection(s) that are to be included as part of the monitoring domain. You can select the required connections that need to be part of the monitoring domain.

4. Click **Next**. The **Edit Monitoring Session** page appears with the new canvas.
5. Click **Options** button. The Monitoring Session Options appears.
6. Enable **Preryption**.
7. Click **Save**. The **Edit Monitoring Session** page appears. You can proceed to create map, tunnels, and adding applications.

**NOTE:** It is recommended to enable the secure tunnel feature whenever the Preryption feature is enabled. Secure tunnel helps to securely transfer the cloud captured packets or prerypted data to a GigaVUE V Series Node. For more information, refer to Secure Tunnel .

## Validate Preryption connection

To validate the Preryption connection, follow the steps:

- To confirm it is active, navigate to the **Monitoring Session** dashboard and check the Preryption option, which should show **yes**.
- Click **Status**, to view the rules configured.

## Rules and Notes

- To avoid packet fragmentation, you should change the option preryption-path-mtu in UCT-V configuration file (**/etc/uctv/uctv.conf**) within the range 1400-9000 based on the platform path MTU.

# 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:

### **For V Series Nodes:**

- AWS
- Azure
- OpenStack
- VMware
- Nutanix

### **For UCT-Vs:**

- AWS
- Azure
- OpenStack

### **For VPC Mirroring:**

- AWS

### **For OVS Mirroring and VLAN Trunk Port:**

- OpenStack

To view the configuration health status, refer to the [Configuration Health Monitoring](#) 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 [Configuration Settings](#) 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

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

- [Create Threshold Template](#)
- [Apply Threshold Template](#)
- [Edit Threshold Template](#)
- [Clear Thresholds](#)
- [Supported Resources and Metrics](#)

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 or undeploying the monitoring session will clear all the threshold policies associated with that monitoring session.
- After applying threshold template to a particular application, you need not deploy the monitoring session again.

## Create Threshold Template

To create threshold templates:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. Then, click on the **Threshold Template** tab in the top navigation bar.
2. The **Threshold Template** 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
<b>Threshold Template Name</b>	The name of the threshold template.
<b>Thresholds</b>	
Monitored Objects	Select the resource for which you wish to apply the threshold template. Eg: TEP, REP, Maps, Applications like Slicing, Dedup etc
Time Interval	Frequency at which the traffic flow needs to be monitored.
Metric	Metrics that needs to be monitored. For example: Tx Packets, Rx Packets.
Type	<b>Difference:</b> The difference between the stats counter at the start and end time of an interval, for a given metric. <b>Derivative:</b> Average value of the statistics counter in a time interval, for a given metric.
Condition	<b>Over:</b> Checks if the statistics counter value is greater than the 'Set Trigger Value'. <b>Under:</b> 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 Template** 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. Select the monitoring session and click **Actions > Apply Thresholds**.
3. The **Apply Thresholds** page appears. To apply a threshold template across a monitoring session, select the template you wish to apply across the monitoring session from the Threshold Template drop-down menu or enter the threshold values manually.
4. Click **Done**.

## 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 **Actions > Edit**. The Edit Monitoring Session page with 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**.

## Edit Threshold Template

To edit a particular threshold template follow the steps given below:

1. On the Threshold Template page, Click **Edit**. The **Edit Threshold Template** page appear.
2. The existing threshold templates will be listed here. Edit the templates you wish to modify.
3. Click **Save**.

**NOTE:** Editing a threshold template does not automatically apply the template to monitoring session. You must apply the edited template to monitoring session for the changes to take effect.

## 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 **Actions > Edit**. The Edit Monitoring Session page with 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, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Select the monitoring session and click **Actions > Apply Thresholds**.
3. The **Apply Thresholds page appears**. Click **Clear**.

