



GigaVUE-FM Administration Guide

GigaVUE

Product Version: 6.14

Document Version: 1.1

(See Change Notes for document updates.)

Copyright © 2026 Gigamon Inc. All rights reserved.

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

Trademark Attributions

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

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

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
6.14	1.0	02/25/2026	The original release of this document with 6.14.00 GA.

Contents

GigaVUE-FM Administration Guide	1
Change Notes	2
Contents	3
Administer GigaVUE-FM	9
Authentication	9
Add Users	12
How to Unlock User Account	14
Create User Groups	15
Create Roles	17
Configure Authentication Type	22
Configure Default User Group	23
Groups Configured in GigaVUE-FM Based on AuthMethod	23
Configure Lock/Unlock Authentication Setting for Local User Accounts	28
Rules and Notes	28
Configure Authentication	29
Supported TACACS+ Servers	31
TACACS+ Section: Controls and Fields	31
Add a New TACACS+ Server	32
Supported RADIUS Servers	34
RADIUS Server Section: Controls and Fields	34
Add a New RADIUS Server	34
Set Default Key, Timeout, and Retransmit Options for RADIUS Servers	36
Supported LDAP Servers	37
LDAP Server Section: Controls and Fields	38
Add a New LDAP Server	38
Set Default Options for LDAP Servers	39
Delete an LDAP Server	40
Configure Remote User Group Mapping	40
LDAP Authentication Failure	41
Assign User Groups in External Authentication Servers	42

Assign Groups with External Authentication Servers	43
Configure Cisco ACS: RADIUS Authentication	44
Configure Cisco ACS: TACACS+ Authentication	45
Configure Cisco Identity Services Engine (ISE): RADIUS Authentication	46
Configure Cisco Identity Services Engine (ISE) TACACS+ Authentication	48
Configure Remote User Group Mapping	50
ADFS	54
Configure GigaVUE-FM in ADFS	55
OKTA	61
Configure GigaVUE-FM in OKTA	61
Microsoft Azure	63
Configure GigaVUE-FM in Microsoft Azure	63
GigaVUE-FM Configured with Internal IdP	65
GigaVUE-FM Configured with External IdP	66
Roles and Users	71
Important Notes on GigaVUE-FM RBAC	72
How to Unlock User Account	75
Tags	82
User Association with Roles and Tags	85
Node Level Tagging	91
Tagging Ports	92
Bulk Upload Tags	94
Alarms	98
Suppressing from Alarms page	100
Suppressing from Physical Nodes page	101
Filter Suppression Rule	102
Export Suppression Rule	102
Events	112
Alarms for Inline Network Resources	115
Alarms for GigaSMART Operations	115
Export Event Records	118
All Audit Logs	119
Export Event Records	125
System	125
Are all versions of GigaVUE-FM validated for FIPS compliance?	138
Can you enable FIPS using the fmctl command?	139
Can you add a device that is not FIPS-compliant to a FIPS enabled GigaVUE-FM?	139

What happens to the GigaVUE-FM database after you enable FIPS?	139
How do I perform backup and restore operation on a FIPS enabled GigaVUE-FM?	139
Is the FIPS certification applicable for GigaVUE-FM instance irrespective of where it is deployed?	139
Traffic Health State Based on SNMP Traps	140
Configure SNMP Traps	140
Configure GigaStream Imbalance per GigaStream	153
Add New Template	157
Edit Custom Template	158
Using the “Default” Credentials Effectively	159
Node Details Fields and Page Controls	159
How Alert Policies Work	162
Tunnel Traffic Drop Identification	163
Rules, Notes, and Limitations	164
Configure Alert Policy	165
Rules and Notes	168
GigaVUE-FM Backup	168
GigaVUE-FM Restore Process	169
Recovery Process	169
Data Saved When Backing Up GigaVUE-FM	169
Backup Immediately	170
Schedule Backups	170
Restore GigaVUE-FM Configuration Files	171
Archive Servers	172
Add an Archive Server	172
Edit an Archive Server	173
Delete an Archive Server	173
Archive Server Requirements for Linux machine	173
Enable Do Not Purge	174
Disable Do Not Purge	174
Download Backup Files.	175
Device Configuration Backup	175
Version Compatibility	175
Points to Remember	175
Restore Configuration (RMA'ed device)	175
Standalone Devices (RMA):	176
A node of the cluster (RMA):	176
Pre-requisites	182
Limitations	183
CLI Command	183
CLI Command	184

CLI Command	185
CLI Command	186
CLI Command	186
Example for Certificate Issuance	187
Pre-requisites	188
Updating Trust Store	192
Certificate Issuance	192
Certificate Renewal	194
Certificate Revocation	194
Certificate Deletion	194
Notes	195
Certificate Issuance	197
Certificate Renewal	199
Certificate Deletion	199
Audit	199
Rules and Notes	199
Generate CSR	200
Upload CA Certificate	200
Configure Notification Receivers	208
Validate SNMP Receiver Configuration	210
Enable SNMP Trap and Events	210
Send Test Email	211
Editing a Proxy Server Profile	221
Delete a Proxy Server Profile	221
Upgrade Considerations	223
Editing a Split DNS Profile	224
Delete a Split DNS Server Profile	225
Tasks	225
View the Upgrade Sanity Check	227
Delete an Admin Task	227
Delete a Scheduled Task	228
Reports	228
CEF Message Format	238
Configure Security Options	240
Are all versions of GigaVUE-FM validated for FIPS compliance?	243
Can you enable FIPS using the fmctl command?	243
Can you add a device that is not FIPS-compliant to a FIPS enabled GigaVUE-FM?	243
What happens to the GigaVUE-FM database after you enable FIPS?	243
How do I perform backup and restore operation on a FIPS enabled GigaVUE-FM?	244

Is the FIPS certification applicable for GigaVUE-FM instance irrespective of where it is deployed?	244
Behavior	251
NTP Server for Clock Synchronization	254
Before you begin	255
View Information About GigaVUE-FM	257
Generate a Report for Customer Deployed Assets	258
High Availability for Physical Environment	259
Create and Add GigaVUE-FM Instances to HA Group	266
Encryption using Pre-Shared Secret Keys	292
Encryption using Certificates	292
Rules and Notes	292
Configure Certificates in FMHA Nodes	293
Prerequisite	293
Import Self Certificates for Each FMHA Node to NSS DB	293
Share Certificates to Peer FMHA Nodes	294
Import Peer Certificates	294
Verify Imported Self Node Certificates and Peer Node Certificates on NSS DB	295
Create fmha.yaml	295
Switch to Certificate Based From GigaVUE-FM GUI	296
Rules and Notes	296
High Availability for Cloud Infrastructure	296
Software Licensing Reference	318
Setting the GigaVUE-FM Admin Password	318
Logging in to GigaVUE-FM Command Line Interface	319
GigaVUE-FM CLI Commands	319
Mapping of SNMP Traps with GigaVUE-FM Events and Alarms	327
GigaVUE® Fabric Management Events	336
Corrective Actions for GigaVUE-FM Alarms	372
Port Unhealthy	373
Port Pair Unhealthy	373
Port Group Unhealthy	373
Tunnel Port Unhealthy	374
IP Interface Unhealthy	374
Map Unhealthy	374
GigaStream Unhealthy	375
Inline Network Unhealthy	375
Inline Network Group Unhealthy	375
Inline Tool Unhealthy	375
Inline Tool Group Unhealthy	376
Tunnel Logical Group Unhealthy	376
Traffic Drop Threshold Exceeded	376

Giga Fabric Map Unhealthy	377
Low Memory	377
CPU Overloaded	378
Operational Mode [SAFE or Limited]	378
Card Unhealthy	378
Abnormal Fan Operation	380
Faulty Power Module	381
G-TAP Battery Unhealthy	381
G-TAP Port Group Incompatible	382
Device CPU Temperature Unhealthy	382
Stack Link Unhealthy	382
Device Unreachable/Health Indeterminable	383
Device Not Reported/Health Indeterminable	383
Cluster Member Not-reachable	384
Gsgroup Unhealthy	384
Virtual Port Unhealthy	384
GigaSMART Operation Unhealthy	385
Glossary	386

Administer GigaVUE-FM

Featured topics:

- [Authentication](#)
- [Tags](#)
- [Roles and Users](#)
- [Alarms](#)
- [Events](#)
- [All Audit Logs](#)
- [Tasks](#)
- [Reports](#)
- [System](#)

Authentication

This chapter describes how to configure authentication and authorization settings for GigaVUE-FM.

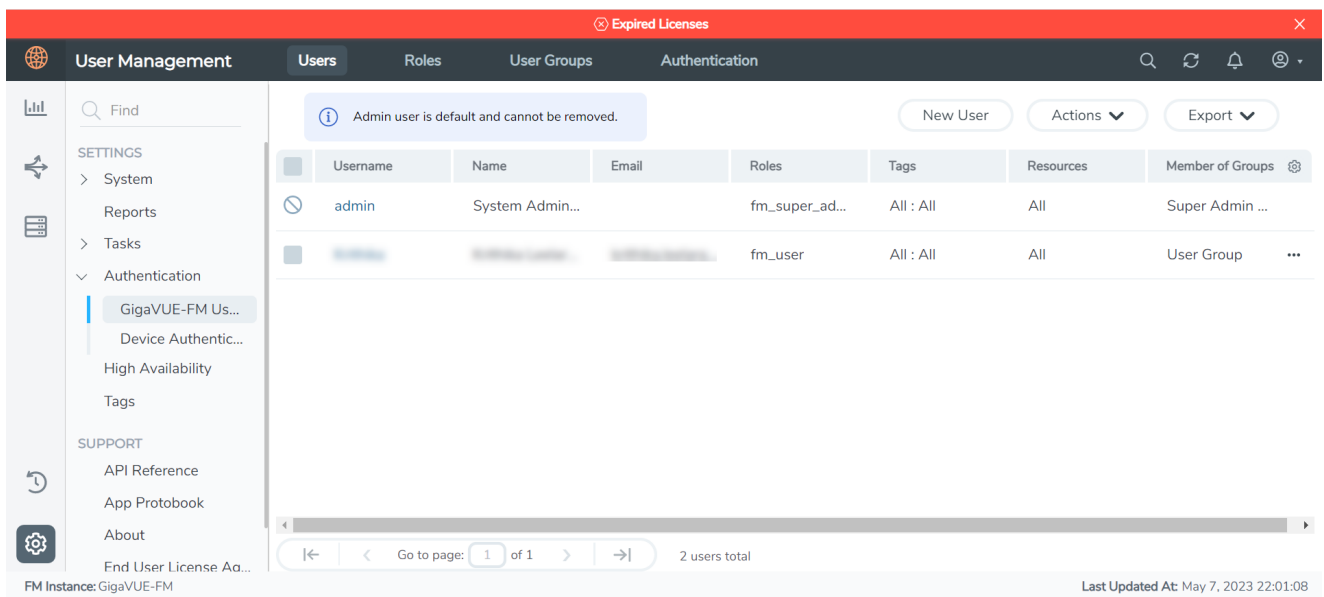
This section covers of the following main topics:

- [Overview of Authentication](#)
- [GigaVUE-FM User Management](#)
- [Single Sign-on](#)
- [Authentication Type](#)
- [Supported RADIUS Servers](#)
- [Supported TACACS+ Servers](#)
- [LDAP](#)
- [Assign Groups with External Authentication Servers](#)
- [Configure User Groups in External Authentication Servers](#)

Overview of Authentication

Authentication pages are used to configure authentication and authorization settings for GigaVUE-FM. To view the authentication pages:

1. Go to **Settings** and select **Authentication**.



The following table describes the pages available when **Authentication** is selected from the left navigation pane

Page	Description
GigaVUE-FM User Management	Manage local user accounts. From here, you can add new accounts, edit existing accounts, or delete users. Refer to GigaVUE-FM User Management for details.
Device Authentication Services	Manage authentication priority and user mapping settings globally for all the devices managed by GigaVUE-FM. You can also perform LDAP Server and LDAP User Group mapping configurations globally for all the nodes managed by GigaVUE-FM. Refer to GigaVUE-FM User Management for details.

Important: Always use HTTPS to run GigaVUE-FM . Running GigaVUE-FM on other non-secure protocols does not generate IDP metadata.

The following table details the AAA configuration support for the various software versions in GigaVUE-FM and CLI.

Software Version	AAA Configuration in GigaVUE-FM	AAA Configuration in CLI	Comments
5.6.0.0 and Below	Yes	Yes	You can view the AAA settings configured using GigaVUE-FM in CLI and vice-e-versa.
5.7.00	Yes	Yes	You cannot view the AAA settings configured using GigaVUE-FM in CLI

Software Version	AAA Configuration in GigaVUE-FM	AAA Configuration in CLI	Comments
			and vice-e-versa.
5.8.00 and above	Yes	No	You can configure the AAA settings only using GigaVUE-FM. AAA Configuration using CLI is not supported.

GigaVUE-FM User Management

The GigaVUE-FM User Management page consists of the following tabs using which you can add users, create groups and create roles. Refer to the following section for details:

- [Users](#)
- [User Groups](#)
- [Roles](#)
- [Configure Authentication Type](#)

Users

The Users page lets you manage the GigaVUE-FM users. You can also configure user's role and user groups to control the access privileges of the user in GigaVUE-FM. To add users you must be a user with **fm_super_admin** role or a user with either read/write access to the GigaVUE-FM security Management category.

NOTE: GigaVUE-FM is preconfigured with one user with the **fm_super_admin** role assigned (user name - **admin**, password - **admin123A!!**).

Accounts and credentials configured in Users page are stored to a local database in GigaVUE-FM.

The Users page lists the details of the users configured in GigaVUE-FM:

Field	Description
Username	User name configured in GigaVUE-FM
Locked	Indicates if the user account is locked or not.
Locked Time	User account locked time
Name	Actual name of the user.
Email	User email.
Roles	User role.

Field	Description
Resources	Resources available to the user based on the role.
Tags	Tags applicable to the user.
Member of Groups	Group to which the specific user belongs to.

For information about adding users, refer to the [Add Users](#) section.

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 GigaVUE-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. Go to **Settings** and select **Authentication > GigaVUE-FM User Management > Users**. The **User** page is displayed.

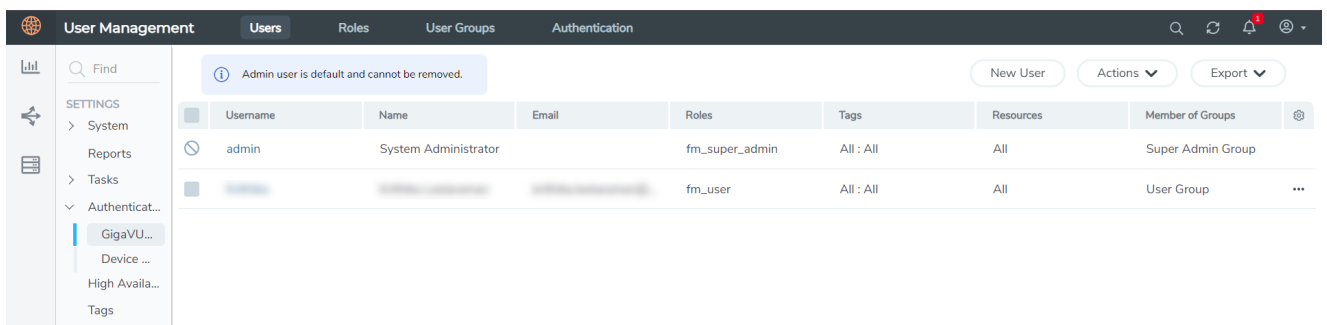


Figure 1 FM Users Page

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 -!@#\$%^&*()+

Figure 2 *Create User*

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

- **Assign User Group:** Assign user group to users.
- **Edit:** Edit the user details.
- **Delete:** When you delete a user, all sessions associated with them will be logged out.
- **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 GigaVUE-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.

User Groups

The User Groups configured in GigaVUE-FM helps to associate the users with tags and roles. A user group consists of a set of roles and set of tags associated with a group. When a user is created they can be associated with one or more user groups.

The User Groups page lists the user groups available in GigaVUE-FM. The following user groups are available by default in GigaVUE-FM:

- **Super Admin Group:** Users belonging to this group have access to all the resources in the system, and the users can perform any operation on the resources.
- **Admin Group:** The admin user can perform all GigaVUE-FM operations except adding or modifying users, configuring AAA settings, adding certificates in the trust store, and adding an external data server. Users cannot create, modify, or delete the resources with GigaVUE-FM security management permission.
- **View only User Group:** Users belonging to this group have read access to all resources in the system. The users can view the resources, but will not be able to modify the resources.

You can create custom user groups in addition to the default user groups in GigaVUE-FM. Refer to the [Create User Groups](#) section for more details to associate a group to a user.

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.

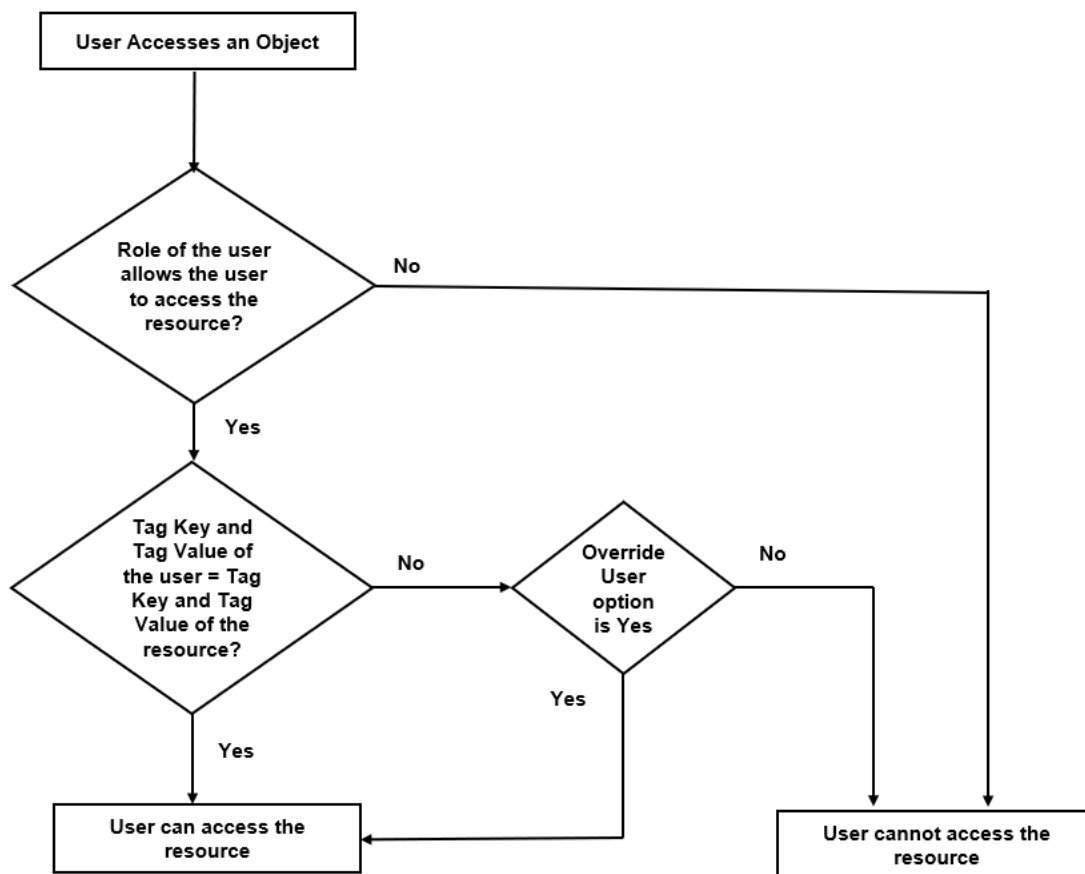
The following user groups are available by default in GigaVUE-FM. You will not be able to edit or change these groups in the system.

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:

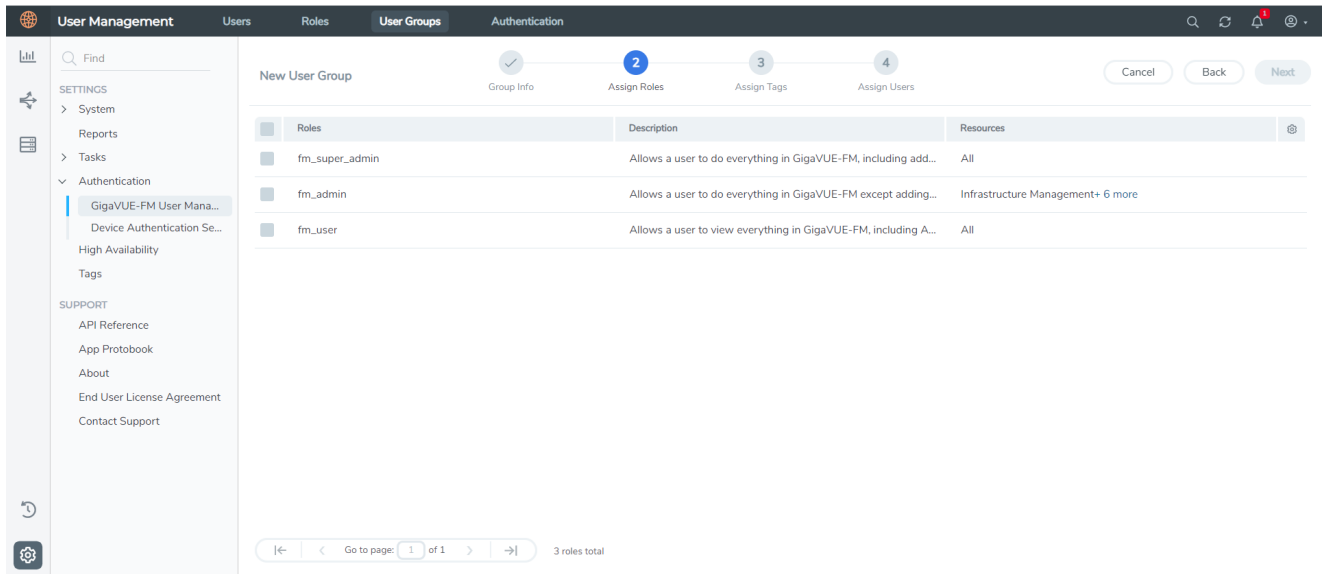
- The category of resources which the user can access, such as the clusters, ports, maps and so on. This is defined using the **Roles** option. Refer to the Roles section for more details.
- The physical and logical resources that the user can access, such as the ports in a cluster that belong to a specific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



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 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.

Roles

The Roles page lists the roles available in GigaVUE-FM. Refer to the [Create Roles](#) for more details to associate a role to a user.

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 GigaVUE-FM 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 GigaVUE-FM 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 GigaVUE-FM 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
All	Manages all resources • A user with fm_super_admin role has both read and write access to all the resource categories. • A user with fm_user role has only read access to all the resource categories.
Infrastructure Management	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: • Physical resources: Chassis, slots, cards ports, port groups, port pairs, cluster config, nodes and so on • GigaVUE-FM inventory resources: Nodes, node credentials • Device backup/restore: Device and cluster configuration • Device license configuration: Device/cluster licensing • Statistics: Device, port • Tags: Events, historical trending • Device security: SystemTime, System EventNotification, SystemLocalUser, System Security Policy Settings, AAA Authentication Settings, Device User Roles, LDAP Servers, RADIUS Servers, TACACS+ Servers • Device maintenance: Sys Dump, Syslog • Cloud Infrastructure resources: Cloud Connections, Cloud Proxy Server, Cloud Fabric Deployment, Cloud Configurations,

Category	Associated Resources
	Sys Dump, Syslog, Cloud licenses, Cloud Inventory. Note: Cloud APIs are also RBAC enabled.
Traffic Control Management	Manages inline resources, flow maps, GigaSMART applications, second level maps, map chains, map groups. The following resources belong to this category: • Infrastructure resources: IP interfaces, circuit tunnels, tunnel endpoints, tunnel load balancing endpoints, ARP entries • Intent Based Orchestration resources: Policies, rules • GigaSMART resources: GigaSMART, GSgroups, vPorts, NetFlow exporters • Map resources: Fabric, fabric resources, flow maps, maps, map chains, map groups, map templates • Application intelligence resources: Application visibility, Metadata, application filter resources • Tag: Flow manipulation - NetFlow operations, Statistics - device port • Active visibility • Inline resources: Inline networks, Inline network groups, Inline tools, Inline tool groups, Inline serial tools, Inline heartbeat profile • Cloud operation resources: Monitoring session, stats, map library, tunnel library, tools library, inclusion/exclusion maps. NOTE: Cloud APIs are also RBAC enabled.
FM Security Management	Ensures secure GigaVUE-FM environment. Users in this category can manage user and roles, AAA services and other security operations.
System Management	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: • Backup/restore • Archive server • License • Storage management • Image repo config • Notification target/email
Forward list/CUPS Management	Manages the forward list configuration. The following resources belong to this category: • GTP forward list • SIP forward list

Category	Associated Resources
Third Party Orchestration	Used to deploy fabric components using external orchestrator.
Device Certificate Management	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 GigaVUE-FM Security Management category.

To create a role

1. Go to **Settings** and select **Authentication > GigaVUE-FM User Management > Roles**.
2. Click **New Role**.

The screenshot displays the 'New Role' configuration page in the GigaVUE-FM User Management interface. The page has a dark header with tabs for 'Users', 'Roles', 'User Groups', and 'Authentication'. The 'Roles' tab is active. On the left, a sidebar menu shows 'Authentication' expanded, with 'GigaVUE-FM User Management' selected. The main content area contains the 'New Role' form, which includes a 'Role Name' text field, a 'Description' text area, and a 'Select Permission' table. The table has columns for 'Resources', 'Permissions', and 'Description'. The 'Resources' column lists 'Infrastructure Management', 'Traffic Control Management', 'FM Security Management', 'System Management', and 'Forwardlist Management'. The 'Permissions' column shows a dropdown menu for each resource, currently set to 'Select a permission'. The 'Description' column provides a brief description for each resource. At the bottom of the form, there are 'Cancel' and 'Apply' buttons. The footer of the interface shows 'FM Instance: GigaVUE-FM' and 'Last Updated At: May 9, 2023 15:03:36'.

3. In the New Role page, select or enter the following details:
 - **Role Name:** Name of the role.
 - **Description:** Description of the role.

- **Select Permission:** In the **Select Permission** table, select the required permission for the various resource categories.

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

NOTE: GigaVUE-FM does not allow you to import Users, User Groups and Roles. You can only export the configurations.