**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](#)

## 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	<ol style="list-style-type: none"> <li>1. Tx Packets</li> <li>2. Rx Packets</li> <li>3. Tx Bytes</li> <li>4. Rx Bytes</li> <li>5. Tx Dropped</li> <li>6. Rx Dropped</li> <li>7. Tx Errors</li> <li>8. Rx Errors</li> </ol>	<ol style="list-style-type: none"> <li>1. Difference</li> <li>2. Derivative</li> </ol>	<ol style="list-style-type: none"> <li>1. Over</li> <li>2. Under</li> </ol>

RawEnd Point	<ol style="list-style-type: none"> <li>1. Tx Packets</li> <li>2. Rx Packets</li> <li>3. Tx Bytes</li> <li>4. Rx Bytes</li> <li>5. Tx Dropped</li> <li>6. Rx Dropped</li> <li>7. Tx Errors</li> <li>8. Rx Errors</li> </ol>	<ol style="list-style-type: none"> <li>1. Difference</li> <li>2. Derivative</li> </ol>	<ol style="list-style-type: none"> <li>1. Over</li> <li>2. Under</li> </ol>
Map	<ol style="list-style-type: none"> <li>1. Tx Packets</li> <li>2. Rx Packets</li> <li>3. Packets Dropped</li> </ol>	<ol style="list-style-type: none"> <li>1. Difference</li> <li>2. Derivative</li> </ol>	<ol style="list-style-type: none"> <li>1. Over</li> <li>2. Under</li> </ol>
Slicing	<ol style="list-style-type: none"> <li>1. Tx Packets</li> <li>2. Rx Packets</li> <li>3. Packets Dropped</li> </ol>	<ol style="list-style-type: none"> <li>1. Difference</li> <li>2. Derivative</li> </ol>	<ol style="list-style-type: none"> <li>1. Over</li> <li>2. Under</li> </ol>
Masking	<ol style="list-style-type: none"> <li>1. Tx Packets</li> <li>2. Rx Packets</li> <li>3. Packets Dropped</li> </ol>	<ol style="list-style-type: none"> <li>1. Difference</li> <li>2. Derivative</li> </ol>	<ol style="list-style-type: none"> <li>1. Over</li> <li>2. Under</li> </ol>
Dedup	<ol style="list-style-type: none"> <li>1. Tx Packets</li> <li>2. Rx Packets</li> <li>3. Packets Dropped</li> </ol>	<ol style="list-style-type: none"> <li>1. Difference</li> <li>2. Derivative</li> </ol>	<ol style="list-style-type: none"> <li>1. Over</li> <li>2. Under</li> </ol>
HeaderStripping	<ol style="list-style-type: none"> <li>1. Tx Packets</li> <li>2. Rx Packets</li> <li>3. Packets Dropped</li> </ol>	<ol style="list-style-type: none"> <li>1. Difference</li> <li>2. Derivative</li> </ol>	<ol style="list-style-type: none"> <li>1. Over</li> <li>2. Under</li> </ol>
TunnelEncapsulation	<ol style="list-style-type: none"> <li>1. Tx Packets</li> <li>2. Rx Packets</li> <li>3. Packets Dropped</li> </ol>	<ol style="list-style-type: none"> <li>1. Difference</li> <li>2. Derivative</li> </ol>	<ol style="list-style-type: none"> <li>1. Over</li> <li>2. Under</li> </ol>
LoadBalancing	<ol style="list-style-type: none"> <li>1. Tx Packets</li> <li>2. Rx Packets</li> <li>3. Packets Dropped</li> </ol>	<ol style="list-style-type: none"> <li>1. Difference</li> <li>2. Derivative</li> </ol>	<ol style="list-style-type: none"> <li>1. Over</li> <li>2. Under</li> </ol>
SSLDecryption	<ol style="list-style-type: none"> <li>1. Tx Packets</li> <li>2. Rx Packets</li> <li>3. Packets Dropped</li> </ol>	<ol style="list-style-type: none"> <li>1. Difference</li> <li>2. Derivative</li> </ol>	<ol style="list-style-type: none"> <li>1. Over</li> <li>2. Under</li> </ol>

Application Metadata	<ol style="list-style-type: none"> <li>1. Tx Packets</li> <li>2. Rx Packets</li> <li>3. Packets Dropped</li> </ol>	<ol style="list-style-type: none"> <li>1. Difference</li> <li>2. Derivative</li> </ol>	<ol style="list-style-type: none"> <li>1. Over</li> <li>2. Under</li> </ol>
AMI Exporter	<ol style="list-style-type: none"> <li>1. Tx Packets</li> <li>2. Rx Packets</li> <li>3. Packets Dropped</li> </ol>	<ol style="list-style-type: none"> <li>1. Difference</li> <li>2. Derivative</li> </ol>	<ol style="list-style-type: none"> <li>1. Over</li> <li>2. Under</li> </ol>
Geneve	<ol style="list-style-type: none"> <li>1. Tx Packets</li> <li>2. Rx Packets</li> <li>3. Packets Dropped</li> </ol>	<ol style="list-style-type: none"> <li>1. Difference</li> <li>2. Derivative</li> </ol>	<ol style="list-style-type: none"> <li>1. Over</li> <li>2. Under</li> </ol>
5G-SBI	<ol style="list-style-type: none"> <li>1. Tx Packets</li> <li>2. Rx Packets</li> <li>3. Packets Dropped</li> </ol>	<ol style="list-style-type: none"> <li>1. Difference</li> <li>2. Derivative</li> </ol>	<ol style="list-style-type: none"> <li>1. Over</li> <li>2. Under</li> </ol>