Change Your Password

Users authenticated against GigaVUE-FM's local user database can always change their own passwords. The Password can be a minimum of 8 characters and a maximum of 64 characters, and must comply with the character requirements specified below:

- One numerical character
- One uppercase character
- One lowercase character
- One special character (!, @, #, and so on)

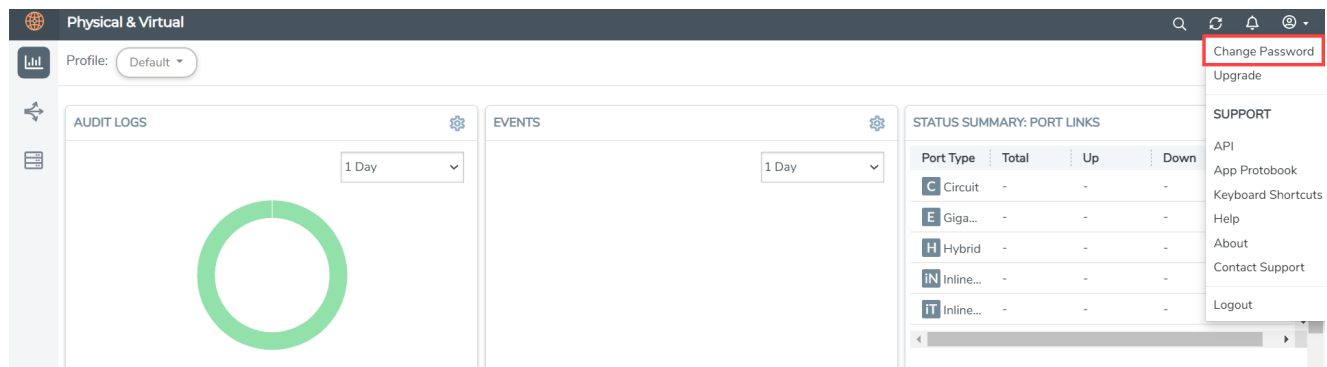


Notes:

- The **Change Your Password** link is available only for locally authenticated users, and will be unavailable for users authenticated against external authentication servers.
- Resetting a user's password automatically logs out all active sessions for that user.
- Externally authenticated users can change their admin password as follows:
 - Use the fmctl command.
 - Change the authentication method to 'Local' and change the password.

The following are the steps for changing your password:

1. Click on the button in the upper right-hand corner of GigaVUE-FM, where your user name is displayed, and select **Change Password**.



The Change Password page displays.

2. On the Change Password page, do the following:
 - Enter your current password in the **Current Password** field.
 - Enter the new password in the **New Password** and **Confirm Password** fields.
3. Click **Save**.

GigaVUE-FM logs out to reset the password. Enter your new password to log in again.

NOTE: Use the **sudo passwd admin** command to change the GigaVUE-FM Shell password.

Authentication Type

Use the Authentication Type page to configure the following:

- [Configure Authentication Type](#)
- [Configure Default User Group](#)
- [Configure Lock/Unlock Authentication Setting for Local User Accounts](#)
- [Configure Authentication](#)

Configure Authentication Type

GigaVUE-FM supports and authenticates users against the following authentication methods:

- **Local:** Local database configured through the [GigaVUE-FM User Management](#) page.
- **External authentication servers:** Includes LDAP, RADIUS, or TACACS+
- **Third Party:** External identity provider.

NOTE: When you change the authentication type, GigaVUE-FM automatically logs out all users from their current sessions.

You can select only one of the authentication methods depending on your requirement. That is, you can select any one of the remote authentication methods or use the local authentication method or the external identity provider. This allows for enhanced security by maintaining the user names and passwords in a single location.

In case of remote authentication methods, you can configure fall back within the same scheme of AAA authentication. For example, for RADIUS authentication, you can add multiple RADIUS servers, so that, if the first server is not reachable, the second server is tried for accessibility and so on.

NOTE: If you cannot access GigaVUE-FM due to failure in authentication, you can use the special access provided (<https://<fm ip address>/<dns name>/admin>). This access is applicable only for local users with super admin privileges. You can also access GigaVUE-FM through the Command Line Interface and locate the following log file to determine the reason for the failure in authentication:
`/var/log/shibboleth/idp-process.log`

If authentication is done in the local server, then authorization is also performed locally. If authentication is done in the remote server, then authorization is also done at the remote server. Therefore, it is not required to configure extra roles for mapping purposes.

Configure Default User Group

For security reasons, the **Default User Group** option is not configured by default in GigaVUE-FM. If required, you can configure the **Default User Group** option to specify how the local and externally authenticated users can be granted privileges in GigaVUE-FM. If there are no valid GigaVUE-FM specific groups configured in the remote server but if a default user group is configured in GigaVUE-FM, then that group will be assigned. Otherwise, the user cannot login in to GigaVUE-FM without groups being configured.

NOTE: You are responsible for configuring the groups at the remote server in the specified format for TACACS+ and RADIUS servers. For LDAP, you must configure the list of groups for Group Base DN in GigaVUE-FM.

Groups Configured in GigaVUE-FM Based on AuthMethod

The following table consists of examples with groups resolved in GigaVUE-FM based on the AuthMethod field:

AuthMethod	Logged in User	MapDefaultUserGroup	Remote Roles/Group Base DN (if configured)	Expected Group	Assigned Group	Notes
Local	test	-	-	fm_user	fm_user	The authMethod is 'LOCAL'. Therefore, the logged-in user group will be assigned.
TACACS+	tacacsuser1	-	fm_admin	fm_admin	fm_admin	The role which

AuthMethod	Logged in User	MapDefaultUserGroup	Remote Roles/Group Base DN (if configured)	Expected Group	Assigned Group	Notes
						has been assigned remotely will be assigned.
TACACS+	tacacsuser3	-	fm_non_exist_group [specified group Does not match any roles in GigaVUE-FM]	-	-	If non-exist group is being assigned remotely, then that user cannot login into GigaVUE-FM. GigaVUE-FM will reject that user.
TACACS+	tacacsuser3	User Group	fm_non_exist_group [specified group Does not match any roles in GigaVUE-FM]	User Group	User Group	If non-exist group is being assigned remotely, then GigaVUE-FM will check if Default User Group has been configured. If Default User Group is configured, then it will assign the same and allow the user to log in to GigaVUE-FM.
TACACS+	tacacsuser2	-	-	-	-	If there are no groups configured remotely and Default User Group is also not configured in

AuthMethod	LoggedIn User	MapDefaultUserGroup	Remote Roles/Group Base DN (if configured)	Expected Group	Assigned Group	Notes
						GigaVUE-FM, then that user cannot log in to GigaVUE-FM. GigaVUE-FM will reject that user.
RADIUS	radiususer1	-	fm_admin	fm_admin	fm_admin	The role which has been assigned remotely will be assigned.
RADIUS	radiususer3	-	fm_non_exist_group [specified group Does not match any roles in GigaVUE-FM]	-	-	If non-exist group is being assigned remotely, then that user cannot log in to GigaVUE-FM. GigaVUE-FM will reject that user.
RADIUS	radiususer3	User Group	fm_non_exist_group [specified group Does not match any roles in GigaVUE-FM]	User Group	User Group	If non-exist group is being assigned remotely, then GigaVUE-FM will check whether Default User Group has been configured; If Default User Group is configured, then it will assign the same and allow the user

AuthMethod	Logged in User	MapDefaultUserGroup	Remote Roles/Group Base DN (if configured)	Expected Group	Assigned Group	Notes
						to log in to GigaVUE-FM.
RADIUS	radiususer2	-	-	-	-	If there are no groups configured remotely and Default User Group is also not configured in GigaVUE-FM, then that user cannot log in to GigaVUE-FM. GigaVUE-FM will reject that user.
LDAP	ldapuser1	-	CN=FMQA-SSO,DC=hqdevtest,DC=com	fm_admin	fm_admin	The mapped group for the provided Group Base DN will be assigned to the logged in user.
LDAP	ldapuser2	-	CN=FMQA-SSO,DC=hqdev,DC=com	-	-	If there are no group mapped to the provided/associated GROUP BASE DN, then GigaVUE-FM will reject the user and will not allow the user to log in as well.

AuthMethod	Logged in User	MapDefaultUserGroup	Remote Roles/Group Base DN (if configured)	Expected Group	Assigned Group	Notes
LDAP	ldapuser 2	User Group	CN=FMQA-SSO,DC=hqdev,DC=com	User Group	User Group	If there are no group mapped to the provided/associated GROUP BASE DN, then GigaVUE-FM will check whether Default User Group has been configured; If so, it will assign the same and allow the user to login to GigaVUE-FM.
LDAP	ldapuser 3	-	-	-	-	If the LDAP user is not associated to any GROUP in LDAP and it does not return any group, then GigaVUE-FM will reject the user and will not allow the user to login as well.
LDAP	ldapuser 3	User Group	-	User Group	User Group	If the LDAP user is not associated to any GROUP in LDAP and it does not return any group, then

AuthMethod	Logged in User	MapDefaultUserGroup	Remote Roles/Group Base DN (if configured)	Expected Group	Assigned Group	Notes
						GigaVUE-FM will check whether Default User Group has been configured; If so, it will assign the same and allow the user to log in to GigaVUE-FM.

Configure Lock/Unlock Authentication Setting for Local User Accounts

Until software version 6.2.00, when locally authenticated users log in to GigaVUE-FM, user credentials are validated and upon successful validation of the credentials, the user is logged into GigaVUE-FM. If validation of user credentials fails, incorrect user name and password message prompts up. GigaVUE-FM does not impose any restriction on unsuccessful login attempts.

Starting from software version 6.3.00, when locally authenticated users try to login to GigaVUE-FM, and if the login fails after a defined number of failed password attempts, the user account is locked. Only an admin user can unlock the user account. The lock-unlock authentication prevents unauthorized user access and also limits the number of login attempts, thereby controlling the number of brute-force password attacks.

Rules and Notes

Refer to the following rules and notes:

- The lock-unlock authentication option is enabled by default.
- To disable the lock-unlock authentication option from the Authentication Type page, you must be a user with fm_super_admin role or a user with read/write access to the GigaVUE-FM Security Management category.

NOTE: The default fm_super_admin (preconfigured in GigaVUE-FM with username: admin) user can be unlocked only from the GigaVUE-FM Command-line Interface using the fmctl command. Refer to the [GigaVUE-FM CLI Commands](#).

- Once your user account is unlocked, you can login with the default password. Ensure to change the default password to a new password for security reasons.
- You can view the status of locked and unlocked users from the GigaVUE-FM User Management page. However, the status in this page does not depict the Near-real Time status. You must manually refresh the screen to know the status. Refer to the [Users](#) section for more details.
- Whenever a user account is locked or unlocked, events are triggered and can be viewed in the GigaVUE-FM Events page.
- You can also configure Event Notification settings for the events triggered for the lock-unlock authentication. Refer to the [Event Notifications](#) section for more details.
- The Events captured in the Events page are not near-real time events.
- Unsuccessful Login attempts and locked/unlocked user information is captured in the Audit Logs page.

Configure Authentication

Use the **Authentication > Authentication Type** to configure how user logins are authenticated in GigaVUE-FM.

To access the Authentication Type page:

1. Go to **Settings**, select **Authentication > GigaVUE-FM User Management > Authentication**. In the **Authentication Type** page that appears:

The screenshot displays the 'Authentication Type' configuration page in the GigaVUE-FM User Management interface. The left sidebar shows the navigation menu with 'Authentication' selected. The main content area contains the following settings:

- Authentication Server:** Local (dropdown menu)
- Default User Group:** None (dropdown menu)
- Basic Authentication:** Disabled (toggle switch)
- Lock User:** Enabled (toggle switch)
- Maximum Failed Login Attempts:** 5 (dropdown menu)

Two informational messages are displayed on the right side of the page:

- Enabling this option will transmit credentials in plain text (Base64 encoded) and may expose users to security risks.
- After 5 consecutive failed login attempts your account will be locked and can be unlocked only by a privileged user.

Buttons for 'Cancel' and 'Apply' are located at the top right of the configuration area.

- a. Select the required **Authentication Type**. Refer to [Configure Authentication Type](#) section for more details.
- b. Set the **Default User Group** to one of the options: Refer to [Configure Default User Group](#) section for more details.
 - Super Admin Group
 - Admin Group
 - User Group
 - None
- c. Use the **Basic Authentication** Toggle option to enable and disable the Basic Authentication. When you first install GigaVUE-FM, the Basic Authentication option is disabled by default to enhance security. You can enable it manually if required. However, when you upgrade GigaVUE-FM (from 6.10.00 or 6.11.00 versions), Basic Authentication is automatically enabled.
- d. Use the **Lock User** Toggle option to enable and disable the lock-unlock authentication setting.
- e. Configure the **Maximum Failed Login Attempts**. Allowable range is from 3 to 5. Default is 5. Refer to [Configure Lock/Unlock Authentication Setting for Local User Accounts](#) section for more details.

2. Click **Apply**.

TACACS+

Only users belonging to the **Super Admin User Group** or users with write access to GigaVUE-FM Security Management category can use the **Authentication Server > TACACS+** to add entries to GigaVUE-FM's list of available TACACS+ authentication servers.

You can add multiple TACACS+ servers. Servers are used as fallbacks in the same order they are specified – if the first server is unreachable, the second is tried, and so on, until all named servers have been used. If a server is reachable and authentication fails, the authentication process terminates.

Figure 3 TACACS+ Page

NOTE: If you are deploying GigaVUE-FM inside AWS, make sure to provide the private IP address of GigaVUE-FM to the TACACS+ server for authentication and not its public IP address.

Supported TACACS+ Servers

GigaVUE-FM has been tested with the TACACS+ implementation provided by Cisco Secure ACS v5.4.0.46.0 and CISCO ISE v3.3.x. Although other versions and implementations may operate acceptably, they have not been tested.

TACACS+ Section: Controls and Fields

TACACS+ server section has the following buttons that allow you to manage the information that appears in the table.

Controls	Description	
Add Server	Allows you to add a new TACACS+ Server to the list. See Add a New TACACS+ Server for details.	
Actions	Click the Actions drop-down to perform the following: Edit: Allows you to change the settings for an existing TACACS+ Server entry. Select a server's entry and click Edit to open a dialog where you make the changes.	

Controls	Description	
	Delete: Allows you to delete a TACACS+ Server entry.	
Default Settings	Allows you to set default Shared Secret , Timeout , Retransmit , and Services options for TACACS+ Servers. When you add a new TACACS+ Server to the list, you have the option of accepting these default settings or providing custom values.	

Add a New TACACS+ Server

Add a new TACACS+ Server to GigaVUE-FM's list by clicking **Add** and setting the options on the Add TACACS Server page shown in [Figure 4 Adding TACACS+ Server Settings](#).

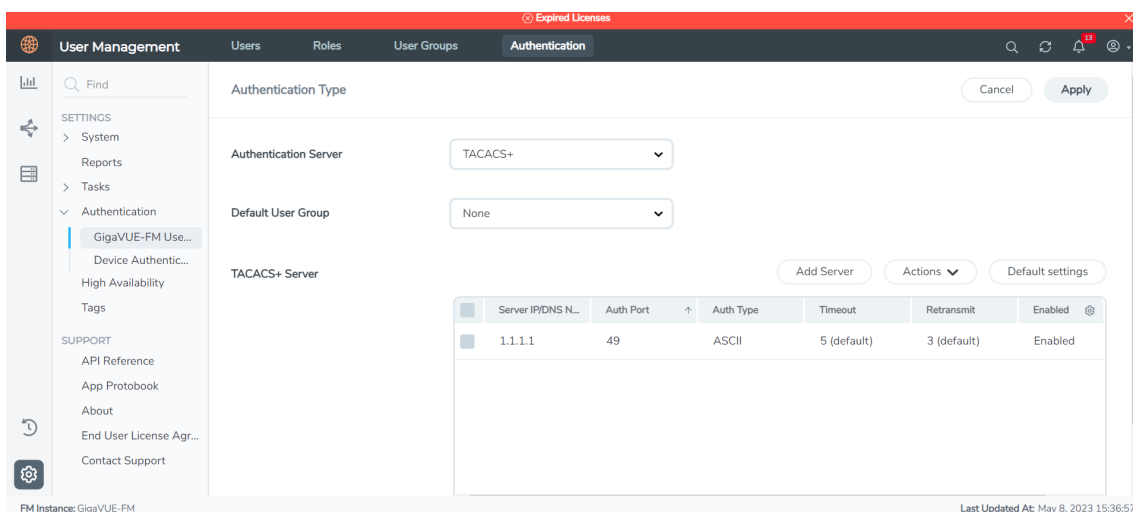


Figure 4 Adding TACACS+ Server Settings

The following table describes the settings.

Field	Description
Enabled	Specify whether this server is currently enabled for use with authentication requests.
Server IP/DNS Name	The IPv4/IPv6 address or the DNS name configured for this TACACS+ Server entry. The same IP address can be used for more than one TACACS+ server as long as they use different Auth Port values.
Auth Port	The UDP port number on which the TACACS+ server is running. If not specified, the port is set to the default TACACS+ port number of 49.
Auth Type	The authentication type used by the TACACS+ server. The valid values are: - PAP. This is the default - ASCII
Use defaults for following	Leave this box checked to accept the default values for the Key , Timeout , and Retransmit options configured by clicking the Edit Default button at the top of the TACACS+ . Alternatively, you can leave this box unchecked and set custom values for the Key , Timeout , and Retransmit options with the respective fields.
Shared	Specifies a shared secret string to be used for encryption of authentication packets sent

Field	Description
Secret	between GigaVUE-FM and this TACACS+ server.
Timeout	Specifies how long GigaVUE-FM will wait for a response from this TACACS+ server to an authentication request before declaring a timeout failure. The valid range is 0-60 seconds; default value is five seconds.
Retransmit	Specifies the number of times GigaVUE-FM will attempt to authenticate with this TACACS+ server before moving on to the next authentication server or method. The valid range is 0-5; default is two. Set to 0 to disable retransmissions.

RADIUS

NOTE: The instructions given in the topic are based on ISE v3.3.x.

Only users belonging to the Super Admin User Group or users with write access to GigaVUE-FM Security Management category can use the **Authentication Server > RADIUS** to add entries to GigaVUE-FM's list of available RADIUS authentication servers.

You can add multiple RADIUS servers. Servers are used as fallbacks in the same order they are specified – if the first server is unreachable, the second is tried, and so on, until all named servers have been used. If a server is reachable and authentication fails, the authentication process terminates.

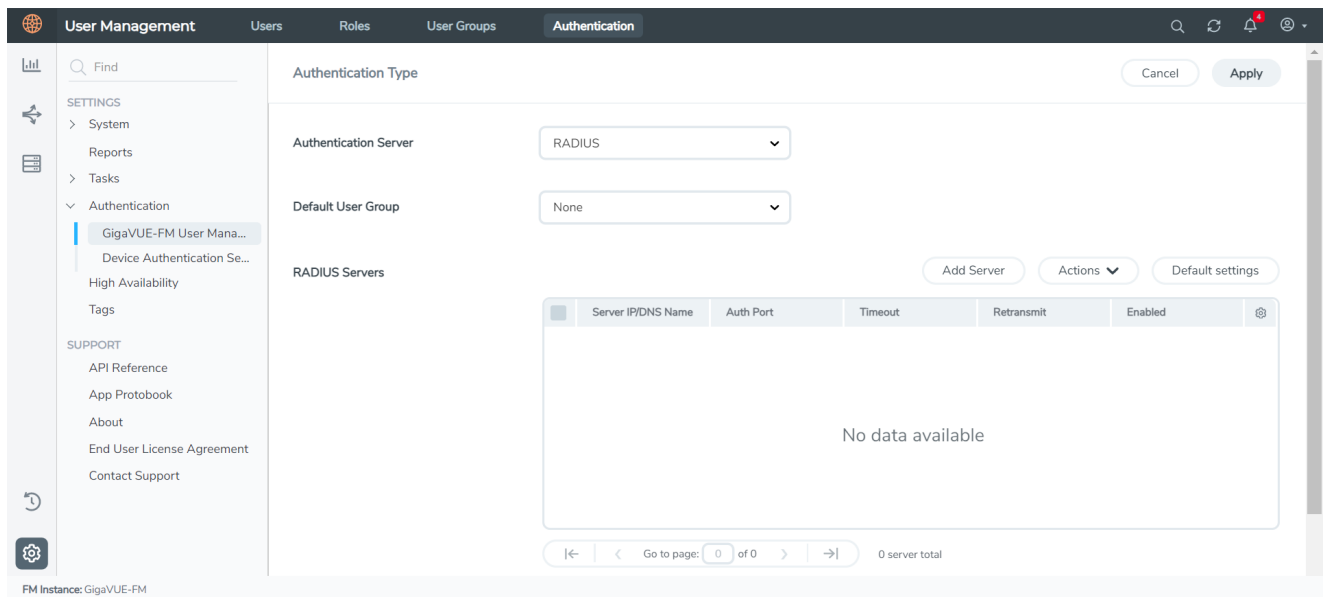


Figure 5 Radius Server

NOTE: If you are deploying GigaVUE-FM inside AWS, make sure to provide the private IP address of GigaVUE-FM to the Radius server for authentication and not its public IP address.

Supported RADIUS Servers

GigaVUE-FM has been tested with the RADIUS implementation provided by Cisco Secure ACS v5.4.0.46.0 and CISCO ISE v3.3.x. Although other versions and implementations may operate acceptably, they have not been tested.

RADIUS Server Section: Controls and Fields

RADIUS Servers section has the following buttons that allow you to manage the information that appears in the table.

Controls	Description
Add Server	Allows you to add a new RADIUS Server to the list. See Add a New RADIUS Server for details.
Actions	Click the Actions drop-down to perform the following: Edit: Allows you to change the settings for an existing RADIUS Server entry. Select a server's entry and click Edit to open a dialog where you make the changes. Delete: Allows you to delete a RADIUS Server entry.
Default Settings	Allows you to set default Shared Secret , Timeout , and Retransmit options for RADIUS Servers. When you add a new RADIUS Server to the list, you have the option of accepting these default settings or providing custom values. See Set Default Key, Timeout, and Retransmit Options for RADIUS Servers for details.

Add a New RADIUS Server

You can add a new RADIUS Server to GigaVUE-FM. Click the **Add Server** button and set the options shown in [Figure 6 Adding Radius Server](#).

Figure 6 Adding Radius Server

Enter the following details in the Add Radius Server pop-up.

Setting	Description
Enabled	Specifies whether this server is currently enabled for use with authentication requests
Server IP/DNS Name	Specifies the IPv4/IPv6 address or the DNS name of the RADIUS server. The same IPv4/IPv6 address can be used for more than one RADIUS server as long as they use different Auth Port values.
Auth Port	Specify the UDP port number on which the RADIUS server is running. If not specified, the port is set to the default RADIUS port number of 1812.
Use defaults for following	Leave this box checked to accept the default values for the Shared Secret, Timeout, and Retransmit options configured by clicking the Edit Default button at the top of the RADIUS page. Alternatively, you can leave this box unchecked and set custom values for the Shared Secret, Timeout, and Retransmit options using the respective fields.

Setting	Description
Shared Secret	Specifies a shared secret string to be used for encryption of authentication packets sent between GigaVUE-FM and this RADIUS server.
Timeout	Specifies how long GigaVUE-FM will wait for a response from this RADIUS server to an authentication request before declaring a timeout failure. The valid range is 0-60 seconds; default value is five seconds.
Retransmit	Specifies the number of times GigaVUE-FM will attempt to authenticate with this RADIUS server before moving on to the next authentication server or method. The valid range is 0-5; default is two. Set to 0 to disable retransmissions.

Set Default Key, Timeout, and Retransmit Options for RADIUS Servers

Click Default Settings to edit the following options:

The following table describes the settings.

Setting	Description
Shared Secret	Specifies a default shared secret string to be used for encryption of authentication packets sent between GigaVUE-FM and all RADIUS servers. Can be overridden with the key specified for a specific RADIUS Server when the server is added.
Timeout	Specifies a default value for how long GigaVUE-FM should wait for a response from a RADIUS server to an authentication request before declaring a timeout failure. This can be overridden with the timeout value specified for a specific RADIUS Server when the server is added. The valid range is 0-60 seconds. The default value is five seconds.
Retransmit	Specifies a default value for the number of times GigaVUE-FM will attempt to authenticate with a RADIUS server. Can be overridden with the retransmit value specified for a specific RADIUS Server when the server is added. The valid range is 0-5; default is two. Set to 0 to disable retransmissions.

LDAP

Only users belonging to the **Super Admin User Group** or users with write access to the GigaVUE-FM Security Management category can use the **Authentication Server > LDAP** section to add entries to GigaVUE-FM's list of available LDAP authentication servers.

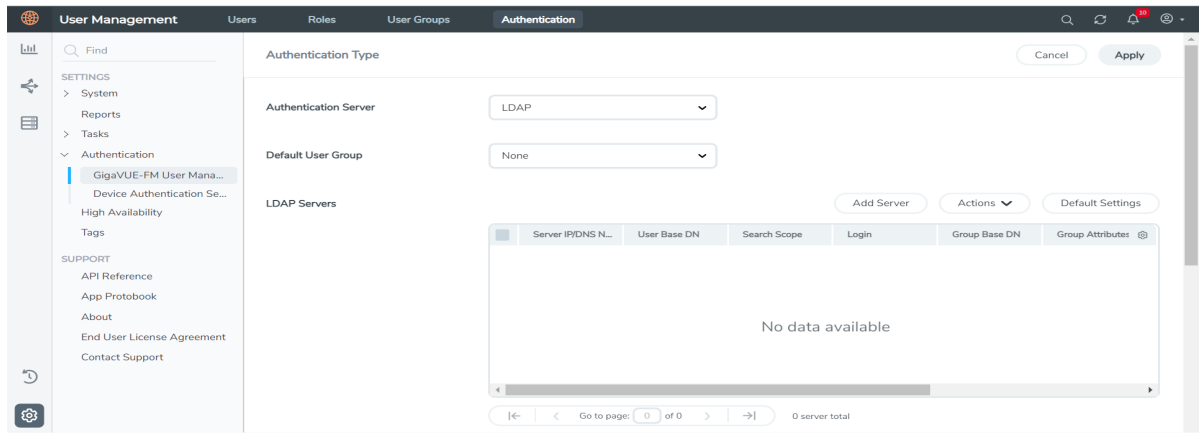


Figure 7 LDAP Section

You can add multiple LDAP servers. Servers are used as fallbacks in the same order they are specified – if the first server is unreachable, the second is tried, and so on, until all named servers have been used. If a server is reachable and authentication fails, the authentication process terminates.

Refer to the following sections for details:

- [Add a New LDAP Server](#) : To add a new LDAP server.
- [Set Default Options for LDAP Servers](#): To set the default options for mapping to the LDAP servers.
- [Configure Remote User Group Mapping](#): To map an LDAP group to pre-configured groups in GigaVUE-FM (Super Admin/Admin/User in Gigamon or the custom user groups).

Supported LDAP Servers

GigaVUE-FM is tested with the LDAP implementation provided by Apache Directory Studio v2.0.0.v20130308. Although other implementations may operate acceptably, they have not been tested.

LDAP Over SSL

GigaVUE-FM supports secure LDAP implementation for authentication and authorization. You can select SSL or TLS as mode. To enable LDAP over SSL:

1. Generate the LDAP SSL certificate. The generated certificate has the DNS name of the LDAP server.
2. Configure the LDAP server in GigaVUE-FM with the same name as you have generated the client certificate. GigaVUE-FM ensures that the DNS name provided in GigaVUE-FM configuration and the DNS name provided in public certificate for the given LDAP server (while communicating over SSL) are the same. In case of mismatches, GigaVUE-FM will not communicate to LDAP over SSL and the authentication will fail.
3. Upload the generated LDAP SSL certificate to GigaVUE-FM trust store.
4. Reboot GigaVUE-FM.

LDAP Server Section: Controls and Fields

LDAP has the following buttons that allow you to manage the information.

Controls	Description
Add Server	Allows you to add a new LDAP Server to the list. See Add a New LDAP Server for details.
Action	Click the Action drop-down button to perform the following: Edit : Allows you to change the settings for an existing LDAP Server in the list. Select a server's entry and click Edit to open a dialog where you make the changes. Delete : Allows you to delete an LDAP Server entry.
Default Settings	Set default options for LDAP Servers. When you add a new LDAP Server to the list, you have the option of accepting these default settings or providing custom values. See Set Default Options for LDAP Servers for details.

Add a New LDAP Server

Select **Authentication Server > LDAP** and click **Add**. The Add LDAP Server dialog is displayed. Enter the following details and click **Save**:

- Server IP/DNS Name
- Priority

A new LDAP Server is added to the list view.

All other settings for LDAP servers are inherited from the defaults configured by clicking the **Default Settings** button at the top of the **LDAP** page. Refer to [Set Default Options for LDAP Servers](#) for details.

Set Default Options for LDAP Servers

Click **Default Settings** to set configuration options for use with all new LDAP server entries, and then set the following options for LDAP servers. Note that these options are all global options and cannot be configured on a per-host basis.

Setting	Description
User Base DN	Identifies the base distinguished name (location) of the user information in the schema of LDAP server. Provide the value as a string with no spaces.
User Search Scope	Specifies the search scope for the user under the base distinguished name (DN): Subtree (default) – Searches the base DN and all of its children. One-Level – Searches only the immediate children of the base DN.
Login UID	Specify the name of the LDAP attribute containing the login name. The default is sAMAccountName . You can also specify a custom string or uid (for User ID).
Bind Password	Provides the credentials to be used for binding with the LDAP server. If Bind DN is left undefined for anonymous login (the default), Bind Password should be left undefined, too.
Group Base DN	Set this option to require membership in a specific Group Base DN for successful login to the appliance. By default, the Group Base DN is left empty – group membership is not required for login to the system. If you do specify a Group Base DN , the attribute specified by the Group Login Attribute option must contain the user's distinguished name as one of the values in the LDAP server or the user will not be logged in.
Bind DN	Specifies the distinguished name (DN) on the LDAP server with which to bind. By default, this is left empty for anonymous login.
Attribute	Use this argument to specify the name of the attribute to check for group membership. If you specify a value for Group Base DN , the attribute you name here will be checked to see whether it contains the user's distinguished name as one of the values in the LDAP server.
LDAP Version	Specify which version of LDAP to use. The default of Version 3 is the current standard; some older servers still use Version 2.
Port	Specify the port number on which the LDAP server is running. If you do not specify a port, the default LDAP authentication port number of 389 is used.
Timeout	Specifies how long the appliance should wait for a response from the LDAP server to an authentication request before declaring a timeout failure.

Setting	Description
	The valid range is 0-60 seconds; default value is five seconds.
SSL Mode	Enables SSL or TLS to secure communications with LDAP servers as follows: - None—Does not use SSL or TLS to secure LDAP - SSL—Secures LDAP using SSL over the SSL port. - TLS—Secures LDAP using TLS over the default server port. NOTE: SSL and TLS modes use TLS 1.2 for negotiation with the LDAP server and the default ports.
SSL Port	Specifies the LDAP SSL port number.
Referrals	Specifies the type of user information search in the LDAP servers. - Yes—Searches the user information in all the LDAP servers. - No—Searches the user information in the selected LDAP server.
Search Timeout	Specifies how long the appliance should wait for a response from the LDAP server over SSL/TLS port before declaring a timeout failure. The valid range is 0-60 seconds; default value is five seconds.

Delete an LDAP Server

To delete an LDP Server, do the following:

1. Select **Settings > Authentication Server > LDAP**.
2. Select the LDAP server to be deleted.
3. Click **Actions > Delete**.

Configure Remote User Group Mapping

GigaVUE-FM provides the ability to assign user groups to the members based on their existing directory server group membership.

Group Mapping enables you to assign a group (that has corresponding user role privileges) to the members of a specific group. Mapping a remote user group to a local user group provides a granular way the roles are assigned to a group when they log in to GigaVUE-FM. Moreover, this eliminates the need to create specific roles on the remote server, since a remote user group can be mapped to a local user group.

For example, consider a remote user group with name *User_Group1* (in LDAP server). If you map *User_Group1* to the Super Admin Group (local user group in GigaVUE-FM), then the users in the *User_Group1* will get the privileges of Super Admin Group when the user logs in to GigaVUE-FM. If other users from any other user group log in, these users will get the privileges of the user group configured in the default user group field.

NOTE: Only users belonging to the **Super Admin User Group** or users with write access to the GigaVUE-FM Security Management category can enable or disable Group Mapping.

Refer to the following steps to enable User Group Mapping:

1. Under **LDAP > User Group Mapping**, click on **New**.
2. Enter the **Remote Group Base DN** and select the required **Map to Group(s)** option for which you want the remote user group to map to.

The following table describes the settings.

Setting	Description
Remote Group Base DN	Specifies the user mapping for a specific Remote Group Base.
Map to Groups	Specifies groups that a remote group can be mapped to.

NOTE: Group Base DN is case insensitive. **CN=FMtest** is same as **cn=FMtest**.

3. Click **OK** to configure remote user group mapping.
4. Check **User Group Mapping** to enable it.

Now when a remote user logs in, they would be given the role of user admin.

LDAP Authentication Failure

LDAP authentication attempts can sometimes fail due to issues such as DNS, TCP, TLS, LDAP server reachability issues, FM configuration and, operational issues. Until software version 6.2.00, user needs to check the logs individually in GigaVUE-FM to troubleshoot these issues. Starting in software version 6.3.00, to enable better troubleshooting, GigaVUE-FM will display an error message in the description field of the audit logs for all the failed LDAP authentication attempts. For more information on error codes, Refer to [Audit Logs Failure](#).

External Authentication Server Group Assignments

For user group configuration, in TACACS+ and RADIUS, the following user group mapping configuration must be performed in the remote servers:

Remote Server	In GigaVUE-FM Release 5.7 and earlier (Role Mapping)	In GigaVUE-FM Release 5.8 and further (User Group Mapping)	Example
TACACS+	<mapping_local_user> [:role- <mapping_local_role_1> [role- <mapping_local_role_2> [...]]]	gigamon:groups=<comma separated FM groups>	gigamon:groups=Super Admin Group,Admin Group
RADIUS	<mapping_local_user> [:role- <mapping_local_role_1> [role- <mapping_local_role_2> [...]]]	Class=<comma separated FM groups>	Class=Super Admin Group,Admin Group

NOTE: After upgrading to release 5.8.00, you must reconfigure the user groups in the external authentication servers in the specified format to access GigaVUE-FM.

Assign User Groups in External Authentication Servers

Refer to [Configure User Groups in External Authentication Servers](#) for instructions on assigning the user groups in RADIUS, TACACS+, and LDAP servers.

Configure User Groups in External Authentication Servers

This section describes how to set up RADIUS, TACACS+, and LDAP servers to perform authentication for GigaVUE-FM, including how to include a local user mapping attribute that GigaVUE-FM can use to assign user groups to an externally-authenticated user. See the following sections for details:

- [Assign Groups with External Authentication Servers](#)
- [Configure Cisco ACS: RADIUS Authentication](#)
- [Configure Cisco ACS: TACACS+ Authentication](#)

Assign Groups with External Authentication Servers

GigaVUE-FM provides the following default user groups:

- **Super Admin User Group**— Allows users associated with this group to do everything in GigaVUE-FM, including adding or modifying users and configuring all AAA settings in the RADIUS, TACACS+, and LDAP pages. Can change password for all users.
- **Admin User Group** — Allows users associated with this group to do everything in GigaVUE-FM except adding or modifying users and change AAA settings. Can only change their own password.
- **View Only User Group**— Allows a user to view everything in GigaVUE-FM, including AAA settings, but not make any changes. Can only change their own password.

NOTE: Access control for each of the groups is based on roles and tags. Refer to the following sections for details: [Roles and Users](#).

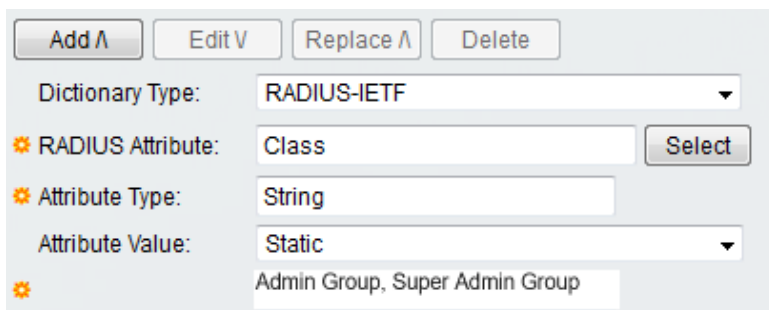
The default groups can be assigned based on the groups assigned in the external authentication server. Refer to Use AAA Server Role Assignments for details.

Configure Cisco ACS: RADIUS Authentication

Use the following steps to configure Cisco ACS 5.x (RADIUS) for externally authenticated groups in GigaVUE-FM:

1. Navigate to **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles** and click **Create** to add a new authorization profile.
2. Give the profile a name and description and click on the **RADIUS Attributes**.
3. Leave **Dictionary Type** set to **RADIUS-IETF** and click the **Select** button adjacent to the **RADIUS Attribute** field.
4. Select the **Class** attribute from the dialog that appears and click **OK**.
5. Leave the **Attribute Type** and **Attribute Value** fields at their default value (**String** and **Static**, respectively).
6. Provide the list of GigaVUE-FM specific groups in the following format:

Class=<comma separated FM groups> with no space in between the groups



The screenshot shows the 'RADIUS Attributes' configuration window in Cisco ACS 5.x. At the top are buttons: 'Add A', 'Edit V', 'Replace A', and 'Delete'. Below these are the following fields:

- Dictionary Type:** A dropdown menu set to 'RADIUS-IETF'.
- RADIUS Attribute:** A text field containing 'Class' with a 'Select' button to its right.
- Attribute Type:** A text field containing 'String'.
- Attribute Value:** A dropdown menu set to 'Static'.
- Below the 'Attribute Value' field is a text input field containing 'Admin Group, Super Admin Group'.

7. Click the **Add** button  to add this attribute to the authorization profile.
8. Assign this authorization profile to a group and populate it with GigaVUE-FM users.

Figure 8 Supplying the Class Field for RADIUS (ACS 5.x) shows these settings in a CiscoSecure ACS 5.x authorization profile.

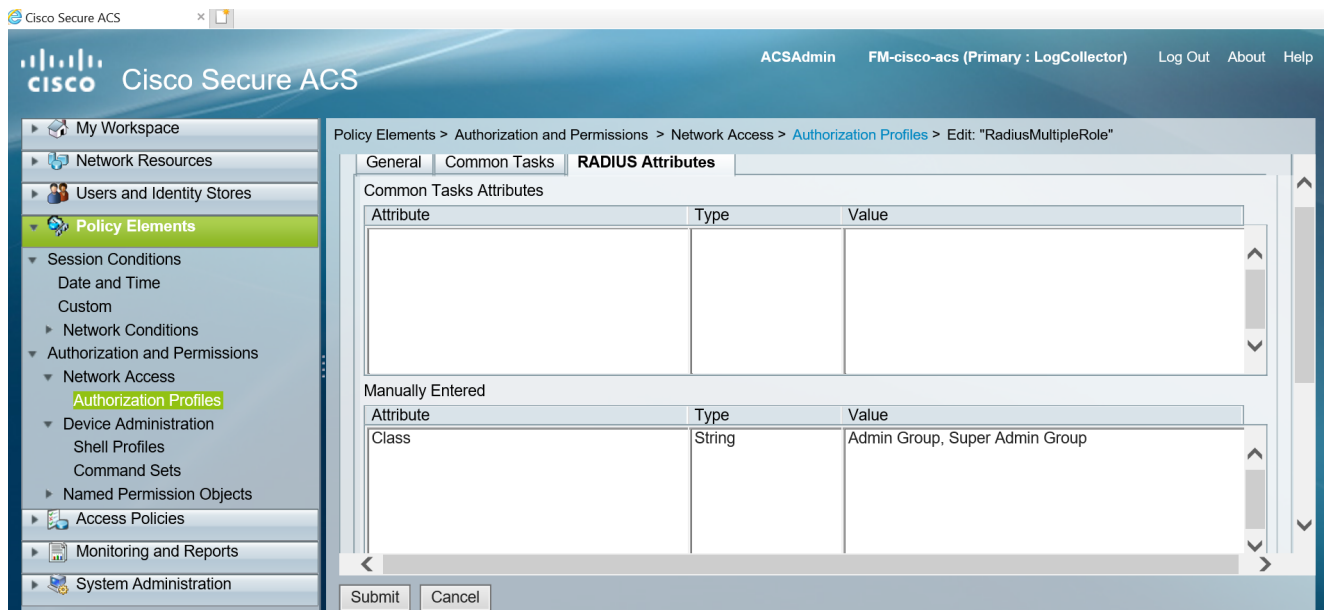


Figure 8 Supplying the Class Field for RADIUS (ACS 5.x)

Configure Cisco ACS: TACACS+ Authentication

Use the following steps to configure Cisco ACS 5.x (TACACS+) to assign user groups to externally authenticated users in GigaVUE-FM:

1. Navigate to **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles** and click **Create** to add a new shell profile.
 - a. Give the profile a name and description in the **General** page.
 - b. Click the **Custom Attributes** page.
 - c. Set the **Attribute** field to **local-user-name**.
2. Leave the **Requirement** and **Attribute Value** fields at their default value (**Mandatory** and **Static**, respectively).
3. Provide the list of GigaVUE-FM specific groups in the following format:

gigamon:groups=Super Admin Group,Admin Group

Buttons: Add, Edit, Replace, Delete, Bulk Edit

Attribute: local-user-name

Requirement: Mandatory

Attribute Value: Static

Value: bposey,role-fm_super_admin

4. Click the **Add** button  to add this attribute to the shell profile.
5. Click **Submit** to finalize this shell profile.
6. Create Service Selection Rules that will assign this shell profile to desired GigaVUE users.

Figure 9 Supplying local-user-name and groups in ACS 5.x for TACACS+ shows the an example of a shell profile for TACACS+ in ACS 5.x with the local-user-name attribute supplied.

Cisco Secure ACS

ACSAdmin FM-cisco-accs (Primary : LogCollector) Log Out About Help

Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "tacacs-multirole"

Manually Entered

Attribute	Requirement	Value
gigamon:groups	Mandatory	Super Admin Group,Admin Group

Buttons: Add, Edit, Replace, Delete, Bulk Edit

Attribute:

Requirement: Mandatory

Buttons: Submit, Cancel

Figure 9 Supplying local-user-name and groups in ACS 5.x for TACACS+

Configure Cisco Identity Services Engine (ISE): RADIUS Authentication

NOTE: The instructions given in the topic are based on ISE v3.3.x.

1. Log into ISE.
2. Go to **Administration>Network Devices**.
3. Click **Add**. The **New Network Device** page appears.
 - a. Enter the device name in the **Name** field.
 - b. Enter the IP address and net mask value of the GigaVUE-FM device in the **IP Address** field.
 - c. Select the **RADIUS Authentication Settings** checkbox.
 - d. Configure a key for the RADIUS authentication in the **Shared Secret** field.
4. Click **Submit**.
5. Go to **Administration>Identity Management>Identities**.
 - a. Create users for RADIUS authentication.
6. Go to **Administration>Identity Management>Groups>User Identity Groups**.
 - a. Create user groups and assign the users to specific user groups.

NOTE: Refer Add Users and Create User Groups topics in [CISCO ISE documentation](#) for more information.

7. Go to **Policy>Policy Elements>Results**.
8. In the **Results** page, go to **Authorization>Authorization Profiles**.
 - a. Click **Add** to create an authorization profile that will be mapped to the user groups.
 - b. Enter the name for the authorization profile in the **Name** field.
 - c. In the **Common Tasks** section, select the **ASA VPN** option and enter the user group that needs to be mapped to the user group in GigaVUE-FM
9. Go to **Policy>Policy Sets**. The **New Policy Set** page appears.
10. . Do the following steps to create a new policy.
 - a. In the **Authentication Policy** section, create an authentication rule and map it to the users who can be authenticated to access GigaVUE-FM through RADIUS authentication.
 - b. In the **Authorization Policy** section, create an authorization rule that maps the user groups with the created RADIUS authorization profile.

Configure Cisco Identity Services Engine (ISE) TACACS+ Authentication

1. Log into ISE.
2. Go to **Administration>Network Devices**.
3. Click **Add**. The **New Network Device** page appears.
 - a. Enter the device name in the **Name** field.
 - b. Enter the IP address and net mask value of the device in the **IP Address** field.
 - c. Select the **TACACS Authentication Settings** checkbox.
 - d. Configure a key for the RADIUS authentication in the **Shared Secret** field.
4. Click **Submit**.
5. Go to **Administration>Identity Management>Identities**.
 - a. Create users for TACACS authentication.
6. Go to **Administration>Identity Management>Groups>User Identity Groups**.
 - a. Create user groups and assign the users to specific user groups.

NOTE: Refer Add Users and Create User Groups topics in [CISCO ISE documentation](#) for more information.

7. Go to **Work Centers>Policy Elements>Results>TACACS Profile**. In the TACACS Profile tab, **Common Tasks** and **Custom Attributes** sections appears.
 - a. In the **Custom Attributes** section, click **Add** and create an attribute with the Type as Mandatory, Name as gigamon:groups and Value as the GigaVUE-FM group name.
8. Go to **Work Centers>Device Admin Policy Sets**. The **New Policy Set** page appears.
9. Do the following steps to create a new policy.
 - a. In the **Authentication Policy** section, create an authentication rule and map it to users who can be authenticated to access GigaVUE-FM through RADIUS authentication.
 - b. In the **Authorization Policy** section, create an authorization rule that maps the user groups with the created TACACS authorization profile.

Device Authentication Services

The Device Authentication Services page consists of the following tabs with which you can manage the global configuration of devices:

- [Default](#)
- [Managed Nodes](#)

Defaults

With the Defaults page you can configure the authentication priority and user mapping settings globally for all the devices managed by GigaVUE-FM.

- **Authentication Priority:** Specify the authentication methods that must be used for logging in to the GigaVUE HC series node as well as the order in which they must be used.
- **User Mapping:** Specify the Map Order and Map Default User details.

NOTE: GigaVUE-FM and devices must be running software version 5.13.01 and above.

To access the Defaults page:

1. Go to **Settings** and select **Authentication > Device Authentication Services > Defaults**.
2. Select or Enter the required details.
3. Click **Save** to save the configuration.

The configurations performed in this page are similar to the configurations performed from the devices. Refer to the following topics in the GigaVUE-OS section for details:

To configure	Refer
Authentication Priority	Refer to the "Configure AAA Authentication Options" section in the respective Physical Appliances documentation page.
User mapping	Refer to the "User Mapping" section in the respective Physical Appliances documentation page.

LDAP

With the LDAP page in GigaVUE-FM you can perform the LDAP Server and the LDAP User Group mapping configurations globally for all the nodes managed by GigaVUE-FM.

NOTE: GigaVUE-FM and devices must be running software version 5.13.01 and above.

To access the LDAP page:

1. Go to **Settings** and select **Authentication > Device Authentication Services > LDAP**.
2. Select **LDAP Server** to configure LDAP server details. Click **Add Server** to add a new LDAP server.
3. Click **LDAP Default Settings** to configure the settings to be applied to all LDAP servers.

Global configuration from GigaVUE-FM is similar to the configuration performed in the devices. Refer to the following sections for details:

To configure	Refer to...
LDAP server	Add an LDAP Server
LDAP Default All settings	Set the LDAP Server Default Settings

Use the **Audit** button to audit all the LDAP servers in all the nodes managed by GigaVUE-FM.

Configure Remote User Group Mapping

Refer to the following steps to enable User Group Mapping:

1. Under **LDAP > LDAP User Group Mapping**, click **Add Remote User Group**.
2. In the Add Remote User Group for Sync, enter Enter the **Remote Group Base DN** and select the required **Map to Group(s)** option for which you want the remote user group to be mapped to.

The following table describes the settings.

Setting	Description
Remote Group Base DN	Specifies the user mapping for a specific Remote Group Base.
Map to Groups	Specifies groups that a remote group can be mapped to.

NOTE: Group Base DN is case insensitive. **CN=FMtest** is same as **cn=FMtest**.

3. Click **Ok** to configure the remote user group mapping.
4. Check **User Group Mapping** in **Default Settings** to enable it.



Notes:

- On deletion of the last LDAP server from GigaVUE-FM, the LDAP User Group Mapping will be deleted, but the LDAP Default Settings will remain.
- When you add a new device, LDAP Default Settings/LDAP User Group Mapping will not be applied if the LDAP server is not configured.

Configure Tokens

You must configure tokens for registering GigaVUE Fabric Components using Third Party Orchestration and registering UCT-V with GigaVUE-FM.

This feature verifies the identity of a user for accessing the GigaVUE-FM REST APIs by generating tokens.

GigaVUE-FM allows you to generate a token only if you are an authenticated user and based on your privileges in accessing the GigaVUE-FM. You can copy the generated tokens from the GUI, which can be used to access the REST APIs. Token inherits the Role-Based Access (RBAC) privilege (read or write) of the user groups assigned to a particular user.

GigaVUE-FM enables the generation of multiple tokens and associates them with the corresponding user groups. If you have GigaVUE-FM Security Management privileges with write access, you can revoke other users' tokens but not view the created tokens.

Prerequisite

You must create user groups in GigaVUE-FM. For details, refer to

Rules and Notes

- Authentication using a token is an additional mechanism to access GigaVUE-FM REST APIs, and it does not replace the existing GigaVUE-FM authentication mechanism.
- Only authenticated users can create tokens.
- The token expires or becomes invalid under the following circumstances:
 - Based on the configured value for expiry:
 - Default value: 30 days
 - Maximum value: 105 days
 - Deleting a related user group that exists as part of the token leads to deletion of the corresponding token.
 - A password change for the user(local) deletes the corresponding token.
 - A change in the authentication type deletes all the tokens.
- During the back up and restoration of GigaVUE-FM, previously generated tokens are not available.
- In FMHA role changeover, active GigaVUE-FM tokens are active.
- For basic authentication, activities such as creating, revoking, and reviewing of Token APIs are restricted.
- For expired or invalid tokens, you notice the error code 401 on GigaVUE-FM REST API access.

This section explains about the following:

- [Create Token](#)
- [Revoke Tokens](#)
- [Export Token](#)
- [Configure Tokens](#)

Create Token

GigaVUE-FM allows you to create a token or multiple tokens if required.

To create a token, follow these steps:

1. Go to , select **Authentication > GigaVUE-FM User Management**. The **User Management** page appears.
2. In the **User Management** page, select **Tokens**.

NOTE: If you are a user with write access, then you can view a drop-down list under **Tokens**. Select **Current User Tokens** to create a token.

3. Select **New Token**.
4. Enter a name for the new token in the **Name** field.
5. Enter the days until the token is valid in the **Expiry** field.
6. Select the user group for which you are privileged to access GigaVUE-FM from the **User Group** drop-down list.
7. Select **OK** to generate a new token.

The generated token appears on the **Tokens** page. You can copy and use the generated token to authenticate the GigaVUE-FM REST APIs.

Copy and Paste a Token

1. Select the token that you want to copy.
2. Select **Actions>Copy Token**.

The token is copied.

3. Paste the copied token in the required areas.

NOTE: You cannot view the generated token. You can only copy and paste the generated token.

Revoke Tokens

You can revoke tokens that other users create.

Prerequisite: Write access in GigaVUE-FM Security Management.

To revoke tokens,

1. Go to , select **Authentication > GigaVUE-FM User Management**.
2. In the **User Management** page, select **Tokens**.
3. From the drop-down, select **Token Management**. You can view the created tokens.
4. Select the token that you want to revoke.
5. Select **Action> Revoke**.

Export Token

GigaVUE-FM allows you to export selected or all the tokens in CSV and XLSX format.

- To export a token, select the token, select the **Export Selected** drop-down list box, and then select the **CSV** or **XLSX** format as per requirement.
- To export all the tokens, select the token, select the **Export All** drop-down list box, and then select the **CSV** or **XLSX** format as per requirement.

Single Sign-On

Single sign-on (SSO) is an authentication process that allows a user to access multiple applications with a single set of log in credentials. GigaVUE-FM provides the following Single sign-on options, which are discussed in this topic:

- [Internal IdP](#)
- [External IdP](#)

Internal IdP

GigaVUE-FM uses Shibboleth SAML 2.0 identity provider (open source IdP) as an internal IdP for authentication and authorization. Shibboleth reads the data from GigaVUE-FM's local database and performs the authentication based on the authentication mechanism selected in the **Authentication Type** settings. GigaVUE-FM is independent of the authentication mechanism (as Shibboleth takes care of authentication and authorization).

Notes:

- GigaVUE-FM starts with internal IdP, by default.
- When you access GigaVUE-FM, you will be navigated to the IdP's URL. You must then log in with your user name and password.
- If you cannot access GigaVUE-FM (due to server issues or any other issues), you can use the special access provided (<https://<fm ip address/dns name>/admin>). This access is applicable only for local users with super admin privileges.
- You must restart GigaVUE-FM every time you configure IdP.

External IdP

The following external IdPs are qualified to be operational with GigaVUE-FM:



NOTE: To configure the Assertion Consumer Service (ACS) URL for FM in the External IDP SSO configuration, follow these steps:

1. Navigate to `https://<FM IP Address>/saml/metadata`. This will download the XML metadata file.
2. Extract the ACS URL from the downloaded XML file.
3. Use this ACS URL to configure the External IDP accordingly.

Ensure that the correct ACS URL from the FM metadata is set in the **Single Sign On URL** field on External IDP for proper integration.

- [ADFS](#)
- [OKTA](#)
- [Microsoft Azure](#)

ADFS

To configure ADFS as external IdP you must perform the following:

1. To configure GigaVUE-FM in ADFS. Refer to [Configure GigaVUE-FM in ADFS](#) for details.
2. Configure external IdP, that is ADFS, in GigaVUE-FM. Refer to [Configure External IdP in GigaVUE-FM](#) for details.
3. Refer to the [Trust Store](#).

NOTE: When you access GigaVUE-FM using the external IdP, you will be navigated to the external IdP URL (Microsoft ADFS). You must then log in using the external IdP user name and password for logging in to GigaVUE-FM.