## 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 the Entire Monitoring Session

To view the health status of a monitoring session:

1. On the Monitoring Session details page, click on the health status displayed in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed, click on the Status displayed in the top left-corner above the canvas. The quick view page appears.

This displays the configuration health and traffic health of the monitoring session and also the thresholds applied to that monitoring session.

### View Health Status of an Application

To view the health status of an application across an entire monitoring session:

1. On the Monitoring Session page, click on the health status displayed in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed.

3. To view application health, click on the application for which you wish to see the health status. The quick view page appears.
4. Click on the **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 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 on the health status in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed. Select the V Series Node from the **View By** drop-down menu and then click on the Status displayed in the top left-corner above the canvas. The quick view page appears.

## View Application Health Status for Individual V Series Nodes

To view the application configuration and traffic health status of the GigaVUE V Series Nodes:

1. On the Monitoring Session page, click on the health status in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed. Select the V Series Node from the **View By** drop-down menu.
3. To view application health, click on the application for which you wish to see the health status. The quick view page appears.
4. Click on the **Status** tab.

The subsession toggle button available in the top-left corner of the canvas allows you to view the statistics of individual paths in the monitoring session. If the traffic health is not configured for monitoring session or a particular application, the traffic health is displayed as **Not Applicable**.

You can also view the cloud health Status in the Monitoring Session Page, refer to [View Health Status on the Monitoring Session Page](#) topic for more detailed information on how to view cloud health status in the Monitoring Session page.

# Fabric Health Analytics for Virtual Resources

Fabric Health Analytics (FHA) in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using FHA<sup>1</sup> 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 FHA. Dashboards, Visualizations and Search Objects are called FHA objects. Refer to [Fabric Health Analytics](#) topic in *GigaVUE Fabric Management Guide* for more detailed information on Fabric Health 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 for more details.
- Use the Time Filter option to select the required time interval for which you need to view the visualization.

## Virtual Inventory Statistics and Cloud Applications Dashboard

Fabric Health Analytics dashboards allow users to monitor the physical and virtual environment and detect anomalous behavior and plan accordingly. Refer to the [Fabric Health 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:

---

<sup>1</sup>FHA uses the Kibana front-end application to visualize and analyze the data in the Elasticsearch database of GigaVUE-FM. Kibana is an open source data visualization plugin for Elasticsearch.

Dashboard	Displays	Visualizations	Displays
<b>Inventory Status (Virtual)</b>	<p>Statistical details of the virtual inventory based on the platform and the health status.</p> <p>You can view the following metric details at the top of the dashboard:</p> <ul style="list-style-type: none"> <li>● Number of Monitoring Sessions</li> <li>● Number of V Series Nodes</li> <li>● Number of Connections</li> <li>● Number of GCB Nodes</li> </ul> <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> <li>● Platform</li> <li>● Health Status</li> </ul>	<i>V Series Node Status by Platform</i>	Number of healthy and unhealthy V Series Nodes for each of the supported cloud platforms.
		<i>Monitoring Session Status by Platform</i>	Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms
		<i>Connection Status by Platform</i>	Number of healthy and unhealthy connections for each of the supported cloud platforms
		<i>GCB Node Status by Platform</i>	Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms
<b>V Series Node Statistics</b>	<p>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.</p> <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> <li>● Platform</li> <li>● Connection</li> <li>● V Series Node</li> </ul>	<i>V Series Node Maximum CPU Usage Trend</i>	<p>Line chart that displays maximum CPU usage trend of the V Series node in 5 minutes interval, for the past one hour.</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #e6f2ff;"> <p><b>NOTE:</b> The maximum CPU Usage trend refers to the CPU usage for service cores only. Small form factor V-series nodes do not have service cores, therefore the CPU usage is reported as 0.</p> </div>
		<i>V Series Node with Most CPU Usage For Past 5 minutes</i>	<p>Line chart that displays Maximum CPU usage of the V Series node for the past 5 minutes.</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #e6f2ff;"> <p><b>NOTE:</b> You cannot use the time based filter</p> </div>