External IdP Login Screen(ADFS)

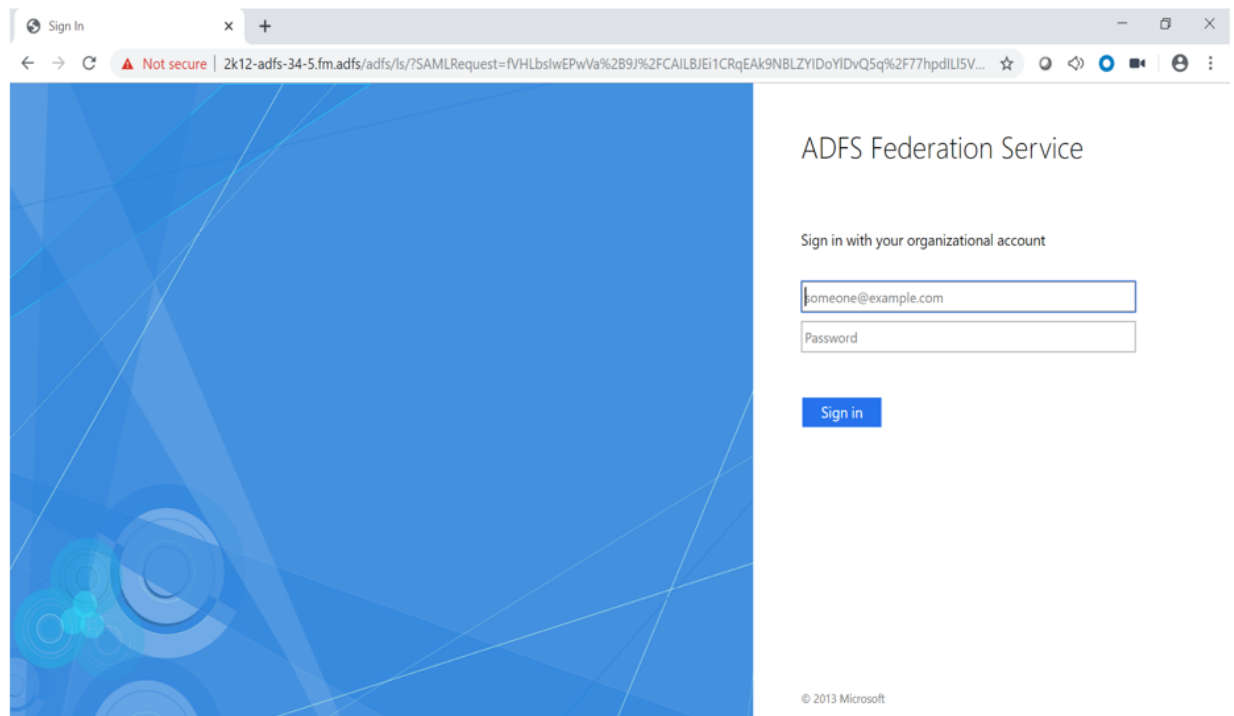


Figure 1 External IdP Login Screen (ADFS):

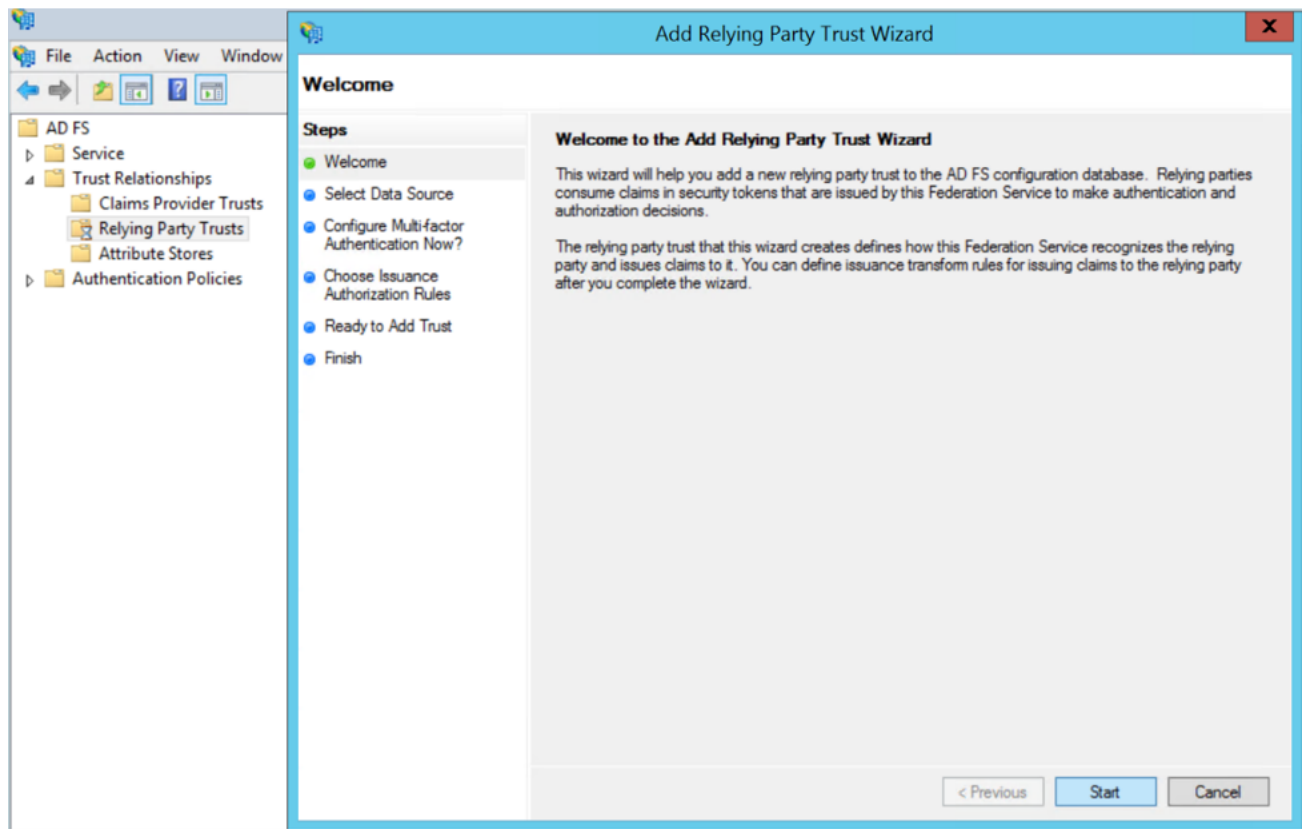
Configure GigaVUE-FM in ADFS

Prerequisite:

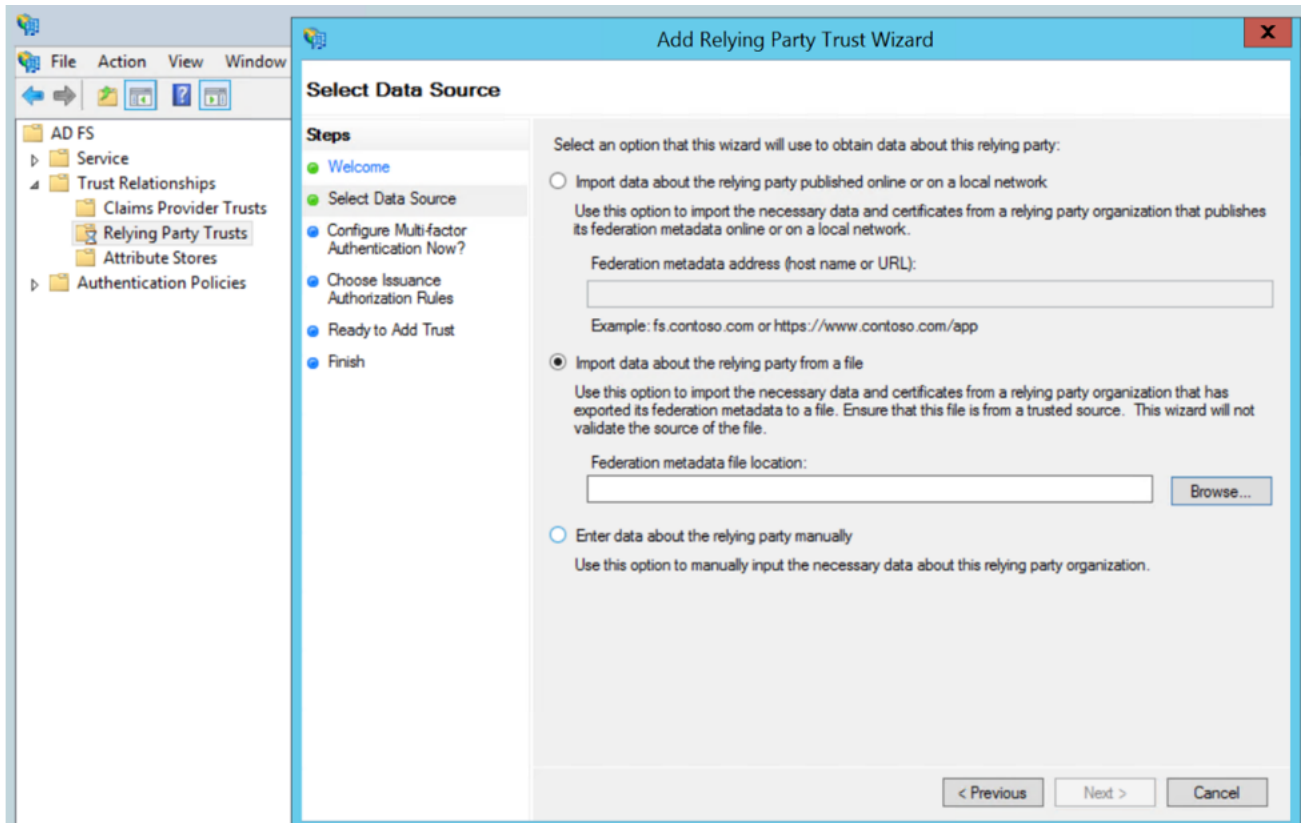
You must retrieve the Service Provider metadata (which is GigaVUE-FM's metadata) from <https://<FM IP Address>/saml/metadata>. This will serve as the service provider metadata file to configure in IDP.

To configure GigaVUE-FM in ADFS as Relying Party:

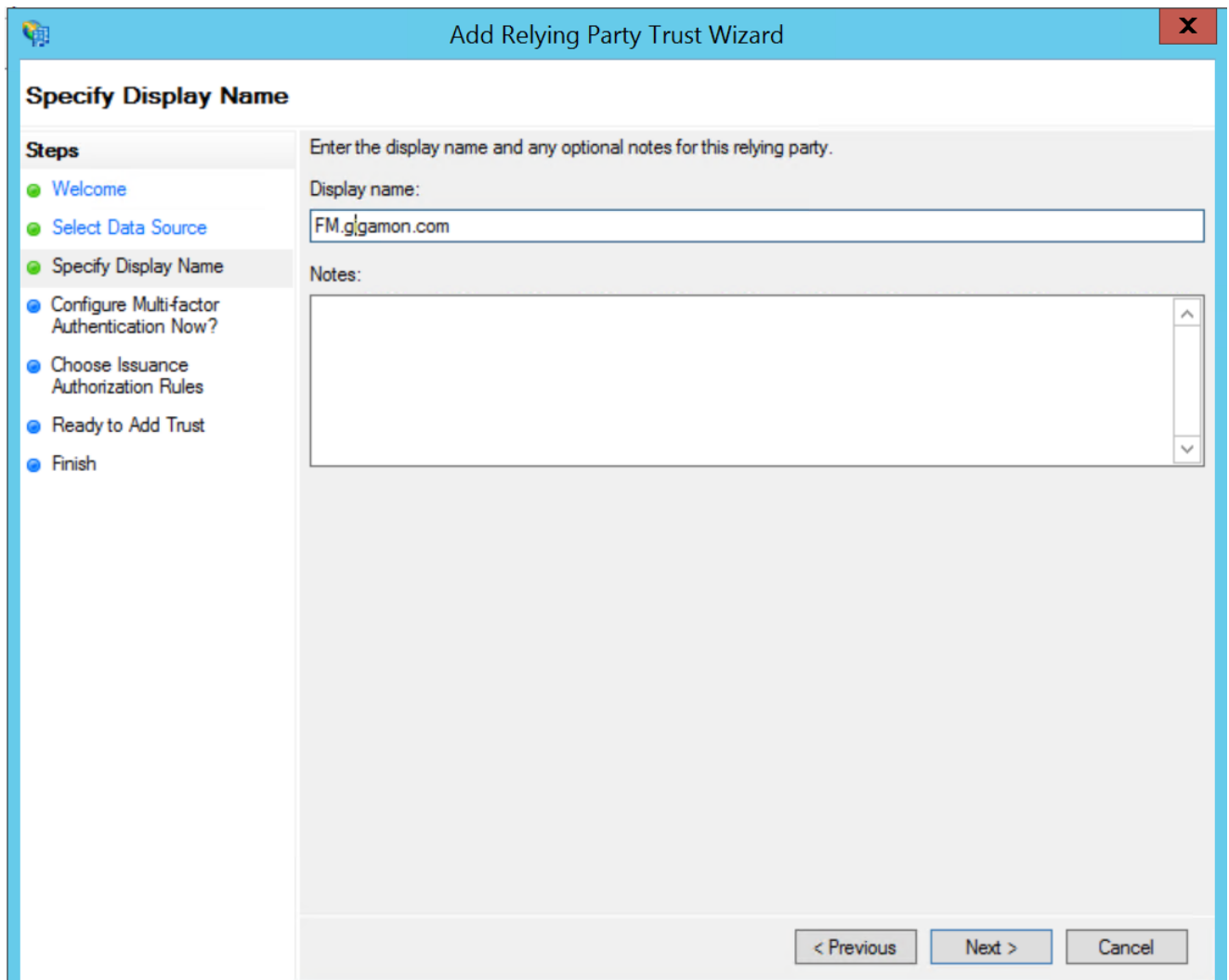
1. From the windows server, select **Start > Administrative Tools > ADFS Management**. The ADFS administrative console appears.
2. Select ADFS folder. Go to the **Actions** menu and select **Add Relying Party Trusts**.



3. **Select Data Source:** Select the **Import Data About the Relying Party from a File** option. Browse for the SAML metadata file as mentioned in the prerequisites.



4. Specify a **Display Name** that identifies the application, example, FM.gigamon.com. Click **Next**.



The image shows a screenshot of the 'Add Relying Party Trust Wizard' window, specifically the 'Specify Display Name' step. The window has a blue title bar with the text 'Add Relying Party Trust Wizard' and a red close button. On the left, a 'Steps' pane lists the following steps: 'Welcome' (green dot), 'Select Data Source' (green dot), 'Specify Display Name' (green dot and highlighted), 'Configure Multi-factor Authentication Now?' (blue dot), 'Choose Issuance Authorization Rules' (blue dot), 'Ready to Add Trust' (blue dot), and 'Finish' (blue dot). The main area of the wizard is titled 'Specify Display Name' and contains the instruction 'Enter the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' label followed by a text box containing 'FM.gigamon.com'. Below the text box is a 'Notes:' label followed by a large, empty text area with a vertical scrollbar. At the bottom right of the wizard, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

Add Relying Party Trust Wizard

Specify Display Name

Enter the display name and any optional notes for this relying party.

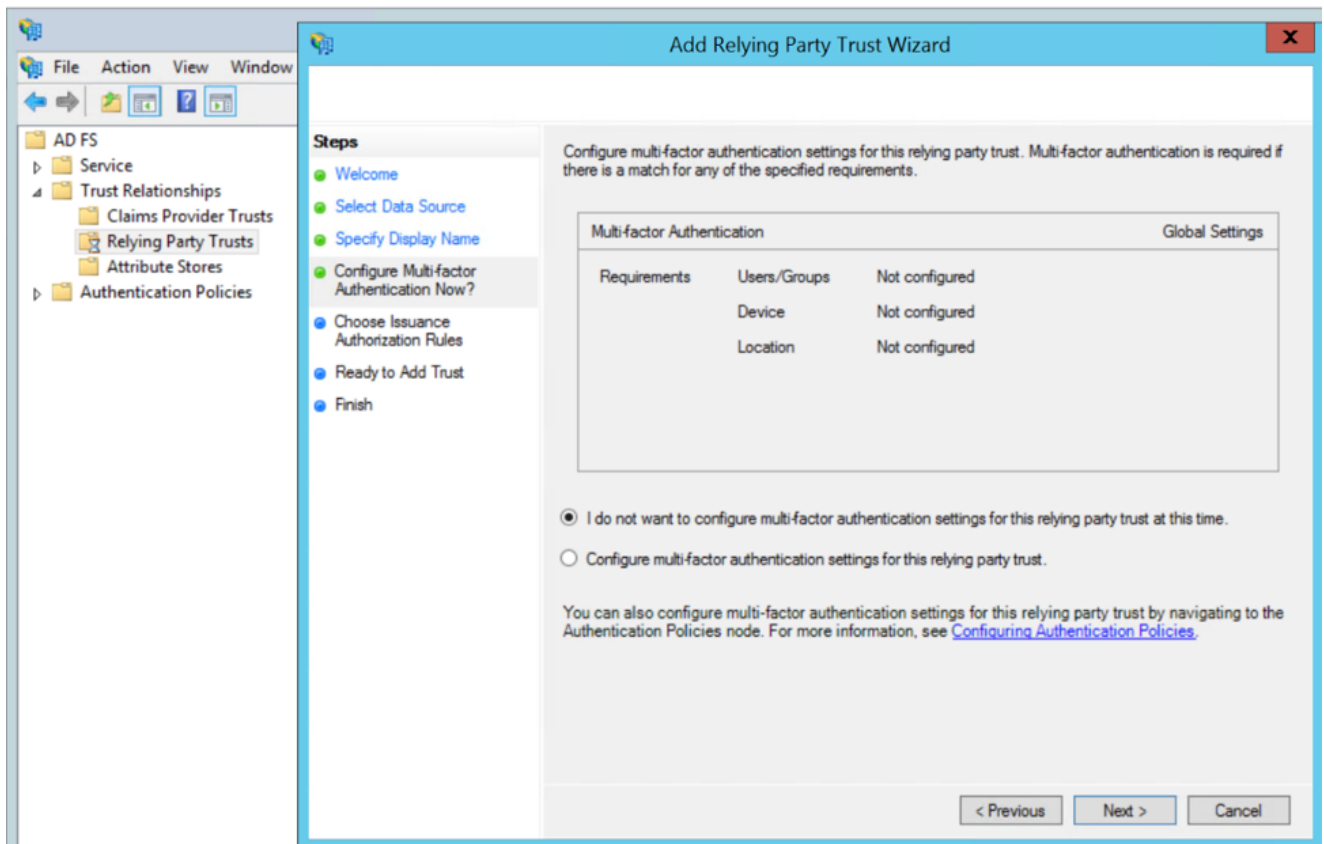
Display name:

FM.gigamon.com

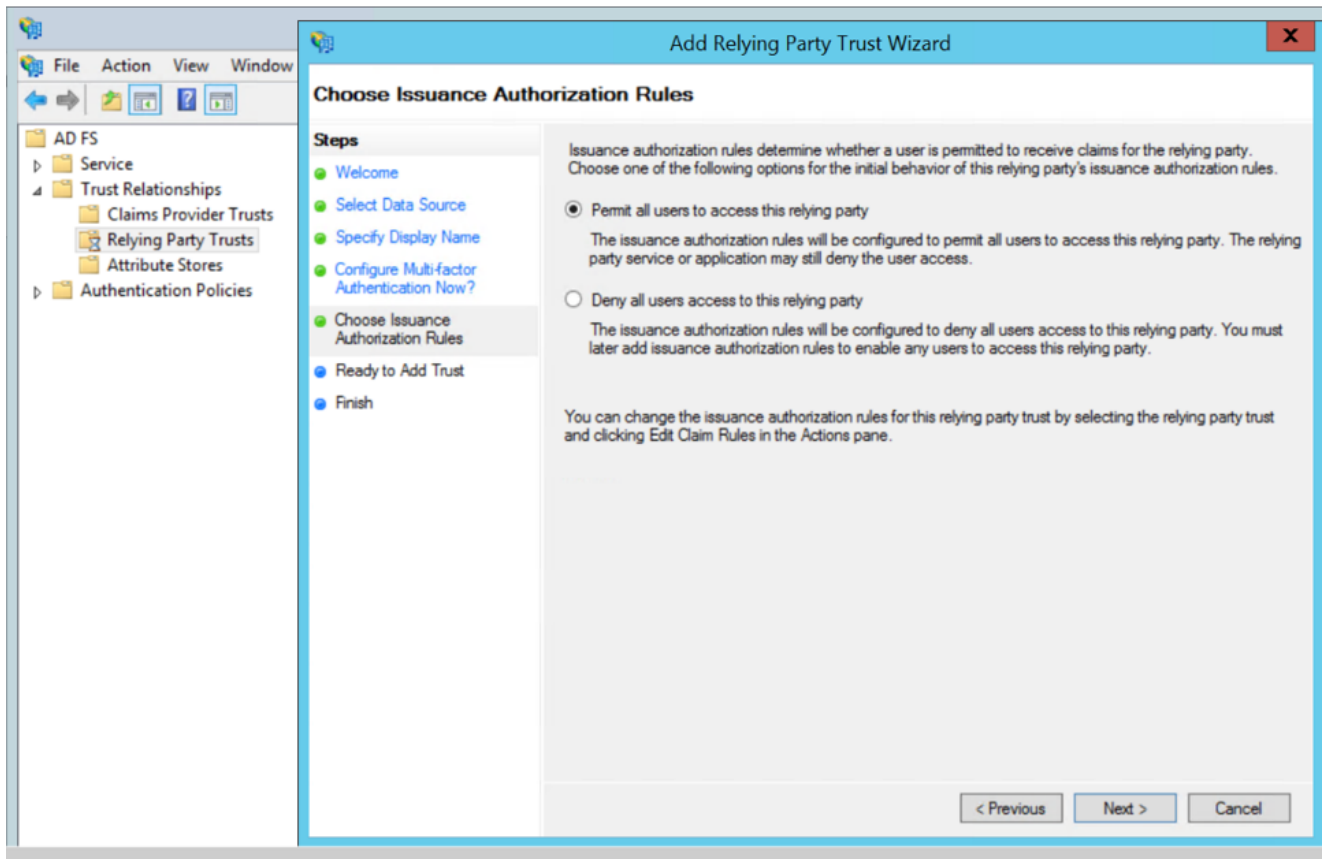
Notes:

< Previous Next > Cancel

5. Select the option **I do not want to configure MFA** and click **Next**.



6. Select **Permit all users to access this relying party**. Click **Next**.



7. Review the data available in preview section and add the relying party.
8. Open **Edit Claim rules** to grant user access:
 - a. Add a New claim rule to transform UserPrincipalName as Namelid:
 - i. Choose the option send LDAP Attributes as claims.
 - ii. Specify claim rule name and choose the required LDAP store.
 - iii. Select LDAP Attribute as UserPrincipalName and outgoing claim type as Namelid.
 - b. Add a New Claim Rule to specify user specific access:
 - i. Choose the option send Group Membership as claim.
 - ii. Specify claim rule name and select AD user group for which FM roles/user Groups must be assigned.
 - iii. Enter outgoing claim type as SAML User Group value configured in GigaVUE-FM (default value is eduPersonAffiliation) and outgoing claim value as one of the following:
 - GigaVUE-FM specific user groups (Super Admin Group or Admin Group or User Group)
 - Organizational specific user group. If organizational specific user group is provided, then you must enable Organizational Group Mapping.

OKTA

To configure OKTA as external IdP you must perform the following:

1. Configure GigaVUE-FM in OKTA. Refer to [Configure GigaVUE-FM in OKTA](#) for details.
2. Configure external IdP, that is OKTA, in GigaVUE-FM. Refer to [Configure External IdP in GigaVUE-FM](#) for details.
3. Install IdP signing certificates (OKTA) in GigaVUE-FM. Refer to the [Trust Store](#).

NOTE: When you access GigaVUE-FM using the external IdP, you will be navigated to the external IdP URL (OKTA). You must then log in using the external IdP user name and password for logging in to GigaVUE-FM.

Configure GigaVUE-FM in OKTA

Prerequisite:

You must retrieve the Service Provider metadata (which is GigaVUE-FM's metadata) from <https://<FM IP Address>/saml/metadata>. This will serve as the sp metadata file to configure in IDP.

Watch the video for configuring OKTA here: [Gigamon Basics: Enabling Single sign-on into Fabric Manager \(SAML\)](#).

To configure GigaVUE-FM in OKTA as External IdP:

1. Login to Okta.
2. Enter the following details:

Field	Description
New Application	
Platform	Web
Sign on Method	SAML 2.0
General Settings	
App Name	Fabric Manager
Configure SAML	
Single Sign on URL	Assertion Consumer Service URL from the service provider metadata. Enable the <i>Use this for Recipient and Destination Address</i> checkbox. NOTE: If you configure External IDP SSO authentication using a CNAME record for the FM DNS name, you must add both URLs to the IDP configuration to ensure seamless SSO: The CNAME-based URL - https://<CNAME>/saml/SSO The FM DNS-based URL - https://<DNS>/saml/SSO
Entity ID	Paste the entity id copied from the Authentication Type page.
Name ID Format	Enter Email Address as name id format.
Authentication User Name	OKTA User Name
Attributes	
Name	SAML User Group Name
Name Format	Basic
Value	Email
Group Attribute Statements	Configure the proper Group Attribute Statements in OKTA
Create SAML Integration	
Enable the check box <i>I am on OKTA Customer adding an internal app.</i>	

NOTE: Click **Identity Provider Metadata** and copy the URL in the address bar and paste it under third party authentication URL.

NOTE: Ensure to download the OKTA Certificate for uploading in Trust Store.

Microsoft Azure

To configure Microsoft Azure as an external IdP you must perform the following:

1. Configure GigaVUE-FM in Azure. Refer to [Configure GigaVUE-FM in Microsoft Azure](#) section for details.
2. Configure external IdP, that is Azure, in GigaVUE-FM. Refer to [Configure External IdP in GigaVUE-FM](#) for details.
3. Install IdP signing certificates in GigaVUE-FM. Refer to the [Trust Store](#).

NOTE: When you access GigaVUE-FM using the external IdP, you will be navigated to the external IdP URL (Microsoft Azure). You must then log in using the external IdP user name and password for logging in to GigaVUE-FM.

Configure GigaVUE-FM in Microsoft Azure

Prerequisite:

You must retrieve the Service Provider metadata (which is GigaVUE-FM's metadata) from <https://<FM IP Address>/saml/metadata>. This will serve as the sp metadata file to configure in IDP.

To configure GigaVUE-FM in Microsoft Azure as External IdP:

1. Log in to Microsoft Azure.
2. Create a new non-gallery application under non Enterprise applications.
3. From the application, access the single sign on option.

NOTE: To configure the SSO url and certificates: you can either perform the manual configuration or upload the metadata file directly using the **Upload Metadata File** option. The following steps are based on uploading the metadata file option.

4. Select **Upload Metadata file**. Upload the metadata taken from GigaVUE-FM. The SSO attributes will be retrieved by default, except the **Unique User Identifier** field.

Field	Description
Basic SAML Configuration	
Identifier (Entity ID)	azure-sso
Reply URL (Assertion)	https://xx.xx.xx.xx:xxx/saml/sso

Field	Description
Consumer Service URL)	NOTE: If you configure External IDP SSO authentication using a CNAME record for the FM DNS name, you must add both URLs to the IDP configuration to ensure seamless SSO: The CNAME-based URL - https://<CNAME>/saml/SSO The FM DNS-based URL - https://<DNS>/saml/SSO
Sign on URL	Optional
Relay State	Optional
Logout URL	https://xx.xx.xx.xx:xxx/saml/singlelogout
User Attributes and Claims	
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
user group name	user.groups
Unique User Identifier	Enter <i>user.userprincipalname</i> .
SAML Signing Certificate	
Status	Active
Thumbprint	
Expiration	
Notification Email	
App Federation Metadata URL	
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download
Set up FM SSO	
You'll need to configure the application to link with Azure AD.	
Login URL	
Azure Identifier	

NOTE: To configure GigaVUE-FM to link with Azure AD, copy the login URL and paste it in the Third Party Authentication URL in the Authentication Type page.