Dashboard	Displays	Visualizations	Displays
			options to filter and visualize the data.
		<i>V Series Node Rx Trend</i>	Receiving trend of the V Series node in 5 minutes interval, for the past one hour.
		<i>V Series Network Interfaces with Most Rx for Past 5 mins</i>	Total packets received by each of the V Series network interface for the past 5 minutes.  <b>NOTE:</b> You cannot use the time based filter options to filter and visualize the data.
		<i>V Series Node Tunnel Rx Packets/Errors</i>	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.
		<i>V Series Node Tunnel Tx Packets/Errors</i>	TX is for output tunnels from VSN. V Series Node Tunnel Tx Packets/Errors
<b>Dedup</b>	Displays visualizations related to Dedup application.  You can filter the visualizations based on the following control filters: <ul style="list-style-type: none"> <li>Platform</li> <li>Connection</li> <li>VSeries Node</li> </ul>	<i>Dedup Packets Detected/Dedup Packets Overload</i>	Statistics of the total dedup packets received (ipV4Dup, ipV6Dup and nonIPDup) against the dedup application overload.
		<i>Dedup Packets Detected/Dedup Packets Overload Percentage</i>	Percentage of the dedup packets received against the dedup application overload.
		<i>Total Traffic In/Out Dedup</i>	Total incoming traffic against total outgoing traffic



Dashboard	Displays	Visualizations	Displays
<b>Tunnel (Virtual)</b>	<p>Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets.</p> <p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> <li>• <b>Monitoring session:</b> 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.</li> <li>• <b>V series node:</b> Management IP of the V Series node. Choose the required V-series node from the drop-down.</li> <li>• <b>Tunnel:</b> Select any of the tunnels shown in the Tunnel drop-down. The direction for each tunnel is shown with the prefix in or out.</li> </ul> <p>The following statistics are displayed for the tunnel:</p> <ul style="list-style-type: none"> <li>• Received Bytes</li> <li>• Transmitted Bytes</li> <li>• Received Packets</li> <li>• Transmitted Packets</li> <li>• Received Errored Packets</li> <li>• Received Dropped Packets</li> <li>• Transmitted Errored Packets</li> <li>• Transmitted Dropped Packets</li> </ul>	<i>Tunnel Bytes</i>	<p>Displays received tunnel traffic vs transmitted tunnel traffic, in bytes.</p> <ul style="list-style-type: none"> <li>• For input tunnel, transmitted traffic is displayed as zero.</li> <li>• For output tunnel, received traffic is displayed as zero.</li> </ul>
		<i>Tunnel Packets</i>	Displays packet-level statistics for input and output tunnels that are part of a monitoring session.
<b>App (Virtual)</b>	Displays Byte and packet level statistics for the applications for the chosen monitoring session on the selected V series node.	<i>App Bytes</i>	Displays received traffic vs transmitted traffic, in Bytes.

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

Dashboard	Displays	Visualizations	Displays
	<p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> <li>• <b>Monitoring session</b></li> <li>• <b>V Series node</b></li> <li>• <b>Endpoint:</b> Management IP of the V Series node followed by the Network Interface (NIC)</li> </ul>		
		<i>Endpoint Packets</i>	Displays received traffic vs transmitted traffic, as the number of packets.

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

# Administer GigaVUE Cloud Suite for Azure

You can perform the following administrative tasks:

- [Set Up Email Notifications](#)
- [Configure Proxy Server](#)
- [Configure Azure Settings](#)
- [Role Based Access Control](#)
- [About Events](#)
- [About Audit Logs](#)

## Set Up Email Notifications

Notifications are triggered by a range of events such as Azure license expiry, VM instance terminated, and so on. You can setup the email notification for a particular event or a number of events and the recipient or recipients to whom the email should be sent.

Gigamon strongly recommends you enable email notifications so there is immediate visibility of the events affecting node health. The following are the events for which you can setup the email notifications:

- Azure License Expire
- Fabric Node Down
- Fabric Node Reboot Failed
- Fabric Node Rebooted
- Fabric Node Replacement Launch Failed
- Fabric Node Replacement Launched
- Fabric Node Restart Failed
- Fabric Node Restarted
- Fabric Node Unreachable
- Fabric Node Up

## Configure Email Notifications

To configure the automatic email notifications:

1. On left navigation pane, select **System > Event Notifications > Email Servers**. The **Email Servers** page appears.

- In the Email Servers page, click **Configure**. The **Configure Email Server** wizard appears. For field information, refer to "Email Servers" section in the *GigaVUE Administration Guide*.

## Configure Email Server

Save

Cancel

Enable SMTP Authentication	<input type="checkbox"/>
Email Host	10.10.1.125
Username	Username
Password	Password
From Email	no-reply@gigavue-fm
Port	25

- Click **Save**.

## Configure Proxy Server

Sometimes, the VNet in which the GigaVUE-FM is launched may not have access to the Internet. Without Internet access, GigaVUE-FM cannot connect to the Azure API endpoints. For GigaVUE-FM to connect to Azure, a proxy server must be configured.

To create a proxy server:

1. Go to **Inventory > VIRTUAL > Azure**, and then click **Settings > Proxy Server Configuration**. The Proxy Server Configuration page appears.
2. In the **Proxy Server Configuration** page, click **Add**. The **Configure Proxy Server** page appears.

Configure Proxy Server

Save

Cancel

<b>Alias</b>	Alias
<b>Host</b>	IP Address
<b>Port</b>	0 - 65535
<b>Username</b>	Username
<b>Password</b>	Password

 NTLM

3. Select or enter the appropriate information as described in the following table.

Field	Description
<b>Alias</b>	The name of the proxy server.
<b>Host</b>	The host name or the IP address of the proxy server.
<b>Port</b>	The port number used by the proxy server for connecting to the Internet.
<b>Username</b>	(Optional) The username of the proxy server.
<b>Password</b>	The password of the proxy server.
<b>NTLM</b>	(Optional) The type of the proxy server used to connect to the VNet.
<b>Domain</b>	The domain name of the client accessing the proxy server.
<b>Workstation</b>	(Optional) The name of the workstation or the computer accessing the proxy server.

4. Click **Save**. The new proxy server configuration is added to the Proxy Server Configuration page. The proxy server is also listed in the Azure Connection page in GigaVUE-FM.

**NOTE:** If you change any of the fields in the Proxy Server Configuration page after the initial connection is established between the GigaVUE-FM and Azure, then you must also edit the connection and select the proxy server again and save (in the Azure Connection Page). Otherwise, GigaVUE-FM will not use the new configuration that was saved and may be disconnected from the Azure platform.

## Configure Azure 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.

Go to **Inventory > VIRTUAL > Azure**, and then click **Settings > Advanced Settings** to edit the Azure settings.

Edit

Refresh interval for VM target selection inventory (secs)	120
Refresh interval for fabric deployment inventory (secs)	900
Number of G-vTap Agents per V Series Node	100
Refresh interval for G-vTAP agent inventory (secs)	900

Refer to the following table for more information about the settings:

Settings	Description
<b>Refresh interval for VM target selection inventory(secs)</b>	Specifies the frequency for updating the state of Virtual Machines target selection in Azure.
<b>Refresh interval for fabric deployment inventory (secs)</b>	Specifies the frequency for updating the state of fabric deployment information such as subnets, security groups, images, and VNETs.
<b>Number of UCT-Vs per GigaVUE V Series Node</b>	Specifies the maximum number of instances that can be assigned to the GigaVUE V Series node.
<b>Refresh interval for UCT-V inventory (secs)</b>	Specifies the frequency for discovering the UCT-Vs available in the VNet.
<b>Traffic distribution tunnel range start</b>	Specifies the start range value of the tunnel ID.
<b>Traffic distribution tunnel range end</b>	Specifies the closing range value of the tunnel ID.