NOTE: Download the certificate (Base64) from Azure and upload in the trust store. Trust store is available under **Administration -> System -> Certificates -> Trust store**.

How Single Sign-on Works

Whenever a user attempts to log in to the GigaVUE-FM user interface, GigaVUE-FM validates if the user is logging in using the internal IdP or External IdP (organization IdP), based on which the signing-in process differs. Refer to the following sections for details:

- [GigaVUE-FM Configured with Internal IdP](#)
- [GigaVUE-FM Configured with External IdP](#)
- [GigaVUE-FM Configured with Internal IdP](#)

GigaVUE-FM Configured with Internal IdP

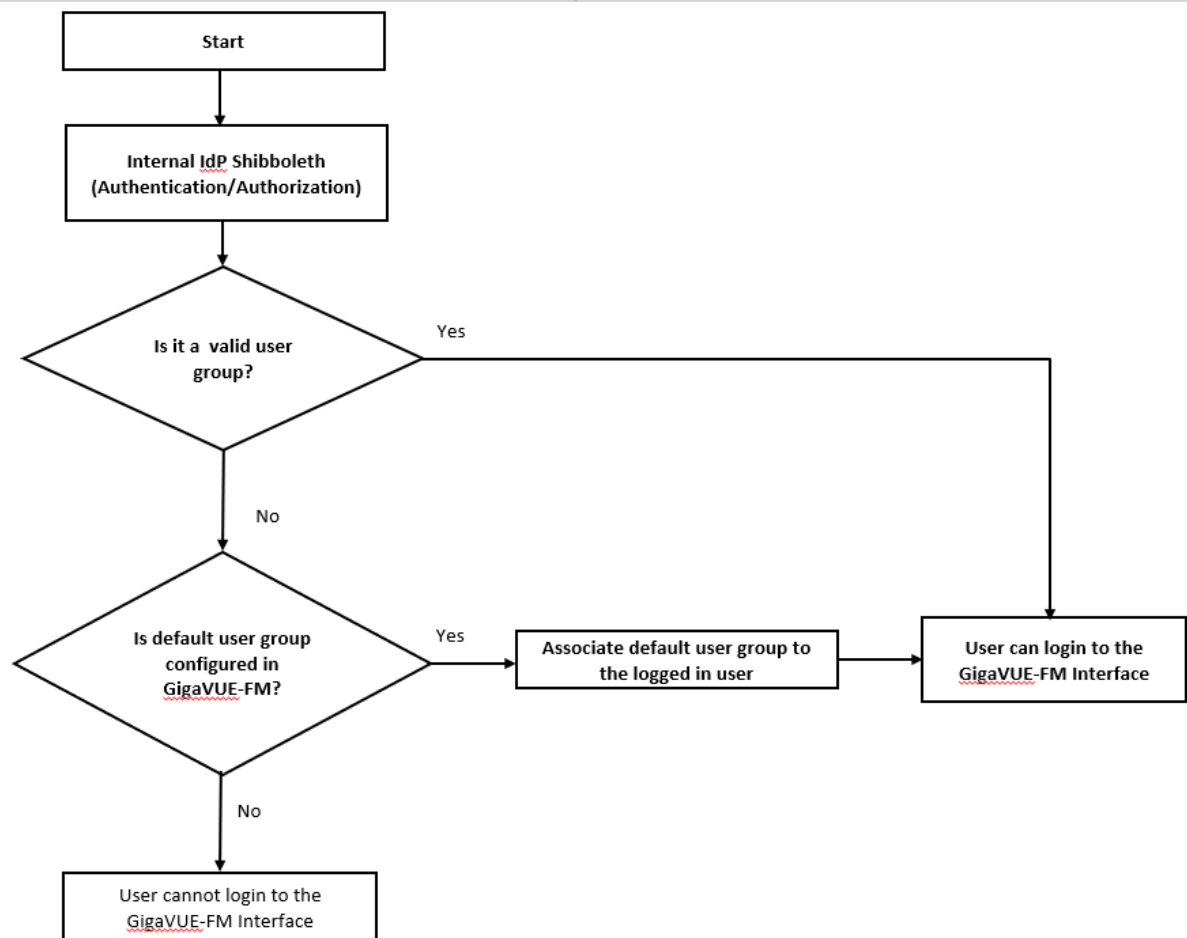
If GigaVUE-FM is configured with internal IdP:

1. GigaVUE-FM sends a request to Shibboleth for authentication.

NOTE: GigaVUE-FM's custom certificate and service provider certificate are the same. To install custom certificate, refer to the Trust Store section for more details.

2. Shibboleth reads and verifies the **Authentication Type** setting in GigaVUE-FM and performs the authentication and authorization:
 - If the user group is configured and if the user group is a valid user group, then the user is allowed to log in to the GigaVUE-FM user interface.
 - If the user group is not configured:
 - if a default user group is configured in GigaVUE-FM, then the user is allowed to log in to the GigaVUE-FM user interface using the default user group.
 - if a default user group is not configured in GigaVUE-FM, then the user is not allowed to log in to the GigaVUE-FM user interface.

Refer to the following flow diagram for detailed flow of the internal IdP process:



GigaVUE-FM Configured with External IdP

If GigaVUE-FM is configured with external IdP:

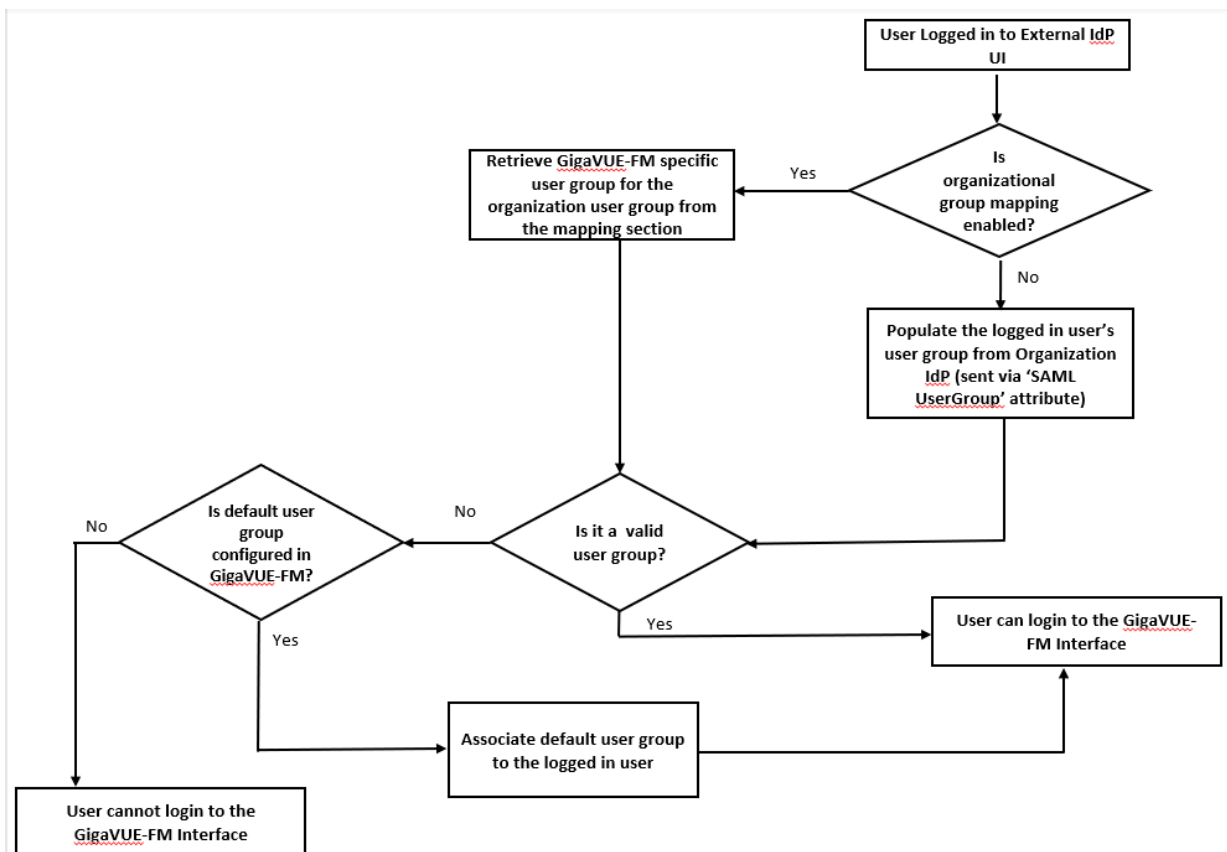
1. GigaVUE-FM sends a request to external organization IdP for authentication and authorization.

2. Authentication and authorization takes place at the external IdP. Once authentication succeeds, external IdP will send the logged in user along with the user's group:

- If user group is configured in external IdP and mapped appropriately to corresponding user groups in GigaVUE-FM:
 - If the user group is a valid group, then the user will be able to login to the GigaVUE-FM UI.
 - If the user group is not a valid user group, GigaVUE-FM determines if a default user group is configured:
 - If a default user group is configured, then the user can log in to the GigaVUE-FM user interface.
 - If a default user group is not configured, then the user cannot log in to the GigaVUE-FM user interface.

NOTE: If the external IdP is not configured with GigaVUE-FM specific user groups, then you must configure mapping between organization specific role/group and GigaVUE-FM specific user group by enabling **Organizational Group Mapping**, based on which the user will be allowed to log in to the GigaVUE-FM interface.

Refer to the following flow diagram for the detailed flow of process:



Refer to the **Authentication Type** for more details about the authentication types.

NOTE: GigaVUE-FM's time should synchronize with the External IDP Server's time for successful authentication. You must enable the NTP to synchronize the GigaVUE-FM's time with the External IDP Server's time.

Configure External IdP in GigaVUE-FM

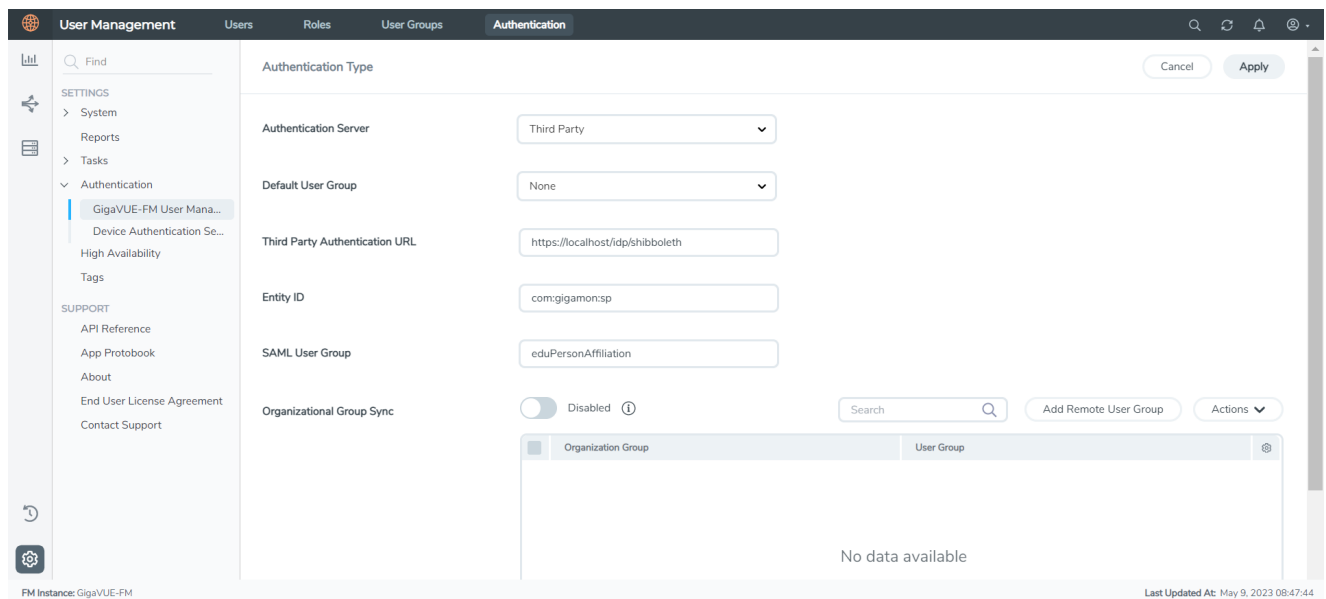
Prerequisites

You can use encryption and signing in IdP only when GigaVUE-FM uses an RSA-based certificate.

To configure external IdP (Active Directory Federation Services (ADFS)/Okta/Microsoft Azure) in GigaVUE-FM:

1. Select **Authentication > Authentication Types**.
2. Select **Authentication Server** as **Third Party**.
3. Enter the following details and click **Apply**.

Field	Description
Third Party Authentication URL	Third party authentication URL. <i>Example:</i> For ADFS: <a href="https://<<ADFS_HOSTNAME>>/FederationMetadata/2007-06/FederationMetadata.xml">https://<<ADFS_HOSTNAME>>/FederationMetadata/2007-06/FederationMetadata.xml
Entity ID	Entity ID of the service provider (GigaVUE-FM). Fetch the Service Provider metadata (which is GigaVUE-FM's metadata) from <a href="https://<FM IP Address>/saml/metadata">https://<FM IP Address>/saml/metadata .
SAML User Group	SAML User Group. This is used for authentication. The SAML User Group name entered here must match the SAML User Group configured in external IdP.
Default User Group	Default User Group
Organizational Group Sync	Map the GigaVUE-FM group to the corresponding organizational groups in ADFS/OKTA/Microsoft Azure.



You must add the IdP signing certificate into the GigaVUE-FM Trust Store (**Administration > System > Trust Store**).

NOTE: It is not required to enable Trust Store Node Certificate based authentication access.

You must restart GigaVUE-FM for the above configuration to be implemented.

Single Sign-on for GigaVUE-FM High Availability

Single Sign-on for GigaVUE-FM High Availability is available from software version 6.14.00 and allows connectivity of the GigaVUE-FM instances in a High Availability group. The following options are available:

- Internal IdP
- External IdP

With GigaVUE-FM HA SSO, if you login to the active GigaVUE-FM instance, the standby instances are also logged in automatically.



- To logout from the GigaVUE-FM High Availability group, you must first log out from the active GigaVUE-FM instance and then from the standby instances. If you attempt to logout from any of the standby instances, you will be redirected to the active GigaVUE-FM instance and the standby will not be logged out.
- If the active instance in a GigaVUE-FM HA group changes, you need not re-login to the GigaVUE-FM HA group.

Internal IdP

GigaVUE-FM HA uses shibboleth 2.0 identity provider for authentication and authorization. The active GigaVUE-FM instance of the High Availability group acts as the Identity provider. The two standby instances serve as the service providers.

Each of the GigaVUE-FM instances in the HA group has the following configurations:

- GigaVUE-FM application
- Shibboleth
- Authentication layer that account for the different authentication mechanisms

If you access a standby GigaVUE-FM instance, you will be redirected to the active GigaVUE-FM's IdP.

- If the active GigaVUE-FM is not authenticated, the login page of the active GigaVUE-FM instance is displayed.
- If the active GigaVUE-FM is authenticated, it will send the authentication response to the browser, and the standby instance will verify the same and will be authenticated.

NOTE: The required signing certificates and SSO certificates are already uploaded in the trust store of the GigaVUE-FM instance.

External IdP

ADFS and Okta are the external IdPs that have been qualified to be operational with GigaVUE-FM. To configure these external IdPs you must perform the following configuration:

1. Download ADFS/Okta server's custom certificate.
2. Upload that certificate in the trust store of the GigaVUE-FM master.

To use the external ADFS, you must perform the following configurations in the active GigaVUE-FM instance.

1. Go to **Authentication > Authentication Type**.
2. Select *Third Party* as **Authentication Type**.
3. Enter the SAML User Group and Default User Group configuration.

Authentication Type

Save

Cancel

Authentication Type Third Party

SAML User Group eduPersonAffiliation

Default User Group User Group

Organizational Group Mapping

New

Delete

Organizational Group Mapping ☒ Enable

☐	Organization Group	User Group
☐	LongevityAdmin	Super Admin Group
☐	Engineering	User Group

<< < Go to page: 1 of 1 > >> Total Records: 2

4. Enter the following details in the HA page for all three GigaVUE-FM instances:

- Entity Id - Each GigaVUE-FM should have a unique entity ID.
- Third Party Authentication URL

High Availability

Healthy
This HA group is Healthy. The members are protected from failure.

No supporting nodes in cluster

Group Name: HA-ESXi-Scale-6TB
No of Nodes: 3

Status	IP Address...	Role	External IP...	Entity ID	Host Name	Application Stat...	Software Version	System Uptime	Third Party...
Standby		Active Eligible			fmha1	Up	6.9.00	1 week, 1 day, 8 ...	https://login.mic...
Active		Active Eligible			fmha2	Up	6.9.00	1 week, 1 day, 8 ...	https://login.mic...
Standby		Active Eligible			fmha3	Up	6.9.00	1 week, 1 day, 8 ...	https://login.mic...

Go to Page: 1 of 1 Total: 3

Note: Please click [Refresh](#) to obtain the latest data.

FM Instance: GigaVUE-FM - 6.9.00

Roles and Users

This chapter provides basic information about role-based access and the procedures to manage roles and users in GigaVUE-FM along with assigning access permissions. The following topics are covered:

- [About Role-Based Access](#)

- [Configure Role-Based Access and Set Permissions](#)

About Role-Based Access

Role Based Access Control (RBAC) controls the access privileges of users and restricts users from either viewing or modifying unauthorized data which could be:

- Data in managed devices
- Data in GigaVUE-FM

Access Privileges in GigaVUE-FM

Access privileges in GigaVUE-FM is controlled by the following:

User role: A user role defines permission for users to perform any task or operation in GigaVUE-FM or on the managed device. Refer to the [Create Roles](#) section for more details on defining user roles.

Access control tags: Access control tags control the way the users access the resources such as clusters, ports, port groups, GigaSMART groups, GigaStreams, port pair and map. Refer to the [Tags](#) section for more information.

User group: A user group consists of a set of roles and set of tags associated with users in that group. When a user is created they can be associated with one or more groups. Refer to the [Create User Groups](#) section for more details on defining user group.

Important Notes on GigaVUE-FM RBAC

A GigaVUE-FM user must have the required privileges to modify the configurations in GigaVUE-FM. For the tasks that are to be performed on a node added to GigaVUE-FM, GigaVUE-FM uses the node credentials that is provided while adding a node to GigaVUE-FM.

It is recommended that the node credentials (username/password) used to add a node in GigaVUE-FM is configured in the node and has the necessary privileges. That is, the node credentials must match the credentials of an admin user on the managed nodes, so that when GigaVUE-FM performs any task or operation on the managed nodes, they all succeed with no errors. If you add a node with read-only privileges, it will impact the device operations performed from GigaVUE-FM.

Refer to Add New Physical Node or Cluster to GigaVUE-FM in the Fabric Management Guide in the Fabric Management Guide for details on how to add a node to GigaVUE-FM.

Configure Role-Based Access and Set Permissions

Configuring RBAC in GigaVUE-FM consists of the following tasks:

- [Add Users](#)

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

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 GigaVUE-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. Go to **Settings** and select **Authentication > GigaVUE-FM User Management > Users**. The **User** page is displayed.

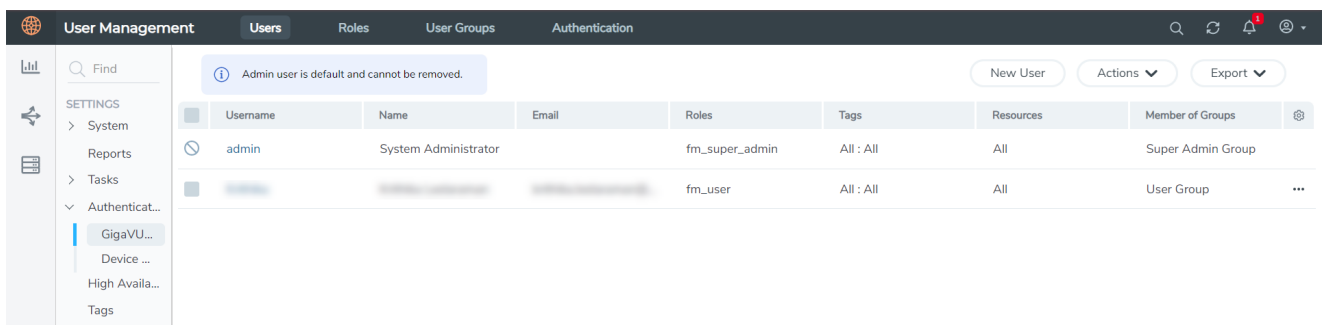


Figure 10 FM Users Page

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 -!@#\$%^&*()+

Figure 11 *Create User*

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

- **Assign User Group:** Assign user group to users.
- **Edit:** Edit the user details.
- **Delete:** When you delete a user, all sessions associated with them will be logged out.
- **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 GigaVUE-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.

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 GigaVUE-FM 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 GigaVUE-FM 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 GigaVUE-FM 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
All	Manages all resources • A user with fm_super_admin role has both read and write access to all the resource categories. • A user with fm_user role has only read access to all the resource categories.
Infrastructure Management	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: • Physical resources: Chassis, slots, cards ports, port groups, port pairs, cluster config, nodes and so on • GigaVUE-FM inventory resources: Nodes, node credentials • Device backup/restore: Device and cluster configuration • Device license configuration: Device/cluster licensing • Statistics: Device, port • Tags: Events, historical trending • Device security: SystemTime, System EventNotification, SystemLocalUser, System Security Policy Settings, AAA Authentication Settings, Device User Roles, LDAP Servers, RADIUS Servers, TACACS+ Servers • Device maintenance: Sys Dump, Syslog • Cloud Infrastructure resources: Cloud Connections, Cloud Proxy Server, Cloud Fabric Deployment, Cloud Configurations, Sys Dump, Syslog, Cloud licenses, Cloud Inventory. Note: Cloud APIs are also RBAC enabled.
Traffic Control Management	Manages inline resources, flow maps, GigaSMART applications, second level maps, map chains, map groups. The following resources belong to this category: • Infrastructure resources: IP interfaces, circuit tunnels, tunnel endpoints, tunnel load balancing endpoints, ARP entries • Intent Based Orchestration resources: Policies, rules • GigaSMART resources: GigaSMART, GSgroups, vPorts, NetFlow exporters • Map resources: Fabric, fabric resources, flow maps, maps, map

Category	Associated Resources
	chains, map groups, map templates • Application intelligence resources: Application visibility, Metadata, application filter resources • Tag: Flow manipulation - NetFlow operations, Statistics - device port • Active visibility • Inline resources: Inline networks, Inline network groups, Inline tools, Inline tool groups, Inline serial tools, Inline heartbeat profile • Cloud operation resources: Monitoring session, stats, map library, tunnel library, tools library, inclusion/exclusion maps. NOTE: Cloud APIs are also RBAC enabled.
FM Security Management	Ensures secure GigaVUE-FM environment. Users in this category can manage user and roles, AAA services and other security operations.
System Management	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: • Backup/restore • Archive server • License • Storage management • Image repo config • Notification target/email
Forward list/CUPS Management	Manages the forward list configuration. The following resources belong to this category: • GTP forward list • SIP forward list
Third Party Orchestration	Used to deploy fabric components using external orchestrator.
Device Certificate Management	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 GigaVUE-FM Security Management category.

To create a role

1. Go to **Settings** and select **Authentication > GigaVUE-FM User Management > Roles**.
2. Click **New Role**.

The screenshot displays the 'New Role' configuration interface. On the left, a sidebar contains navigation options under 'SETTINGS' (System, Reports, Tasks, Authentication, GigaVUE-FM User Management, Device Authentication Se..., High Availability, Tags) and 'SUPPORT' (API Reference, App Protobook, About, End User License Agreement, Contact Support). The main area is titled 'New Role' and includes a note: 'All form elements are mandatory unless indicated as optional.' Below this, there are input fields for 'Role Name' and 'Description'. A 'Select Permission' section contains a table with the following data:

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...

Buttons for 'Cancel' and 'Apply' are located at the top right of the form area.

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

NOTE: GigaVUE-FM does not allow you to import Users, User Groups and Roles. You can only export the configurations.

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.

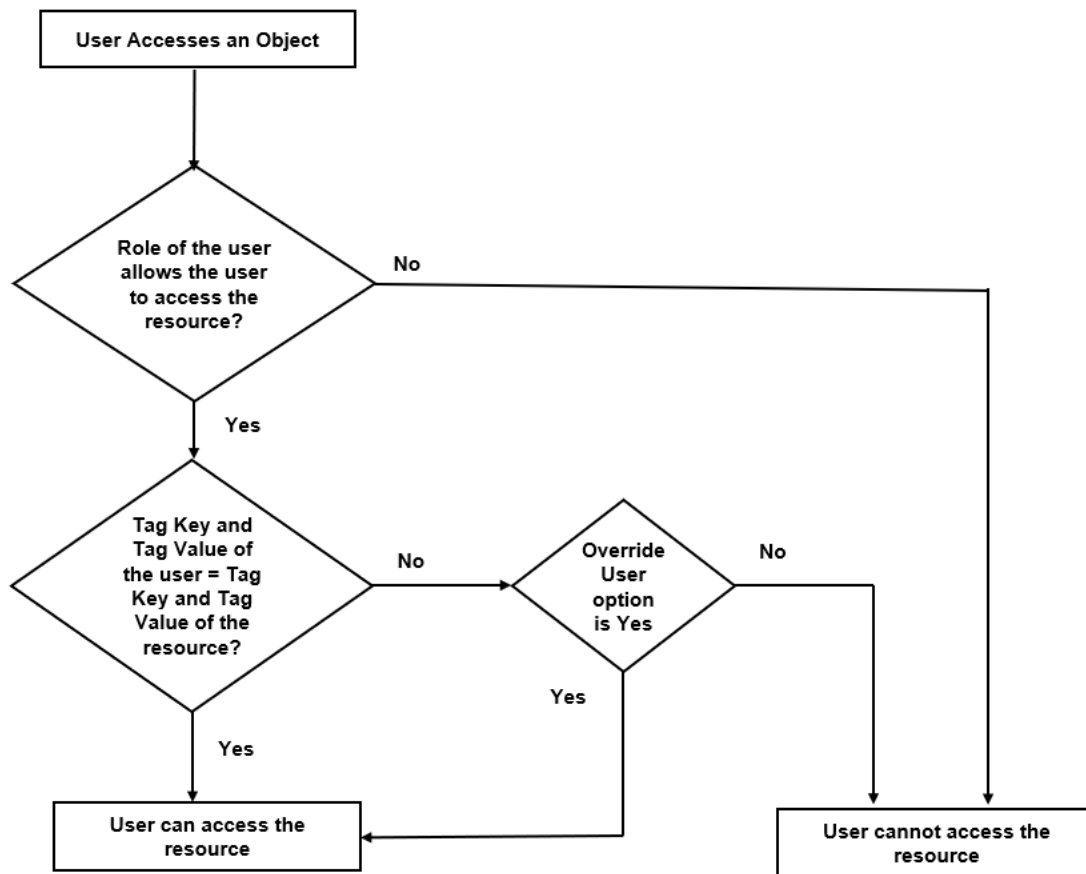
The following user groups are available by default in GigaVUE-FM. You will not be able to edit or change these groups in the system.