## Role Based Access Control

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

which the access rights of a user depends on the following:

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

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

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

**NOTE:** Cloud APIs are also RBAC enabled.

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



## About Events

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

- Cloud provider License Expiry
- UCT-V Inventory Update Completed
- Cloud provider Connection Status Changed

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

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

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

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

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

Controls/ Parameters	Description
<b>Source</b>	The source from where the events are generated. The criteria can be as follows: <ul style="list-style-type: none"> <li>FM - indicates the event was flagged by the Fabric Manager.</li> <li>IP address - is the address of the GigaVUE HC Series or GigaVUE Cloud Suite G Series node that detected the event. For a node to be able to send notifications to the Fabric Manager, the SNMP_TRAP must be configured with the Fabric Manager's IP address specified as a host. Refer to the GigaVUE Administration Guide for instructions on adding a destination for SNMP traps.</li> <li>VMM - indicates the event was flagged by the Virtual Machine Manager.</li> <li>FM Health - indicates the event was flagged due to the health status change of GigaVUE-FM.</li> </ul>
<b>Time</b>	The timestamp when the event occurred. <b>IMPORTANT:</b> Timestamps are shown in the time zone of the client browser's computer and not the time zone of the node reporting the event. The timestamp is based on the correctly configured clock on the GigaVUE-FM server and converted from UTC to the client computer's configured time zone.
<b>Event Type</b>	The type of event that generated the events. The type of events can be CPU utilization high, cluster updated, device discovery failed, fan tray changed, netflow statistics, and so on.
<b>Severity</b>	The severity is one of Critical, Major, Minor, or Info. Info is informational messages. For example, when power status change notification is displayed, then the message is displayed as Info.
Affected Entity Type	The resource type associated with the event. For example, when low disk space notification is generated, 'Chassis' is displayed as the affected entity type.
Affected Entity	The resource ID of the affected entity type. For example, when low disk space notification is generated, the IP address of the node with the low disk space is displayed as the affected entity.
Alias	Event Alias
Device IP	The IP address of the device.
Host Name	The host name of the device.
<b>Scope</b>	The category to which the events belong. Events can belong to the following category: Domain, Node, Card, Port, Stack, Cluster, Chassis, GigaVUE-FM, GigaVUE-VM, and so on. For example, if there is a notification generated for port utilization low threshold, the scope is displayed as Physical Node.

To filter the alarms and event:

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

## About Audit Logs

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

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

**All Audit Logs** Filter Manage

Filter : none

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

Go to page: 1 of 16 Total Records: 106

The Audit Logs have the following parameters:

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

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

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

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

To filter the audit logs, do the following:

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

# Additional Sources of Information

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

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

## Documentation

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

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

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.4 Hardware and Software Guides
<p><b>DID YOU KNOW?</b> 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 <b>Edit &gt; Advanced Search</b> from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.</p>
<p><b>Hardware</b></p> <p>how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices</p>
<b>GigaVUE-HC1 Hardware Installation Guide</b>
<b>GigaVUE-HC2 Hardware Installation Guide</b>
<b>GigaVUE-HC3 Hardware Installation Guide</b>
<b>GigaVUE-HC1-Plus Hardware Installation Guide</b>
<b>GigaVUE-TA25 Hardware Installation Guide</b>
<b>GigaVUE-TA25E Hardware Installation Guide</b>
<b>GigaVUE-TA100 Hardware Installation Guide</b>

## GigaVUE Cloud Suite 6.4 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 Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW**

### Software Installation and Upgrade Guides

**GigaVUE-FM Installation, Migration, and Upgrade Guide**

**GigaVUE-OS Upgrade Guide**

**GigaVUE V Series Migration Guide**

### Fabric Management and Administration Guides

**GigaVUE Administration Guide**

covers both GigaVUE-OS and GigaVUE-FM

**GigaVUE Fabric Management Guide**

how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features

### Cloud Guides

how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms

**GigaVUE V Series Applications Guide**

**GigaVUE V Series Quick Start Guide**

**GigaVUE Cloud Suite Deployment Guide - AWS**

**GigaVUE Cloud Suite Deployment Guide - Azure**

**GigaVUE Cloud Suite Deployment Guide - OpenStack**

**GigaVUE Cloud Suite Deployment Guide - Nutanix**

**GigaVUE Cloud Suite Deployment Guide - VMware**

**GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration**

**Universal Cloud Tap - Container Deployment Guide**

**Gigamon Containerized Broker Deployment Guide**

## GigaVUE Cloud Suite 6.4 Hardware and Software Guides

### GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide

GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions

### Reference Guides

#### GigaVUE-OS CLI Reference Guide

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

#### GigaVUE-OS Security Hardening Guide

#### GigaVUE Firewall and Security Guide

#### GigaVUE Licensing Guide

#### GigaVUE-OS Cabling Quick Reference Guide

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

#### GigaVUE-OS Compatibility and Interoperability Matrix

compatibility information and interoperability requirements for Gigamon devices

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

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

### Release Notes

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

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

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

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

### In-Product Help

#### GigaVUE-FM Online Help

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

## How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

## Documentation Feedback

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

[documentationfeedback@gigamon.com](mailto: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		
<b>About You</b>	<b>Your Name</b>	
	<b>Your Role</b>	
	<b>Your Company</b>	
<b>For Online Topics</b>	<b>Online doc link</b>	<i>(URL for where the issue is)</i>
	<b>Topic Heading</b>	<i>(if it's a long topic, please provide the heading of the section where the issue is)</i>



<b>For PDF Topics</b>	<b>Document Title</b>	<i>(shown on the cover page or in page header )</i>
	<b>Product Version</b>	<i>(shown on the cover page)</i>
	<b>Document Version</b>	<i>(shown on the cover page)</i>
	<b>Chapter Heading</b>	<i>(shown in footer)</i>
	<b>PDF page #</b>	<i>(shown in footer)</i>
<b>How can we improve?</b>	<b>Describe the issue</b>	<i>Describe the error or issue in the documentation. (If it helps, attach an image to show the issue.)</i>
	<b>How can we improve the content?</b> <b>Be as specific as possible.</b>	
	<b>Any other comments?</b>	

## 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](mailto:support@gigamon.com).

## Contact Sales

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

**Telephone:** +1.408.831.4025

**Sales:** [inside.sales@gigamon.com](mailto:inside.sales@gigamon.com)

**Partners:** [www.gigamon.com/partners.html](http://www.gigamon.com/partners.html)

## Premium Support

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

## The VÜE Community

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

Visit the VÜE site to:

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

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

**Register today at** [community.gigamon.com](http://community.gigamon.com)

**Questions?** Contact our Community team at [community@gigamon.com](mailto:community@gigamon.com).

# GigaVUE-FM Version Compatibility Matrix

The following tables list the different versions of GigaVUE Cloud Suite Cloud solution components available with different versions of GigaVUE-FM.

**NOTE:** GigaVUE-FM version 6.4 supports the latest fabric components version as well as (n-2) versions. It is always recommended to use the latest version of fabric components with GigaVUE-FM, for better compatibility.

## GigaVUE-FM Version Compatibility

The following fabric components are renamed as follows:

- G-vTAP Agents - UCT-V
- Next Generation G-vTAP Agents - Next Generation UCT-V
- G-vTAP Controller - UCT-V Controller

GigaVUE-FM	UCT-V Version	Next Generation UCT-V Version	UCT-V Controller Version	GigaVUE V Series Proxy	GigaVUE V Series Nodes
6.4.00	v6.4.00	v6.4.00	v6.4.00	v6.4.00	v6.4.00

GigaVUE-FM	G-vTAP Agent Version	Next Generation G-vTAP Agent Version	G-vTAP Controller Version	GigaVUE V Series Proxy	GigaVUE V Series Nodes
6.3.00	v6.3.00	v6.3.00	v6.3.00	v6.3.00	v6.3.00
6.2.00	v6.2.00	v6.2.00	v6.2.00	v6.2.00	v6.2.00
6.1.00	v6.1.00	N/A	v6.1.00	v6.1.00	v6.1.00
6.0.00	v1.8-7	N/A	v1.8-7	v2.7.0	v2.7.0
5.16.00	v1.8-5	N/A	v1.8-5	v2.6.0	v2.6.0
5.15.00	v1.8-5	N/A	v1.8-5	v2.5.0	v2.5.0

<b>GigaVUE-FM</b>	<b>G-vTAP Agent Version</b>	<b>Next Generation G-vTAP Agent Version</b>	<b>G-vTAP Controller Version</b>	<b>GigaVUE V Series Proxy</b>	<b>GigaVUE V Series Nodes</b>
5.14.00	v1.8-4	N/A	v1.8-4	v2.4.0	v2.4.0
5.13.01	v1.8-3	N/A	v1.8-3	v2.3.3	v2.3.3
5.13.00	v1.8-2	N/A	v1.8-2	v2.3.0	v2.3.0

# 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)