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:

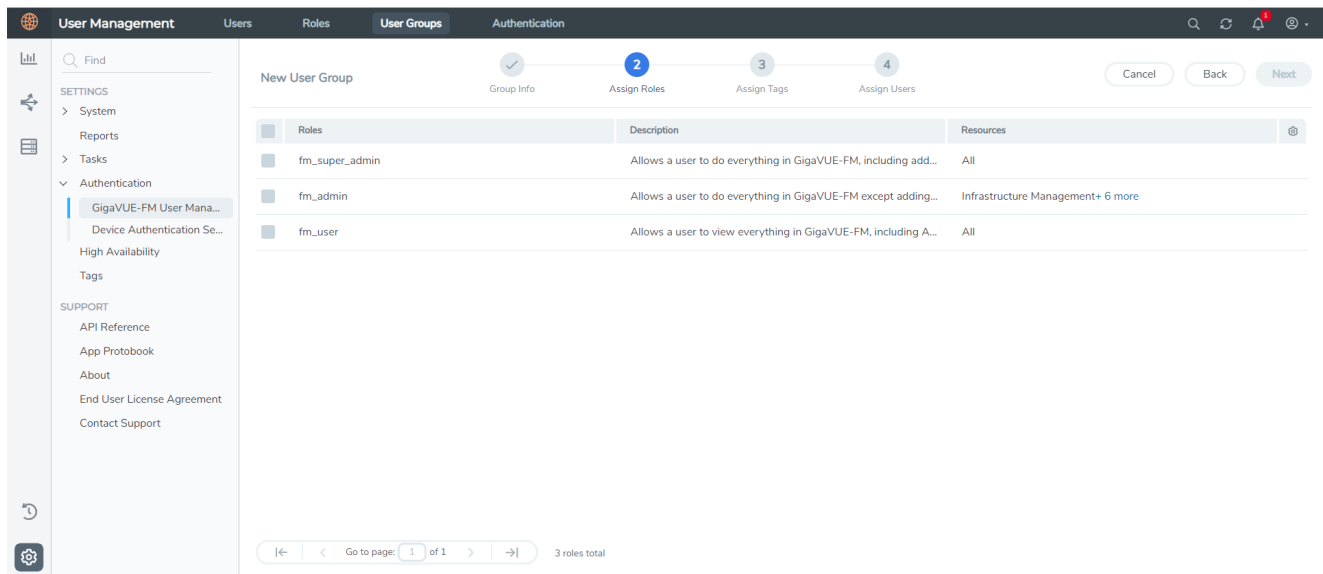
- The category of resources which the user can access, such as the clusters, ports, maps and so on. This is defined using the **Roles** option. Refer to the Roles section for more details.
- The physical and logical resources that the user can access, such as the ports in a cluster that belong to a specific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



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.

View Information About GigaVUE-FM

The About page provides product and version information of GigaVUE-FM that you can use when contacting customer support.

To view the About page for GigaVUE-FM (refer to the following figure), click on the button in the upper right-hand corner of GigaVUE-FM, where your name is displayed. Select **About**.

The following information is displayed:

- Product Name—The name of the product, GigaVUE-FM.
- Version—The current version running. For example, 6.1.00.
- Host ID—Host ID of GigaVUE-FM

- Host Name—Host name
- MAC Address—MAC address of GigaVUE-FM
- IP Address—IP Address
- Netmask—Netmask
- Gateway—Gateway
- IPv6 Address—IPv6 Address
- IPv6 Mask
- IPv6 Gateway
- DNS Server
- NTP Server
- FM Start-up Time
- FM Uptime
- Build ID and Build Date—information about when the current build was created—
- Boot Image
- SHA1-Thumbprint
- SHA-256 Thumbprint

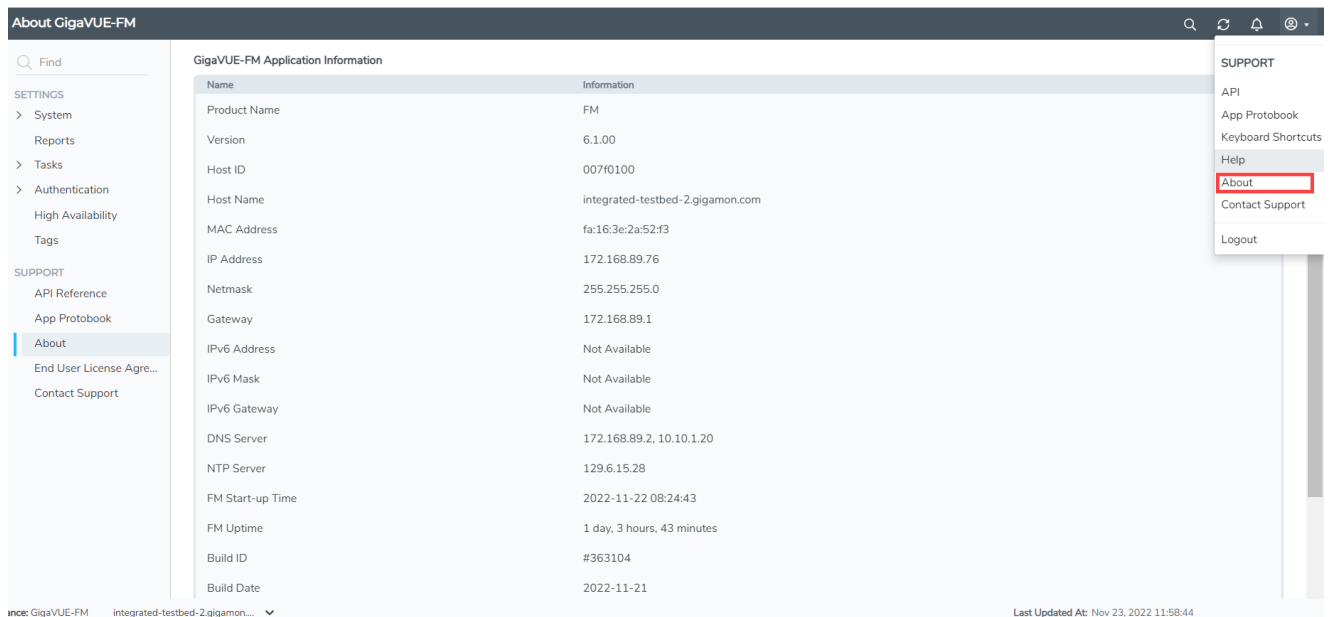


Figure 12 About Page

Tags

This chapter describes how to use tags to group clusters, ports, port groups, GigaSMART groups, GigaStreams, port pairs and maps.

This section covers the following main topics:

- [Introduction to Tags](#)
- [Work with Tags](#)
- [Create User-defined Tag](#)
- [Edit Tags](#)
- [Filter Tags](#)

Introduction to Tags

Managing a large number of clusters and nodes in GigaVUE-FM can be a daunting challenge. Using tags, GigaVUE-FM lets you group similar types of clusters and objects such as ports, port groups, GigaSMART groups, GigaStreams, port pairs and maps. User-defined tags can be associated to clusters as well as other objects.

NOTE: Starting in software version 5.8.01, the number of tag Ids per object is not limited to any hard-coded number nor is the number of tag values per tag ID. However, the following numbers have been qualified: A maximum of 20 tag Ids per object and a maximum of 20 tag values per tag Id.

To create tag, you must be a user with **fm_super_admin** or a user with write access to the GigaVUE-FM Security Management category. You can create the following types of tags:

- Access Control Tags
- Aggregation Tags

Based on the number of values they take, tags can be of the following types:

- **Single valued:** If a tag id is single-valued, then the resource can be assigned only a single tag value.
- **Multi valued:** If a tag id is multi-valued, then the resources can be assigned multiple tag values.

RBAC Tags (Access Control Tags)

Starting in software version 5.8.00, you can use tags for access control operations by associating tags to user groups. Access control tags control the way the users access the resources such as clusters, ports, port groups, GigaSMART groups, GigaStreams, port pair and map. You can use the tags for access control operations in the following ways:

- To associate the resources in the system to tag keys and their associated values.
- To associate the user groups in the system to tag keys and their associated values.

Thus, the tags for access control are associated to the resources as well as to the user groups. The users will be able to access the resources only if the tag value, by virtue of the user group they belong to, matches the tag value of the resources. Tag keys and the corresponding tag values are created in advance in the system. The tag keys are also associated to the tag values in advance.

When a user with a specific tag key and tag value creates a map, the tag key and tag value of the user is associated with the map that is created.

You can define the tag key and tag value depending on what the user is required to perform. Refer to the following examples:

User	User Group	Role	Tag Key and Tag Value	Accessibility
User 1	Super admin group	fm_super_admin [Read/write access to all resources]	Tag Key = All Tag Value = All	The user can: • add, edit, delete, view all resources • can add or modify users, and configure all AAA settings • associate any tag value to any of the resources.
User 2	Admin group	fm_admin [Read access to GigaVUE-FM Security Management Category] [Read/Write access to all other categories]	Tag Key = All Tag Value = All	The user can: • add, edit, delete, view all resources • cannot add or modify users and cannot configure the AAA settings • can change his own password • associate any tag value to any of the resources.

User	User Group	Role	Tag Key and Tag Value	Accessibility
User 3	View only user group	fm_user [Read access to all resources]	Tag Key = All Tag Value = All	The user - can only view all the resources. The role does not allow the user to add, edit or delete resources - cannot associate tag keys to the resources
User 4	Custom user group	Custom role [Read/Write access to resources that belong to Physical Device Infrastructure Management]	Tag Key = Specific tag keys based on the resources to be controlled by the admin user (example location) Tag Value = All	The user can: - manage the resources for which the user has permission depending on their role - can tag/untag ports and other resources for which the user has permission, depending on the role
User 5	Custom user group	Custom role [Read access to resources that belong to Physical Device Infrastructure Management Read/write access to resources that belong to Traffic Control Management Resources]	Tag Key = Specific tag keys based on the resources to be controlled by the admin user (example location) Tag Value = Specific location, e.g. Dubai	The user can: - use the resources that belong to the location Dubai - create a map using the port that has location=Dubai (tag key and value). The map that gets created will have the same tag location=Dubai automatically. - cannot tag/untag ports and other resources for which the user has permission, depending on the role

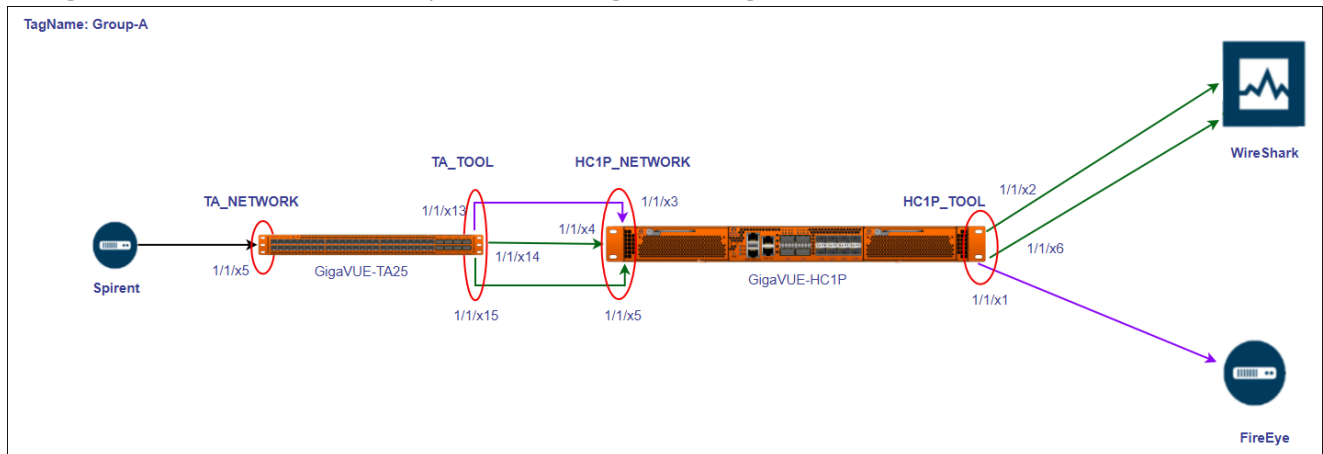
User Association with Roles and Tags

Refer to the [Create User Groups](#) section for more details about roles and tags.

Aggregation Tags

Aggregation tags are used to aggregate the resources for the purpose of collecting and analyzing statistics. For example, using aggregation tags, you can easily view and compare the aggregated traffic flowing through a list of ports. To analyze the aggregated

traffic flowing through the ports highlighted in red in the following figure, you can create a tag ID with the name Group-A and assign the tag values as shown in the table.



Ports	Tag Value
1/1/x5	TA_Network
1/1/x13, 1/1/x14, 1/1/x15	TA_TOOL
1/1/x3, 1/1/x4, 1/1/x5	HC1P_NETWORK
1/1/x2, 1/1/x6, 1/1/x1	HC1P_TOOL

In the physical dashboard, you can create the following widgets to quickly compare the aggregated traffic flowing through the ports associated with TA_NETWORK with the traffic flowing through the ports associated with HC1P_NETWORK:

- Highest Traffic
- Lowest Traffic
- Most Utilized Traffic
- Least Utilized Traffic

Consider another example. The tag ID 'Service' has the following tag values: IMS, GW, 5G. Perform the following tagging operations.

- Tag a set of network ports with service = IMS
- Tag a set of network ports with service = GW, 5G
- Tag a set of tool ports with service = IMS
- Tag a set of tool ports with service = GW, 5G

You can use the aggregation tags and derive the following statistics:

- Get the rate of traffic for all network IMS ports in the system (i.e. the total rate for the last one hour of all ingress IMS traffic)
- Get the rate of traffic for all tool ports with service = GW or 5G or if you have tagged a

set of maps with service = 5G

- Get the total rate of all maps with service = 5G for the past one hour

Rules and Notes

Refer to the following rules and notes for the access control and aggregation tags:

- All GigaVUE-FM users, irrespective of the role and user group they are associated to, can view and access all the resources tagged using aggregation tags. However, to add aggregation tags, the user must have access to the specific resources for which the required aggregation tag ID can be added along with the possible tag values that this tagId can take.
- If you assign a tag ID to a port group, port pair, GigaStream, GigaSMART Group, then the tag ID is associated to all the individual ports in the port group, port pair, GigaStream, GigaSMART Group. This is applicable only for the above mentioned groups and not applicable for maps. If you delete the tag ID or the tag values, or remove the collection, then the tag ID and values of the objects are also updated accordingly.
- You cannot associate aggregation tags to user groups.
- You can use access control tags as aggregation tags for deriving statistics.
- GigaVUE-FM allows you to create tags with prefix "_" (underscore character), however you cannot create tags with prefix "__" (double underscore).
- **Internal Tags:** GigaVUE-FM uses internal tags for aggregation purposes. For example, internal tags are used in fabric maps for statistical purposes. When you create a fabric map, GigaVUE-FM creates the following internal tag key and the tag value is the alias of the Fabric Maps *_fabricMapAlias*. You cannot delete internal tags created with prefix "_".
- Neighbor ports information retrieved from the Ports Discovery page may also include ports that are not permitted for your role. However, you can only view basic information (such as Port ID, Port Type, Alias) of the unpermitted ports and cannot perform any operation on these ports.

Tag Hierarchy

Both access control tags and aggregation tags follow a tag hierarchy. That is, if a tag id is associated with a top-level entity, then all the entities at the lower level will inherit the tag ID:

- Tag Ids assigned to the clusters will be inherited by the devices and port that belong to the cluster.
- Tag ids assigned to the devices will be inherited by the port.

Tag ids are not inherited by other lower level objects such as maps, map rules, gsgroups. The tag id inheritance is applicable only for physical objects such as the follows:

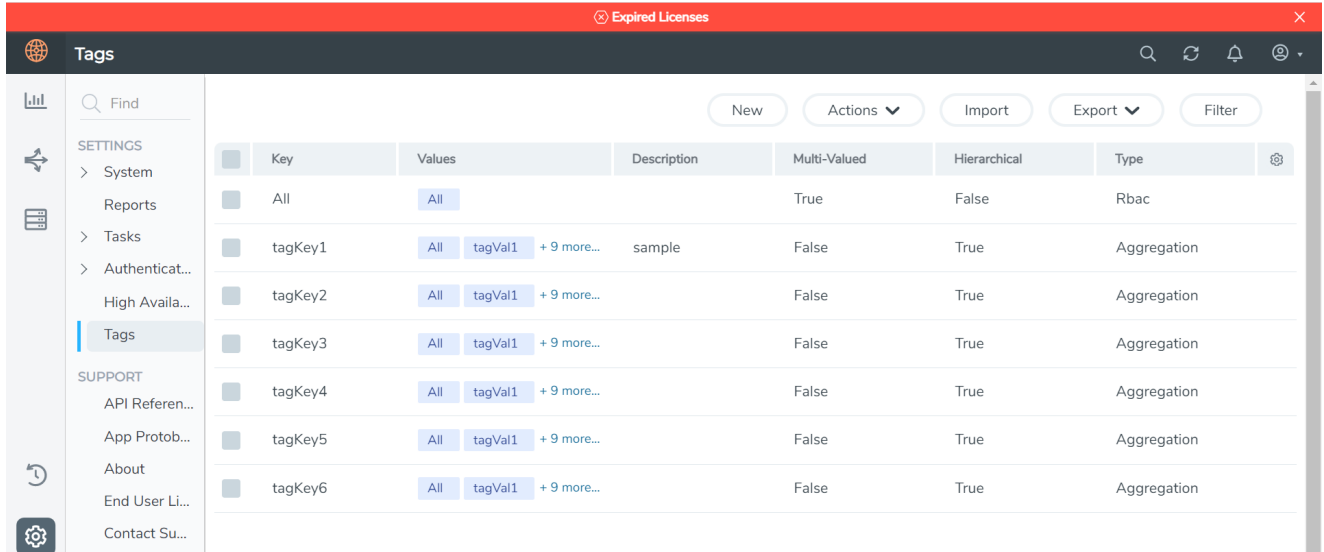
- Cluster
 - Device
 - Port

Notes:

- If a tag ID is multi valued, then the resources at the lower level will have values configured at the higher level and the values configured at its level.
- Tag IDs as well as the Tag Values can be set to the value ALL, depending on the role of the user:
 - The tagID for a user can be set to ALL, which indicates that this user will be associated with all the tagIDs and the associated tag values in the system. For an Admin Super User, the tag ID is associated to ALL, which indicates access to all the resources in the system.
 - The tag value for a user can be set to ALL. For an Admin User, for specific tag IDs, the tag value is set to ALL. For example, if a customer is using department as a way to associate the ports to different groups, then the administrator who decides which ports get used by which department(s), would have the tagId as 'dept' and the associated values as 'ALL'.

Work with Tags

Go to **Settings**, to view the tags and select **Tags**. The existing tags are displayed in the Tags page.



Key	Values	Description	Multi-Valued	Hierarchical	Type
All	All		True	False	Rbac
tagKey1	All tagVal1 + 9 more...	sample	False	True	Aggregation
tagKey2	All tagVal1 + 9 more...		False	True	Aggregation
tagKey3	All tagVal1 + 9 more...		False	True	Aggregation
tagKey4	All tagVal1 + 9 more...		False	True	Aggregation
tagKey5	All tagVal1 + 9 more...		False	True	Aggregation
tagKey6	All tagVal1 + 9 more...		False	True	Aggregation

Figure 13 Tags Home Page

The following columns are displayed in the tags list view:

Field	Description
Key	Tag key.
Values	The values of the tag.
Description	Description for the tag.
Multivalued	Indicates if the tag is single valued or multi-valued. By default, the tag is multi-valued.
Hierarchical	Indicates if tag hierarchy is set to true or not.
Type	Indicates the type of tag: • RBAC • Aggregation

The following buttons are displayed in the Tags page.

Field	Description
New	Creates a new tag. For more information, refer to Create User-defined Tag .
Actions	Use the Actions drop-down option to perform the following: • Edit Tags: Use to edit the tags. • Delete: Use to delete the tags. • Export Tag Resources: Use to download the tags in CSV File format. Refer to Bulk Upload Tags section for more details. • Last Tagging Activity: Use to view the pop-up again for the last activity performed.
Import	Use to import tags.
Export	Use to export tags.
Filter	Filters the tags available in the Tags page. For more information, refer to Filter Tags .

Create User-defined Tag

A user with **fm_super_admin** role or a user with read/write access to the GigaVUE-FM security Management category can create a user-defined tag.

NOTE: All other users can only view the tags depending on the role of the user and can associate resources only to those tags.

To create a tag:

1. Go to **Settings** and select **Tags**.
2. In the Tags page, click **New**.

The screenshot shows the 'New Tag' configuration interface in GigaVUE-FM. The left sidebar contains navigation options like SETTINGS, Reports, Tasks, Authentication, High Availability, Tags, and SUPPORT. The main area is titled 'New Tag' and includes the following fields:

- Name:** Region
- Description (optional):** Region tag
- Multi Valued:** Disabled (toggle)
- Tag Type:** Aggregation (dropdown)
- Hierarchy:** Enabled (toggle)
- Tag Values:** North (dropdown with 'X' icon and text 'Enter Tags separated by comma')

Two informational callouts are displayed on the right:

- Multi-valued:** Multi-valued is turned off: for this tag key, only a single value can be assigned to an asset at a time.
- Hierarchy:** Hierarchy is turned on: for any node or cluster that is tagged, its port and slot will automatically receive RBAC permissions.

Buttons for 'Cancel' and 'Apply' are at the top right. The footer shows 'FM Instance: GigaVUE-FM' and 'Last Updated At: May 8, 2023 15:41:22'.

3. Enter or select the appropriate details:

Field	Description
Name	Name of the tag
Description	Brief description for the tag
Multi Valued	Indicate if the tag is multivalued. This is the default value.
Tag Type	Type of tag. Values include: - Aggregation - RBAC (Access control)
Hierarchy	If enabled, the tag id that is associated with the top level object will be inherited by the objects at the lower level. Refer to the "Tag Hierarchy" section for more details. NOTE: Hierarchy is always set to true for Aggregation tags.
Tag Values	Values for the tag. Type the tag values and click Enter .

4. Click **Apply**. The new tag is added to the list view.

Add Tags To Resources

The following paragraphs describe how to add tags to resources such as clusters, ports, maps.

NOTE: Ensure that the tag keys and tag values are created prior to associating the resources to the tags.

To associate standalone devices or clusters to tags:

1. On the left navigation pane, go to **Inventory**  go to **Physical > Nodes**.
2. Select the device or devices for which you want to add the tag.
3. Click the **Tags** drop-down option in the top navigation bar and select **Add**.

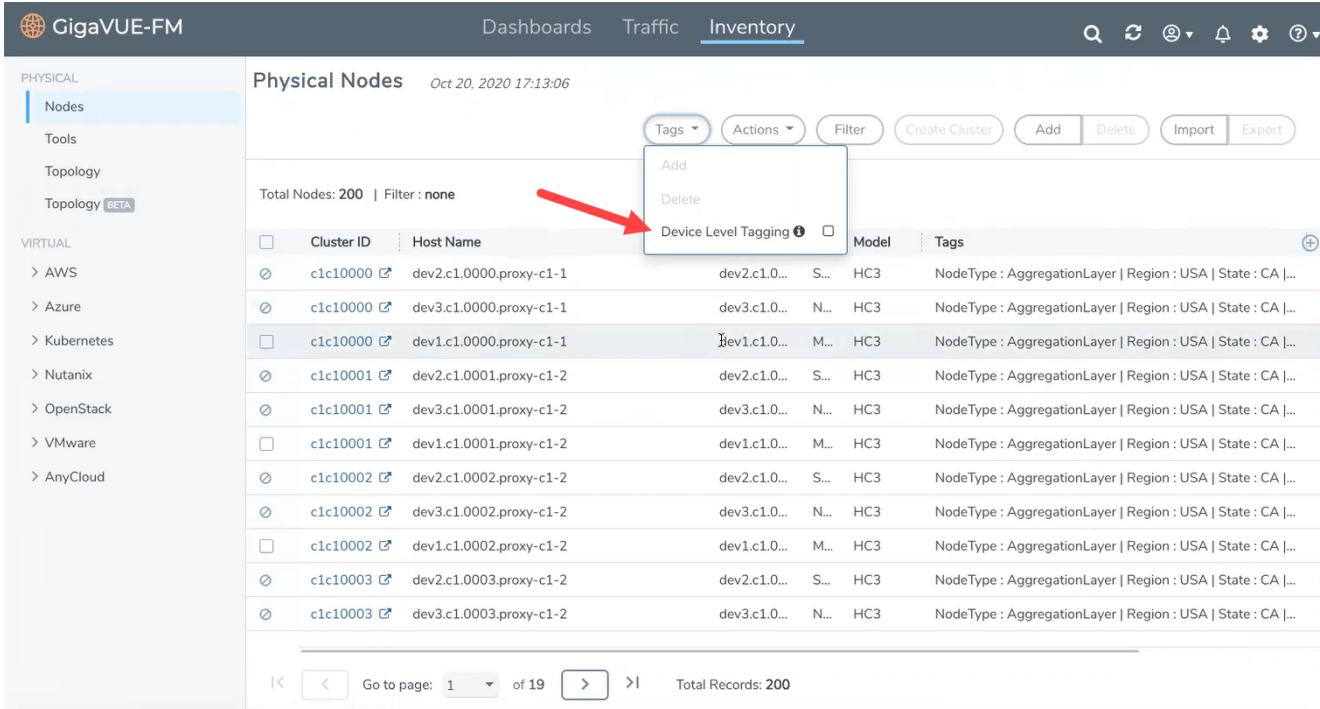
NOTE: The Tag Keys and the Tag Values that are displayed depend on the role of the user.

4. Select the required **Tag Key** and **Tag Value** option in the top navigation bar and click **OK**.

Node Level Tagging

Starting in software version 5.11.00, each of the individual nodes in a cluster can be associated with a tag key and a tag value. To assign a tag key to a node:

1. On the left navigation pane, go to **Inventory**  go to **Physical > Nodes**.
2. Click on **Tags** and select **Device Level Tagging**.
3. Select the required node/nodes and click **Add**. The **Add Tags to Resources** page appears.
4. Select the required tag key and the tag value to which the nodes must be tagged.
5. Click **OK**.



The screenshot shows the GigaVUE-FM interface. The left sidebar has 'PHYSICAL' selected, with 'Nodes' highlighted. The main area is titled 'Physical Nodes' with a timestamp 'Oct 20, 2020 17:13:06'. Above the table are buttons for 'Tags', 'Actions', 'Filter', 'Create Cluster', 'Add', 'Delete', 'Import', and 'Export'. The 'Tags' dropdown menu is open, showing 'Add', 'Delete', and 'Device Level Tagging' (which is highlighted with a red arrow). Below the menu is a table with columns: Cluster ID, Host Name, Model, and Tags. The table lists 200 nodes, with the first three rows visible. The first row is 'c1c10000' with host 'dev2.c1.0000.proxy-c1-1'. The second row is 'c1c10000' with host 'dev3.c1.0000.proxy-c1-1'. The third row is 'c1c10000' with host 'dev1.c1.0000.proxy-c1-1'. The table has a pagination bar at the bottom showing 'Go to page: 1 of 19' and 'Total Records: 200'.

The nodes in a cluster are now associated to tags which can be used for creating the required topology.

Tagging Ports

To associate ports, port groups, GigaSMART groups, GigaStream, or port pairs or maps to the tags, you must navigate to the respective pages and associate the tags. For example to associate the ports to tag:

1. On the left navigation pane, go to **Inventory**  go to **Physical > Nodes**.
2. Select the required node.
3. From the selected node page, go to **Ports > All Ports**.

NOTE: You can view the list of ports for which you have access to.

4. Select the port for which you need to associate tags.
5. Click **Edit**.
6. Scroll down to the **Tags** option.
7. Select the required **Tag IDs** and **Tag Values** that must be associated to the port.
8. Click **OK**.

Ports : 1/1/q4 OK Cancel

Lock shared with Users Click to select

Assigned to Roles

Level 1 Click to select

Level 2 Click to select

Level 3 Click to select

Level 4 Click to select

▼ Tags

Tags

region east × west × ⊖

TagKey Values ⊕ ⊖

To tag multiple resources (bulk update) at a time:

1. Select the required ports.
2. Click the **Tags** drop-down option from the top menu and select **Add**.
3. Select the required **Tag IDs** and **Tag Values** that must be associated to the ports.
4. Click **OK**.

NOTE: New tag ids and tag values will be associated to the selected ports if the ports have already not been associated to the tag Id or tag values.

Remove Tags from Resources

You can remove the tags from the resources by navigating to the respective resource pages. For example, to remove the tags from the ports:

1. On the left navigation pane, go to **Inventory**  go to **Physical > Nodes**.
2. Select the node with the ports for which you want to remove the tags.
3. Go to **Ports > All Ports**.
4. Select the port for which you need to remove the tags.
5. Click **Edit**.
6. Scroll down to the **Tags** option.
7. Select the required **Tag IDs** and **Tag Values** that must be removed from the ports.
8. Click **OK**.

You can also select multiple ports and remove the tags using the **Tags > Delete** option. If you select all the tag values and click delete, the tag key and tag values will be removed from the resource.

NOTE: When you delete the tags from the resources, the resources are no longer associated to the tag keys and tag values. To delete the tag key and tag value from GigaVUE-FM, refer to the [Delete Tags](#) section.

Edit Tags

To edit an existing tag:

1. Go to **Settings** and select **Tags**.
2. In the Tags page, select a tag you want to edit and click **Actions > Edit**.
3. In the Edit Tag page, you can edit the following:
 - Description
 - Multi Valued
 - Tag Type
 - Hierarchy
 - Tag Values
4. Click **Apply** to save the changes.

NOTE: You cannot edit the name of the tag.

Filter Tags

To filter the tags:

1. Go to **Settings** and select **Tags**.
2. In the Tags page, click **Filter** to filter the tags. The Filter quick view is displayed.
3. From the **Keys** drop-down list, select the required tag keys.
4. Click **Clear** to clear the filter.

Delete Tags

You can delete tags only if you are a user with **fm_super_admin** role or a user with write access to the GigaVUE-FM Security Management Category.

Bulk Upload Tags

GigaVUE-FM allows you to, instantaneously:

- Bulk upload a large number of tag keys and tag values.
- Assign tags to the resources such as devices, ports, and maps.

Use the **Import** and **Export Tags as Resources** options under **Action** menu in the Tags page to upload/download a CSV file containing the required fields:

- **For bulk uploading tags:** CSV file must contain tag key, tag value, description and other associated details.
- **For Assigning tags to resources:** CSV file must contain the resource type, resource id, tag key, tag values.

The tag keys and tag values will be added, deleted or replaced in GigaVUE-FM based on the following criteria:

Action	Scenario	Update in GigaVUE-FM
Append	Tag key and tag values are not present in GigaVUE-FM, but are defined in the CSV file.	Tag key and tag values will get added.
	Tag key and tag value are not present in GigaVUE-FM, but the tag key is defined in the CSV file without tag values.	Tag key with tag value 'All' will get added.
	The tag key present in GigaVUE-FM matches with the tag key defined in the CSV file, however tag values defined in the CSV file are not present in GigaVUE-FM (either the complete set of tag values, or a subset of tag values).	Tag values will be merged.
	Tag keys and tag values present in GigaVUE-FM match exactly with the tag keys and tag values defined in the CSV file, however the CSV file indicates changes to the property of the tags (Multivalued, Type, Hierarchical)	The property of the tag keys and tag values will be updated as per the CSV file.
	Tag keys and tag values present in GigaVUE-FM matches exactly with the tag keys and tag values defined in the CSV file.	No updates.

Action	Scenario	Update in GigaVUE-FM
Delete	Tag key and tag values defined in the CSV file are not present in GigaVUE-FM.	No updates.
	Tag key and tag values defined in the CSV file match exactly with tag keys and tag values in GigaVUE-FM.	Tag key and tag values will be deleted.
	Tag key defined in the CSV file is also present in GigaVUE-FM, however the tag values defined in the CSV file are only a subset of what is present in GigaVUE-FM	Tag key is not deleted, but tag values defined in the CSV file are deleted.
Replace	Tag key and tag values are not present in GigaVUE-FM, but are defined in the CSV file.	Tag key and tag values will get added.
	Tag key and tag value are not present in GigaVUE-FM, but the tag key is defined in the CSV file without tag values.	Tag key with tag value 'All' will get added.
	Tag keys and tag values present in GigaVUE-FM matches exactly with the tag keys and tag values defined in the CSV file.	No updates.
	The tag key present in GigaVUE-FM matches with the tag key defined in the CSV file, however tag values defined in the CSV file are not present in GigaVUE-FM (either the complete set of tag values, or a subset of tag values).	Tag values will get replaced as per the CSV file.
	The tag key present in GigaVUE-FM matches with the tag key defined in the CSV file, however tag values are not defined in the CSV file	Tag key is updated and all tag values except 'All' will be deleted
	Tag keys and tag values present in GigaVUE-FM match exactly with the tag keys and tag values defined in the CSV file, however the CSV file indicates changes to the property of the tags (Multivalued, Type, Hierarchical)	The property of the tag keys and tag values will be updated as per the CSV file.

Import Tags

To import a CSV file that has tags or tag resources:

1. Go to **Settings** and select **Tags**.
2. Click **Actions > Import**.
3. In the Import Tags page that appears, you can perform the following actions:
 - **Append:** Appends a new set of tag keys, tag value to the existing list.
 - **Replace:** Replaces the existing tags keys and tag values.
 - **Delete:** Deletes the tag keys and tag values.

NOTE: Refer to table in the previous section to understand the conditions based on which the tags will be appended, deleted or replaced.

4. Click **Select** to browse and select the CSV file.

To import tags: The CSV file must contain the following fields:

- Key
- Values
- Description
- Multi Valued
- Type
- Hierarchical

See the following image:

Import Tags Submit Cancel

Drop a CSV here.
or

Import Action Select one... Select File ⓘ

Key	Values	Description	Multi Valued	Hierarchical	Type
Region			FALSE	TRUE	Aggregation
Dept	IT,Eng		TRUE	TRUE	Aggregation
Service	IMS,Gatewa...		TRUE	FALSE	Rbac
Location	Asia		FALSE	TRUE	Rbac
Nodetype	Master,sta...		FALSE	TRUE	Aggregation

To import tags for resources: The CSV file must contain the following fields:

- Resource Type
- Resource ID
- Key
- Values
- Propagated Values

Import Tag Resources Submit Cancel

Drop a CSV here.
or

Import Action Select one... Select File ⓘ

Resource Type	Resource Id	Key	Values
Port	10.115.38.159:2/1/x1	Region	East,North
Port	10.115.38.159:2/1/x2	Service	IMS
Port	10.115.38.159:2/1/x3	Region	West
Port	10.115.38.159:2/1/x4	Service	IMS
Port	10.115.38.159:2/1/x5	Service	
Port	10.115.38.159:2/1/x6	Service	
Port	10.115.38.159:2/1/x7		IMS
Port	10.115.38.159:2/1/x8		
Port	10.115.38.159:12/1/x1	Service	IMS
Port	10.115.38.40:2/1/x1	Service	IMS

- Click **Done**. A pop-up appears in the bottom right corner of the page with the status.
- Click on the link in the pop-up to navigate to the Audit Logs page.
The Audit Logs page displays the log entries for the added, deleted and replaced tags. There will not be any log entries if the tag keys/tag values were skipped from being updated in GigaVUE-FM.

NOTE: Use the **Last Tagging Activity** button to view the pop-up again for the last activity performed.

Export Tag Resources

GigaVUE-FM allows you to export the tag keys and tag values for resources to a CSV file format from the following pages:

- Tags page
- Physical Nodes Page
- Ports Page
- Maps Page

To export from Tags Page

- Go to **Settings** and select **Tags**.
- Click **Actions** > **Export Tag Resources** button.

The tags keys and tag values for all the resources (Devices, ports and maps) will be exported to the CSV file:

To export from Physical Nodes page

1. On the left navigation pane, go to **Inventory**  and select **Physical**.
2. Select the required device or devices for which you need to export the tags.
3. Click **Tags** and select **Export Tags for Selected** in the drop-down.

The tag keys and tag values associated to a device will be exported to the CSV file:

NOTE: Click **Tags** and select **Export Tag Resources for Selected** to export tag keys and tag values associated to a specific device and to the associated resources such as ports and maps.

To export the tags from the Ports or Maps page

From the Ports or Maps page, click **Tags** and select **Export All tags**. The tag keys and tag values associated to all the ports or maps will be exported to the CSV file.

NOTE: You need not select the individual ports or maps to export the tags.

Alarms

This chapter provides basic information about alarms and the procedure to manage alarms in GigaVUE-FM. The following topics are covered:

- [Overview of Alarms](#)
- [View Alarms](#)
- [View Alarms based on User RBAC Permissions](#)
- [Manage Alarms](#)
- [Manage Multiple Alarms](#)
- [Alarm Correlation](#)
- [Filter Alarms](#)
- [Alarms for Fabric Maps and Policies](#)
- [Alarms for Inline Network Resources](#)
- [Drill down to Alarm Source](#)
- [Events](#)

Overview of Alarms

An alarm in GigaVUE-FM is a condition that requires user attention. GigaVUE-FM triggers alarms based on the health status information of the devices, that is, GigaVUE-FM generates alarms based on the health status of the physical and logical components in the visibility fabric.

GigaVUE-FM generates alarms either as:

- **Active monitoring alarms:** Alarms are generated by actively monitoring the network resources and triggered based on threshold levels.

- **Passive monitoring alarms:** Alarms are generated after a problem has occurred based on the traps generated by the device.

Alarms are classified into the following types based on their status:

- **Acknowledged:** Indicates that the alarm has been viewed by the user and is aware of the alarm, irrespective of the action being taken.
- **Unacknowledged:** Indicates the alarm has not been viewed by the user and is pending action.
- **Suppressed:** Indicates the alarm that are suppressed or auto acknowledged by the user. To learn more about suppressing an alarm refer to Suppressed Alarms.

Based on the severity level, alarms are classified into the following types:

- **Critical:** Indicates service disruption or a total loss of service and needs immediate user attention.
- **Major:** Indicates major degradation to service and needs user attention at the earliest possible time.
- **Minor:** Indicates a minor service disruption which may result in major degradation and therefore needs attention.
- **Warning:** Indicates an information that may result in higher level issues if ignored over a period of time.
- **Information:** Indicates an information or a message that may not have major impact to service.

Suppressed Alarms

GigaVUE- FM allows you to suppress alarms that are raised during maintenance operation of a specific resource, cluster or node.

This section explains about the following:

- [Suppress Alarm](#)
- [Manage Suppression Rules](#)
- [View Suppressed Alarms](#)

Suppress Alarm

You can suppress an alarm or alarms for a specific period or indefinitely by:

- [Suppressing from Alarms page](#)
- [Suppressing from Physical Nodes page](#)

You can also configure auto-suppression of alarms for certain GigaVUE-FM triggered operations on device such as Configuration Restore, Device Reboot, Image Upgrade on a cluster or node and Cluster Creation Operations.

For more information, refer to [Auto-Suppression of Alarms](#)

Stop Suppression

Stop Suppression deactivates the corresponding suppression rule of the alarm. When you select Stop Suppression for a suppressed alarm, GigaVUE-FM displays an appropriate message indicating if the rule is deactivated or if the rule does not exist.

To stop suppression of alarm from the Alarms page, do the following on GigaVUE-FM:

1. On the left navigation pane, click on .
2. Go to **System > Alarms**.
3. Select an alarm and click the ellipsis.
4. Click **Stop Suppress**.

You can also suppress using the **Action** button. For more details, refer to [Buttons](#).



Stop suppression cannot be configured for the following:

- Alarms that are suppressed during implicit operations.
- Correlated alarms.

Suppressing from Alarms page

To suppress alarm from the Alarms page, do the following on GigaVUE-FM:

1. On the left navigation pane, click on .
2. Go to **System > Alarms**.
3. Select an alarm and click the ellipsis.
4. Click **Suppress**. The **Add Suppression Rule** page appears.

You can also suppress using the **Action** button. For more details, refer to [Buttons](#).

5. Enter the following details to suppress the alarm:
 - Reason – You can select from the available reasons in the drop-down list or click **New** to specify a new reason to suppress an alarm.
 - Rule Expiration – Enter the period after which the rule expires.
 - Activate Rule – Enable the button to activate the rule. The default is **On**.
6. Click **Suppress** to suppress the Alarm. A confirmation message appears.

You can view the rule created in the **Suppression Rules** page.

Refer to [Manage Suppression Rules](#) to learn on how to manage the suppression rules that are created.

Suppressing from Physical Nodes page

To suppress alarm from the Physical Nodes page, do the following on GigaVUE-FM:

1. On the left navigation pane, go to **Inventory**  and select **Physical**.
2. Select the cluster for which the alarms are to be suppressed.
3. Click **Actions** and select **Suppress** from the drop-down list. The **Add Suppression Rule** page appears.
4. Perform steps 5 and 6 described in the [Suppressing from Alarms page](#).

Auto-Suppression of Alarms

GigaVUE-FM allows auto-suppression of alarms for certain GigaVUE-FM triggered operations on device such as Configuration Restore, Device Reboot, Image, Upgrade or Cluster Creation Operations on a cluster or node.

When auto-suppression is activated, GigaVUE-FM automatically creates or deletes the suppression rule for the cluster or node for the GigaVUE-FM operations.

To auto-suppress alarms, do the following:

1. On the left navigation pane, click on .
2. Go to **System > Alarms**.
3. Click **Settings** on the top navigation bar.
4. In the **Exclusion and Suppression Rules** section, you can enable the check box for **Automatically Suppress Resources** and for the following operations, which require auto-suppression of alarms:
 - GigaVUE-FM Device Image Upgrade
 - GigaVUE-FM Device Configuration Restore
 - GigaVUE-FM Cluster Creation
 - GigaVUE-FM Device Reboot.
5. Click **Save** to save the settings.

Manage Suppression Rules

GigaVUE-FM allows you to activate, deactivate, view, edit or delete a suppression rule.

NOTE: All GigaVUE-FM users, irrespective of the role and user group they are associated to, can view the suppression rules. However, only users with read-write access to the Infrastructure Management resource category can manage the suppression rules.

To manage a suppression rule, do the following:

1. On the left navigation pane, click on .
2. Go to **System > Alarms**.
3. Click **Suppression Rules** on the top navigation bar. You can view the details of the suppression rules created for a cluster or a node.
4. Click **Actions** drop-down list. You can select and perform the required actions.

The following table explains the actions displayed in the drop-down list:

Action	Description
Edit Suppression Rule	Modify or Update the existing rule.
Activate	Activate the rule.
Deactivate	Deactivate the suppression rule.
Delete	Delete the rule.

Filter Suppression Rule

You can filter the suppression rules based on the suppressed alarm type and the reasons for suppressing it. For more information on filtering alarms, refer to [Filter Alarms](#)

Export Suppression Rule

GigaVUE-FM allows you to export the rules in suppression rules page in CSV and XLSX formats.

To export the suppression rules, do the following:

1. On the left navigation pane, click on .
2. Go to **System > Alarms**.
3. Click **Suppression Rules** on the top navigation bar. You can view the details of the suppression rules created for a cluster or a node.
4. Click **Export** drop-down list. You can view the following options:
 - Export All – Export all the available suppression rules in CSV or XLSX format.
 - Export Selected – Export only the selected suppression rules CSV or XLSX format.

View Suppressed Alarms

GigaVUE-FM allows you to view the alarms that are suppressed. To view the suppressed alarms:

1. On the left navigation pane, click on .

2. Go to **System > Alarms > All Alarms**.
3. Click the widget **Suppressed Alarms**. You can view the suppressed alarms created for a cluster or a node.

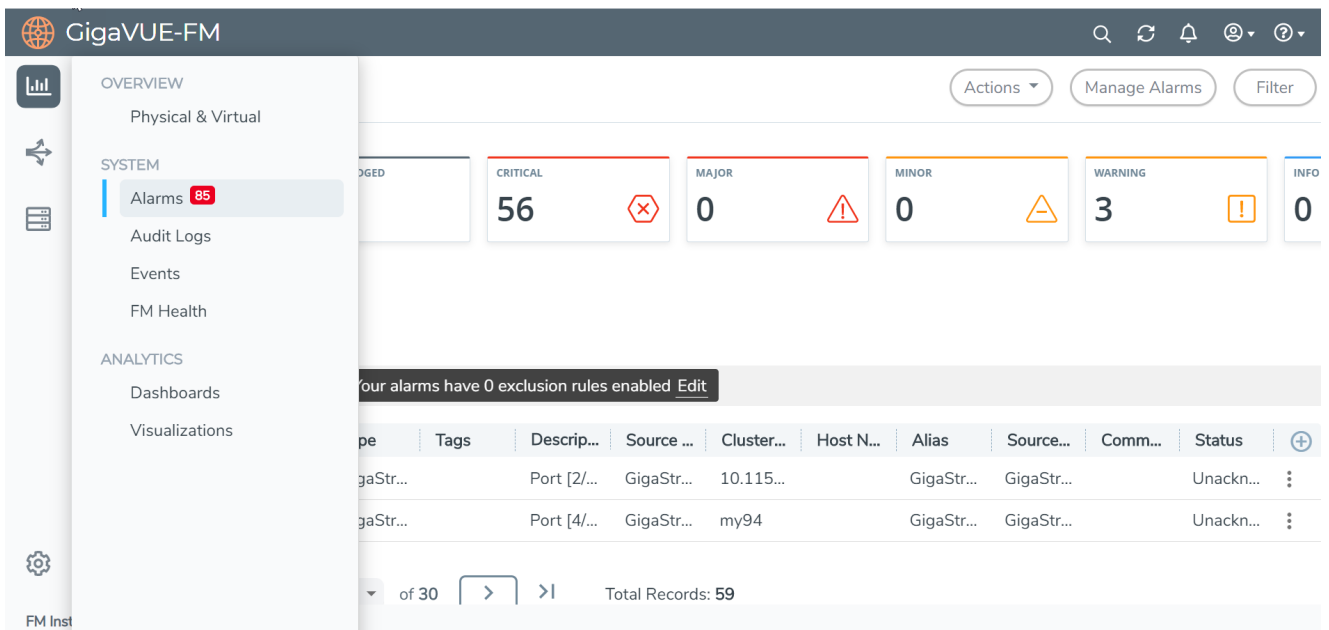
View Alarms

To view the alarms triggered in GigaVUE-FM:

1. On the left navigation pane, click on  and select Alarms. The Alarm page appears. Widgets for the following alarm categories appear on the top of the page.
 - Unacknowledged
 - Acknowledged
 - Suppressed
 - Auto Suppression Rules
 - Critical
 - Major
 - Minor
 - Warning
 - Info
 - Exclusion Rules Applied

NOTE: The widgets display the current system alarms that can be viewed by the logged in user. The data displayed on the widget is global data and will not change depending on the filter configured by the user. This is applicable for All Alarms and Correlated Alarms.

2. Click on the widgets to view the list of alarms belonging to that specific category.



The screenshot shows the GigaVUE-FM interface. The left navigation pane has 'SYSTEM' expanded, with 'Alarms' (85) selected. The main content area shows a summary of alarm counts by severity: CRITICAL (56), MAJOR (0), MINOR (0), WARNING (3), and INFO (0). Below this is a table of alarm details.

Type	Tags	Descrip...	Source ...	Cluster...	Host N...	Alias	Source...	Comm...	Status
GigaStr...		Port [2/...	GigaStr...	10.115...		GigaStr...	GigaStr...		Unackn...
GigaStr...		Port [4/...	GigaStr...	my94		GigaStr...	GigaStr...		Unackn...

At the bottom, it shows 'of 30' records and 'Total Records: 59'.

Figure 14 Alarms

The alarm list view appears below the widgets. The View By option in the page allows you to toggle between the following two views:

- **All Alarms:** Displays all active alarms in the system.
- **Correlated Alarms:** Displays correlated alarms or top-level alarms. Refer to [Alarm Correlation](#)

The following table describes the parameters displayed in the alarm list view:

Permission Level	Description
Time	The time when the alarm was last triggered.
Severity	The severity status of the alarm. This can be critical, major, minor, warning or info.
Type	The type of event that generated the alarm. For example, Faulty power module, Unhealthy map, and so on.
Description	The description of the alarm type in detail.
Source Type	The source type that triggered the alarm, e.g. port, power module, fan.
Source ID	The ID of the resource associated with the alarm. NOTE: You can hover your mouse on the source id to view the cluster-id, source name and alias name for the ports that have an alias.
Comment	Comment added/updated by the user for the alarm.
Status	The status of the alarm. Can be: ▪ Acknowledged. You can hover your mouse to view the details of the user who acknowledged the alarm and the last acknowledged time. ▪ Unacknowledged
Cluster ID	Cluster Id
Host Name	Host name
Alias	Alias name
Last Acknowledged By	User who acknowledged the alarm.
Acknowledged Time	Time the alarm was acknowledged.
Last unAcknowledged By	User who unacknowledged the alarm.
Unacknowledged Time	Time the alarm was unacknowledged.
Tags	Tags associated with the Alarms

3. Select an alarm and click the ellipsis to:

- **Acknowledge:** To acknowledge an alarm.

NOTE: This option is available only for unacknowledged alarms.

- **Suppress:** To suppress an alarm.
- **Add Comment:** To add a comment while acknowledging an alarm. While acknowledging multiple alarms, the comment added will be applied to all the alarms.
- **View Details:** To view the details of an alarm such as alarm type, severity, description and other details.
- **View History:** To view the list of historical alarms.
- **Delete:** To delete an alarm.

View Alarms based on User RBAC Permissions

GigaVUE-FM allows you to view the alarms in the Alarms page based on the following RBAC permissions:

- **User Roles:** User role defines permission for users to perform any task or operation in GigaVUE-FM or the devices. For example, if you are a user with read and write access to the 'FM Security Management' category, then you will be able to see all the alarms related to the resources that belong to the GigaVUE-FM Security Management category such as users, roles, AAA services. Alarms related to other categories will be restricted. That is, you cannot view alarms related to physical resources such as ports, port groups, port pairs, cloud connections, cloud config that belong to the 'Infrastructure Management' category.
- **User Defined Tags:** Tags control the way you access the resources such as clusters, ports, port groups, port pairs, GigaSMART groups, GigaStreams and maps. You can view the alarms associated to tagged resources that you are permitted to access. For example, consider the following port pairs in the system:
 - Port pair PP1 is configured with tagKey: Location, tagValues - Seattle
 - Port pair PP2 is configured with tagKey: Location, tagValues - San FranciscoIf you are configured with tagKey: Location and tagValue: San Francisco, then you will be able to access only port pair PP2 based on your permitted tag. Therefore, you will see only alarms related to port pair PP2.

NOTE: In case of resources that do not support tagging, you will be able to see alarms from resource that are permitted as per your role definitions and alarms from the devices that are permitted as per the tags.

Users belonging to Super Admin, Admin and User groups will be able to view all alarms as they have no restrictions on resources, permissions and tags.

Manage Alarms

To configure the following, navigate to Alarms > Settings page.

- Exclusion Rules
- Suppression Rules ([Manage Suppression Rules](#))
- Threshold Values for Memory and CPU Status

Exclusion Rules

GigaVUE-FM allows you to enable exclusion rules for the alarms using which you can choose to exclude health computation of the physical and logical components which do not require user attention, thereby preventing an alarm to be triggered.

NOTE: Use the toggle bar to toggle between enabling and disabling the selected option.

To do this:

1. Click the **Alarms** button on the left navigation bar.
2. Choose the exclude rules to apply while computing the health status of physical and logical components. The following options are available:
 - Ports that are admin disabled
 - Ports that do not have aliases
3. Click the required checkbox. A confirmation dialog appears. Select 'Yes, remove the alarms' to check the box and remove the alarms. Select Cancel to cancel the operation.
4. Click **Save** to save the settings.

Threshold Values for Memory and CPU Status

You can configure the threshold limits for the following:

- **Memory Status:** You can configure the device memory usage threshold limit as follows:
 - *Alert as critical if the memory threshold exceeds:* Upper threshold limit for triggering the alarm
 - *Clear the alarm if the memory threshold falls below:* Lower threshold limit for clearing the alarm
- **CPU Status:** You can configure the device CPU usage threshold limit as follows:
 - *Alert as critical if the CPU threshold exceeds:* Upper threshold limit for triggering the alarm
 - *Clear the alarm if the CPU threshold falls below:* Lower threshold limit for clearing the alarm

Manage Multiple Alarms

To acknowledge multiple alarms at a time:

1. Click **Alarms** on the left navigation bar.

2. Select the alarms that you want to acknowledge.
3. Click Acknowledge.

A confirmation dialog appears saying that you are acknowledging these alarms. Click acknowledge to proceed. If you add a comment, the comment will be added to all the alarms.

You can also unacknowledge and delete multiple alarms at a time.

Filter Alarms

You can search and narrow down the alarms you want to be displayed on the alarms list view page. To filter alarms:

1. Click the **Filter** button. The Filter quick view is displayed.
2. Select the required criteria for filtering the alarms:
 - Start Time
 - End Time
 - Severity
 - Type
 - Source Type
 - Status
 - Cluster ID
 - Host Name
 - Source ID
 - Alias
 - Tags
3. Click **Apply Filter** to apply the filter.
4. Click **Clear** to clear the filter.

The alarms list view displays the alarms based on the filter applied.

Alarm Correlation

GigaVUE-FM correlates alarms generated due to simultaneous network or resource faults to prevent flooding of alarms. Select the Correlated View option in the Alarms page to view the correlated alarms. Correlated alarms are the top-level alarms with all the other related alarms displayed underneath.

NOTE: To view the related alarms for a top-level alarm, click on the ellipsis and select **View Details**.

Consider the following example: Port 1/1/x1 is used as source port of a map that has an alias map1.

- Port 1/1/x1 becomes unhealthy (port is down or faces packet drops, errors or higher or lower utilization).
- Consequently, map1 is also unhealthy.
- Fixing the issue in port x1 will bring back map1 to healthy state.
- In this example, the Port Unhealthy alarm triggered for port 1/1/x1 is the top-level alarm. This will be displayed in the correlated view.
- Click View Details to view the related Map Unhealthy alarm for the map. However, Map Unhealthy alarm will be displayed as a separate entity in flat view.

Alarms for Fabric Maps and Policies

GigaVUE-FM generates alarms to track the changes in the health status of the fabric maps. That is, whenever the health status of a fabric map changes from healthy to unhealthy (or state changes within an unhealthy state), an alarm is triggered and the

same can be viewed in the Alarms page.

Starting in software version 5.11.00, GigaVUE-FM generates alarms to track the changes in the health status of the orchestrated policies. Consider the following example in which the user has created the following two policies:

NOTE: Whenever an intent policy is created, a number of Fabric Maps and internal cluster maps are created using circuit ports, stack ports and other type of ports.

Orchestrated Policies	Fabric Maps	Cluster Level Maps	Ports
Policy_1	Fabric_map_1	Map_1	Port_11 Port_12
		Map_2	Port_21 Port_22
	Fabric_map_2	Map_3	Port_31 Port_32
		Map_2	Port_21 Port_22
Policy 2	Fabric_map_4	Map_4	Port_41 Port_42
		Map_5	Port_51 Port_52

Refer to the following notes:

- If the health status of Port_21 (circuit port) turns red, then the following alarms are generated:
 - One port level alarm for the circuit port Port_21.
 - One cluster map level alarm for Map_2.
 - Two fabric map level alarms for Fabric_map_1 and Fabric_map_2.
 - One policy level alarm for Policy_1.

- If the health status of Port_51 (stack port) turns red, then the following alarms are generated:
 - One port level for the stack port Port_51
 - One cluster map level alarm for Map_5
 - One fabric map level alarms for Fabric_map_4
 - One policy level alarm for Policy_2

Events

GigaVUE-FM keeps track of all alarms that has occurred in the system. Whenever an alarm is created, updated or deleted, a corresponding event entry is added to the events table. The Events page lists all notifiable events that have occurred in the physical, virtual, and cloud environment. Refer to [Events](#) for details.

Drill down to Alarm Source

The Alarms page in GigaVUE-FM displays alarms triggered due to faults in the health status of the physical and logical components. Few of the alarms listed in the alarms page are configured with hyperlinks to the source that triggered the alarm thus providing a quick view of the alarm resource and the reason for failure.

The source-ID field of the following alarm types are configured as hyperlinks which when clicked opens the quick view of the resource or navigates to the respective resource pages.

Alarm	Hyper-linked to
Port Group Unhealthy	Port Group Quick View
Port Pair Unhealthy	Port Pair Quick View
Inline Network Unhealthy	Inline Network Quick View
Inline Tool Unhealthy	Inline Tool Quick View
Inline Tool Group Unhealthy	Inline Tool Group Quick View
IP Interface Unhealthy	IP Interface Quick View
IBO Policy	IBO Policy page
Fabric Maps	Fabric Maps page
Map related alarms	Map Quick View
Device level alarms	Device-specific pages

NOTE: Based on your user role, you can edit the resources and resolve the alarm. For example, if you are a user with read and write access to the 'Infrastructure Management' category, you will be able to edit the ports and device configuration accordingly.

Refer to the following example images:

- **Inline Tool Group Quick View:** Appears on clicking the source-id field on the Inline Tool Group Unhealthy alarm.

The screenshot shows the 'Alarms' tab in the GigaVUE-FM interface. A table of alarms is displayed, with the 'Source ID' column highlighted. The 'Inline Tool Group' source ID is selected, and a 'Quick View' panel is open on the right. The panel shows details for the 'Inline Tool Group: IN-Tool-Grp', including its alias, description, ports, and configuration.

Time	Severity	Source ID	Type	Description
2022-05-16 15:...	Major	IN-Tool-Grp	Inline Tool Group...	Component(s) IN-tool-1 po...
2022-05-16 15:...	Critical	IN-tool-1	Inline Tool Unhea...	Operational State is down...
2022-05-16 15:...	Critical	FmAuto-Collecto...	Map Unhealthy	Inline Network component...
2022-05-16 15:...	Critical	FmAuto-Map_16...	Map Unhealthy	Inline Network component...

The 'Quick View' panel for 'Inline Tool Group: IN-Tool-Grp' includes the following sections:

- Inline Tool Group Info:**
 - Alias: IN-Tool-Grp
 - Description: asdfghjklpoiuytrewqasdfghjklkasqasqasdfghwqasqasdfghjklkasdfghjklpoiuytrewqasdfghjklkasdfghjklpoiuytrewqasdfghjkl
- Ports:**
 - Inline Tool: IN-tool-1 (Critical), test-1 (OK)
 - Inline Spare Tool: test-112 (OK)
- Configuration:**
 - Enabled: ☐
 - Release Spare If Possible: ☒
 - Fallover Mode: spread
 - Fallover Action: toolBypass
 - Release Spare: true
 - Minimum Healthy Group Size: 1
 - Hash: advanced
 - Spare Tool Status: in use

- **Port Group Quick View:** Appears on clicking the source-id field on the Port Group Unhealthy alarm.

The screenshot shows the 'Alarms' tab in the GigaVUE-FM interface. A table of alarms is displayed, with the 'Source ID' column highlighted. The 'Port Group Unhealthy' source ID is selected, and a 'Quick View' panel is open on the right. The panel shows details for the 'Port Group: PG-1', including its alias, description, type, and port details.

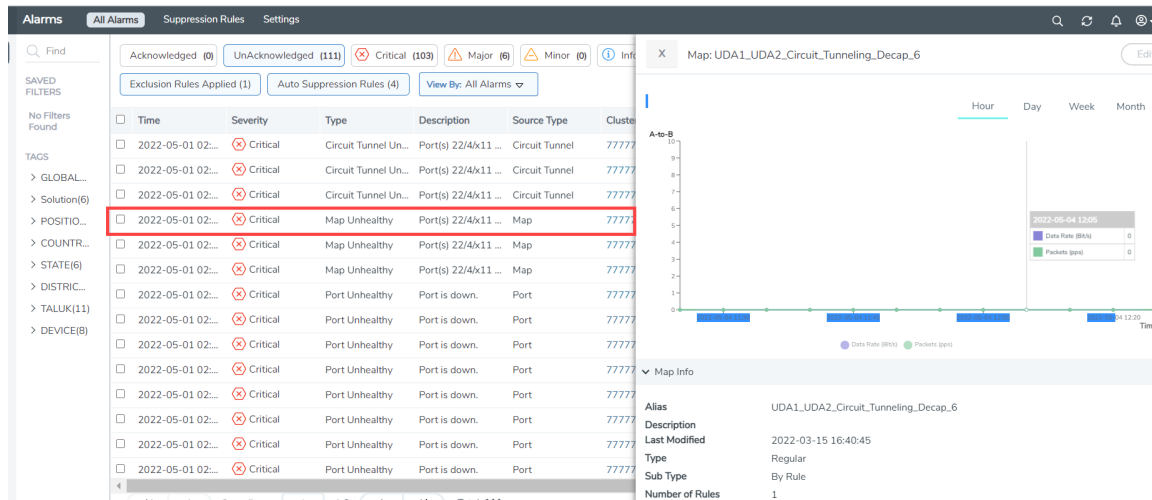
Time	Severity	Type	Description
2022-05-12 14:...	Critical	Inline Network Group U...	Component(s) IN-Net, IN-NET-2 ports...
2022-05-12 14:...	Critical	Inline Network Unhealthy	Port(s) 8/2/c7 are link down.
2022-05-12 14:...	Critical	Inline Network Unhealthy	Port(s) 8/4/c5, 8/4/c6 are link down.
2022-05-12 14:...	Critical	Inline Network Unhealthy	Port(s) 8/2/c2 (Err-Port-12345678987...
2022-05-12 14:...	Critical	Map Unhealthy	Inline Network component(s) in-test po...
2022-05-12 14:...	Critical	Map Unhealthy	Port(s) 8/2/c1 (port-admin-enabled-12...
2022-05-12 14:...	Critical	Map Unhealthy	Port(s) 8/2/c2 (Err-Port-12345678987...
2022-05-12 14:...	Critical	Map Unhealthy	Inline Network component(s) in-test po...
2022-05-12 14:...	Critical	Map Unhealthy	Port(s) 8/2/c5 (test123456789123456...
2022-05-12 14:...	Critical	Map Unhealthy	Port Group component(s) PG-1 ports a...
2022-05-12 14:...	Critical	Map Unhealthy	Port(s) 8/2/c4 are link down.
2022-05-12 14:...	Critical	IP Interface Unhealthy	Port(s) 8/2/c6 are link down.
2022-05-12 14:...	Critical	Port Group Unhealthy	Port(s) 8/2/c3 are link down.
2022-05-12 14:...	Critical	Port Group Unhealthy	Port(s) 8/2/c4 are link down.

The 'Quick View' panel for 'Port Group: PG-1' includes the following sections:

- Info:**
 - Alias: PG-1
 - Description: Network Port Group
- Port Details:** 1 Port unhealthy

Port	Type	Status
8/1/x1	N	port is healthy
8/2/c3	N	Port is down
- Related Maps:** 0

- **Map Quick View:** Appears on clicking the source-id field on the 'Map Unhealthy' alarm.



Events

GigaVUE-FM keeps track of all events that occur in the system. The Events page lists all notifiable events that have occurred in the physical, virtual, and cloud. A variety of filters are also available to filter what events are displayed on the page.

This chapter covers the following topics:

- [Overview of Events](#)
- [View Events based on User RBAC Permissions](#)
- [Filter Events](#)
- [Archive or Purge Event Records](#)

Overview of Events

The Events page display the events generated from GigaVUE V Series Nodes or clusters, GigaVUE-VM virtual traffic visibility nodes, and cloud such as AWS that are stored in the GigaVUE-FM database. Refer to the following figure.

You can also manage the records by archiving them or purging them on a regular basis. Refer to [Archive or Purge Event Records](#).

Events											
All Events											
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...	

[Table 1: Event Parameters](#) describes the parameters recording for each event. You can also use filters to narrow down the results. Refer to [Filter Events](#).

Table 1: Event Parameters

Controls/ Parameters	Description
Source	The source from where the events are generated. The criteria can be as follows: - FM - indicates the event was flagged by the GigaVUE-FM. - IP address - is the address of the GigaVUE HC Series node that detected the event. For a node to be able to send notifications to the GigaVUE-FM, the SNMP_TRAP must be configured with the IP address of GigaVUE-FM specified as a host. Refer to the GigaVUE-Administration Guide for instructions on adding a destination for SNMP traps. - VMM - indicates the event was flagged by the Virtual Machine Manager. - FM Health - indicates the event was flagged due to the health status change of GigaVUE-FM.
Time	The timestamp when the event occurred. IMPORTANT: Timestamps are shown in the time zone of the client browser's computer and not the time zone of the node reporting the event. The timestamp is based on the correctly configured clock on the GigaVUE-FM server and converted from UTC to the client computer's configured time zone.
Event Type	The type of event that generated the events. The type of events can be CPU utilization high, cluster updated, device discovery failed, fan tray changed, netflow statistics, and so on.
Severity	The severity is one of Critical, Major, Minor, or Info. Info is informational messages. For example, when power status change notification is displayed, then the message is displayed as Info.
Affected Entity Type	The resource type associated with the event. For example, when low disk space notification is generated, 'Chassis' is displayed as the affected entity type.
Affected Entity	The resource ID of the affected entity type. For example, when low disk space notification is generated, the IP address of the node with the low disk space is displayed as the affected entity.
Alias	Event Alias
Device IP	The IP address of the device.
Host Name	The host name of the device.
Scope	The category to which the events belong. Events can belong to the following category: Domain, Node, Card, Port, Stack, Cluster, Chassis, GigaVUE-FM, GigaVUE-VM, and so on. For example, if there is a notification generated for port utilization low threshold, the scope is displayed as Physical Node.
Tags	Tags associated with the event
Description	The description of the event, which includes any of the possible notifications with additional identifying information where appropriate (such as reporting nodes IP address, username, and so on).

NOTE: The columns in the Events page can be customized based on the type of content you want to view in the table. For customizing the columns, refer to the “Table View Customization” section in the *GigaVUE Fabric Management Guide*.

View Events based on User RBAC Permissions

GigaVUE-FM allows you to view the events in the Events page based on the following RBAC permissions:

- **User Roles:** User role defines permission for users to perform any task or operation in GigaVUE-FM or the devices. For example, if you are a user with read and write access to the 'FM Security Management' category, then you will be able to see all events related to resources that belong to the GigaVUE-FM Security Management category such as users, roles, AAA services. Events related to other categories will be restricted. That is, you cannot view events related to physical resources such as ports, port groups, port pairs, cloud connections, cloud config that belong to the 'Infrastructure Management' category.
- **User Defined Tags:** Tags control the way you access the resources such as clusters, ports, port groups, port pairs, GigaSMART groups, GigaStreams and maps. You can view the events associated to tagged resources that you are permitted to access. For example, consider the following port pairs in the system:
 - Port pair PP1 is configured with tagKey: Location, tagValues - Seattle
 - Port pair PP2 is configured with tagKey: Location, tagValues - San FranciscoIf you are configured with tagKey: Location and tagValue: San Francisco, then you will be able to access only port pair PP2 based on your permitted tag. Therefore, you will see only events related to port pair PP2.

NOTE: In case of resources that do not support tagging, you will be able to see events from resource that are permitted as per your role definitions and events from the devices that are permitted as per the tags.

Users belonging to Super Admin, Admin and User groups will be able view all events as they have no restrictions on resources, permissions and tags.

Alarms for GigaVUE-FM Configurations

GigaVUE-FM generates alarms to track the changes in the health status of the following configurations:

- [Alarms for Inline Network Resources](#)
- [Alarms for GigaSMART Operations](#)
- [Alarms for Fabric Maps and Policies](#)

Alarms for Inline Network Resources

GigaVUE-FM generates alarms to track the changes in the health status of the inline network configurations. That is, whenever the health status of the following inline network resources changes from healthy to unhealthy, an alarm is triggered and the same can be viewed in the Alarms page. Alarms are cleared when the health status is green.

- Inline network
- Inline serial network
- Inline network group
- Inline network lag
- Inline tool
- Inline tool group
- Inline tool serial
- IB Pathway

For example, consider an inline network group created with two inline networks. If a port in one of the inline networks goes down, then the health status of the inline network and the inline network group also goes down. An alarm is triggered accordingly in the alarms pages. Alarms are cleared when the health status is green. You can view the alarms from the All Alarms and the Correlated Alarms view

Alarms for GigaSMART Operations

GigaVUE-FM generates alarms to track the changes in the health status of the GigaSMART operations.

Multiple GigaSMART engines can be grouped together to form a GigaSMART group . GigaSMART operations are tied to the GigaSMART groups. GigaVUE-FM monitors the health status of GigaSMART operations and triggers alarms when the status is unhealthy. The alarms are cleared when the health status is green.

Filter Events

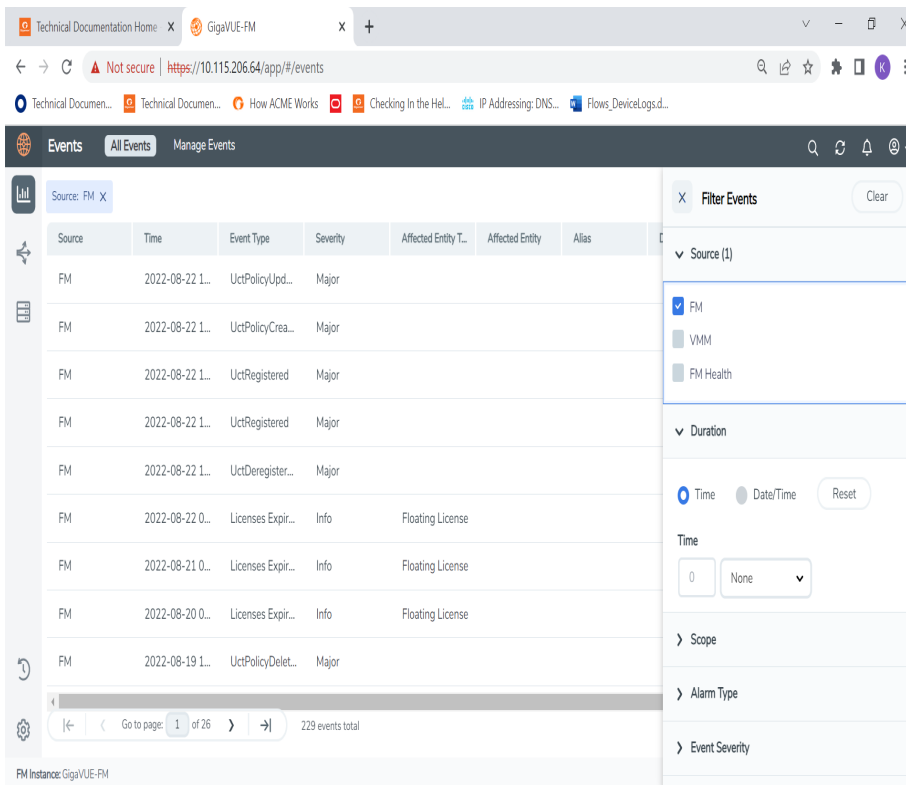
The events can be filtered based on the following criteria:

Controls/ Parameters	Description
Source	Displays the events generated by a specific source. NOTE: This option is not available in the Virtual Events page.
Duration	Displays the events occurred within a specific date range.
Scope	Displays the events associated with the selected category. For example, physical node, physical port, appliance server, and so on.
Event Type	Displays the events associated with the selected event type.
Alarm Type	Displays the events associated with the selected alarm type (applicable only for users with prime package license).
Event Severity	Displays the events that match the selected severity level.
Affected Entity Type	Displays the events associated with the affected entity type. The affected entity type can be Port, Cards, Chassis, and so on.
Status	Displays alarm events based on alarm status. Alarm status can be acknowledged or unacknowledged (applicable only for users with prime package license).
Cluster ID	Cluster ID of the cluster (applicable only for users with prime package license).
Affected Entity	Displays the events associated with the affected entity. The affected entity can be port ID, slot label, fan name, and so on.
Device IP	Displays the events associated with the IP address of the device. Partial IP addresses may be entered to display the results containing the specified octets. For example, if the last 2 octets of the IP address entered is 46.100, the IP addresses listed will include all those that end with 46.100.
Host Name	Displays the events associated with the host name of the device. Partial host name may be entered to filter the events. For example, if the first portion of the host name entered is GIMO, the host names listed will include all those that contain GIMO.
Alias	Displays alarm related events based on alarm component alias or id (applicable only for users with prime package license).
Show non-taggable Entities	Displays events for entities that cannot be tagged, such as Policies, GigaVUE-FM instance.
Tags	Tags associated with the event

To filter the event:

1. Click **Filter**.

The Filter quick view appears.



2. Specify the filter criteria. The event records will get filtered and displayed.
3. Click **Clear** to clear the filter.

Archive or Purge Event Records

Events are saved in the GigaVUE-FM database. Events records continues to grow over time. GigaVUE-FM allows you to archive and purge these records based on a specific date. Records older than that date will be exported to an SFTP server.

When archiving, the records are archived as a CSV file with a timestamp appended. For example, event-archive20200605143323.csv. The file is compressed to a zip file before exporting to the server.

The archive and purge option for events records is available to the following user categories:

- Users with Write permission on the Infrastructure Management, Traffic Control Management, FM Security Management, Whitelist Cups Management, Device Certificate, System Management, Others resource categories can archive their permitted Events.
- Users with Write permission on System Management category can purge events. Users belonging to this category will be able to purge all events older than the date provided. The Purge option will delete all events in the system, even those events that

are not visible to the user as per his role definition.

- Super-admin users can perform all the activities mentioned above.

NOTE: The archive and purge action for events is also recorded to the audit log.

To archive and purge the event records:

Manage Event Records

Event records can be purged by performing the following:

1. Select **Events** in the navigation pane.
2. Click **Manage Events**.
3. Click the Calendar icon and select a date. Records older than this date will be purged.

NOTE: The Purge operation removes the records from the database permanently.

Export Event Records

You can export the event records to an external server or download them as CSV or XLSX file to your local drive.

To export the event records to an external server:

1. Select **Events** in the navigation pane.
2. Click **Export > Export to Server**.
3. In the Export to Server pop-up that appears, click the Calendar icon and select a date. Records older than this date will be exported.
4. Specify the following details:
 - The address of the SFTP Server to which the records will be exported.
 - The user name and password for the SFTP server.
 - The file path on the server where the files will be archived.
4. Click **OK** to exported the records to the SFTP server, and then purge the records.

To download event records as a CSV or XLSX file:

1. Select **Events** in the navigation pane.
2. Click **Export > Export All** and specify the required format.

The Events file will get downloaded to the local folder.

All Audit Logs

This section describes the Audit Logs page and provides information about filtering and managing the logs. The topics covered are:

- [Overview of Audit Logs](#)
- [Filter Audit Logs](#)
- [Audit Logs Failure](#)
- [Archive or Purge Audit Log Records](#)

Overview of Audit Logs

The Audit Logs page captures audit logs for all users connected to the given GigaVUE-FM. There are 10 results shown by default on every page. The logs can also be further filtered to view specific information. Unlike the zipped logs under **Admin > System > Logs**, the audit logs can be seen by users. For more information about filtering, refer to .

The Audit Logs page displays the following parameters:

Parameters	Description
Time	Provides the timestamp on the log entries.
User	Provides the logged user information.
Operation Type	Provides specific entries that are logged by the system such as: • Log in and Log out based on users. • Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.
Entity type	Name of the resource type that the audit log is associated to such as port, port group, user, host name, device IP.
Source	Provides details on whether the user was in GigaVUE-FM or on the node when the event occurred.
Device IP	IP address of the device.
Hostname	Host name of the device.
Status	Success or Failure of the event.
Description	In the case of a failure, provides a brief update on the reason for the failure.
Tags	Tags associated with the audit logs

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

GigaVUE-FM allows you to filter and view audit logs based on the following RBAC permissions:

- **User Roles:** You can view the audit logs based on your user role which defines the category of resources that you can access.

- **User Defined Tags:** You can view the audit logs associated to tagged resources which you are permitted to access.

Filter Audit Logs

Filtering the audit logs allows you to display only those items of interest. You can filter based on any of the following:

- **Duration**—display logs that occurred within a specified time range.
- **Users**—display logs related a specific user or users.
- **Operation Type**—display logs for one or more operations, such as Create, Read, Update, and so on.
- **Source Type**—display logs for resource types that the audit log is associated to.
- **Status**—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:

- **Duration:** Select the required Date and Time range to display logs within a specific time range.
- **Users** limits the scope of what displays on the Audit Logs page to a specific user or users.
- **Operation Type** narrows the logs to the types of operation that the log is related to. You can select multiple operations.
- **Source:** Narrows the logs to the selected source such as GigaVUE-FM, VM, Devices.
- **Status** narrows the logs related to failures or successes.
- **Source Type** allows you to select the required entity type such as host name, device ip and so on.
- **Tags** associated to the audit logs which are acquired from a resource object

3. Click **Clear** to clear the selected filters to the Audit Logs page.

Audit Logs Failure

Starting in software version 6.3.00, for all LDAP errors, GigaVUE-FM will display an error message in the audit logs description field for all the failed authentication attempts. For authentication failures (48 and 49) alone, GigaVUE-FM will map the LDAP error codes and display a custom description.

Audit Logs										
All Audit Logs										
Manage Audit Logs										
	Time	User	Operation Type	Entity Type	Source	Device IP	Hostname	Status	Description	Tags
	2023-04-06 16...	SSOAdminUser	login fmUser S...	User	fm			SUCCESS		
	2023-04-06 16...	SSOAdminUser	login fmUser S...	User	fm			FAILURE	User [SSOAdmi...	
	2023-04-06 16...	admin	login fmUser ad...	User	fm			SUCCESS		
	2023-04-06 16...	SSOAdminUser	login fmUser S...	User	fm			FAILURE	User [SSOAdmi...	
	2023-04-06 15...	SSOAdminUser	logout fmUser ...	User	fm			SUCCESS		
	2023-04-06 15...	admin	logout fmUser ...	User	fm			SUCCESS		
	2023-04-06 15...	SSOAdminUser	login fmUser S...	User	fm			SUCCESS		
	2023-04-06 15...	admin	logout fmUser ...	User	fm			SUCCESS		

For all other error codes, GigaVUE-FM will display only the error code details. The following are examples of the error code message formats for LDAP errors.

[LDAP: error code 32 - 0000208D: NameErr: DSID-03100241, problem 2001 (NO_OBJECT), data 0, best match of: 'DC=hqdevtest,DC=com']

[LDAP: error code 34 - 0000208F: NameErr: DSID-0310022D, problem 2006 (BAD_NAME), data 8350, best match of: 'userbasedncheck']

Audit Logs										
All Audit Logs										
Manage Audit Logs										
	Time	User	Operation Type	Entity Type	Source	Device IP	Hostname	Status	Description	Tags
	2023-03-30 00...	SSOAdminUser	login fmUser S...	User	fm			FAILURE	User [SSOAdmi...	
	2023-03-30 00...	admin	update fmLdap...	FM LDAP Server	fm			SUCCESS		
	2023-03-30 00...	SSOAdminUser	login fmUser S...	User	fm			SUCCESS		
	2023-03-30 00...	admin	update fmAuth...	fm authentication	fm			SUCCESS		
	2023-03-30 00...	admin	update fmAuth...	fm authentication	fm			SUCCESS		
	2023-03-30 00...	admin	update fmLdap...	FM LDAP Server	fm			SUCCESS		
	2023-03-30 00...	admin	create fmLdapS...	FM LDAP Server	fm			SUCCESS		
	2023-03-30 00...	admin	delete fmLdapS...	FM LDAP Server	fm			SUCCESS		
	2023-03-29 23...	admin	login fmUser ad...	User	fm			SUCCESS		
	2023-03-29 23...	admin	login fmUser ad...	User	fm			FAILURE	User [admin] au...	

NOTE: In the event of failure of all the configured LDAP servers, GigaVUE-FM will display a single common error message in the audit logs description field. Refer to the following example.

Error connecting to all LDAP servers configured. Please see the logs for more detailed info

Refer to the following table for more information on the LDAP error codes, error message, and exception details.

LDAP Status Code	Meaning	Exception or Action
0	Success	Report success
1	Operations error	NamingException
2	Protocol error	CommunicationException
3	Time limit exceeded	TimeLimitExceededException
4	Size limit exceeded	SizeLimitExceededException
5	Compared false	Used by DirContext.search(). Does not generate an exception.
6	Compared true	Used by DirContext.search(). Does not generate an exception.
7	Authentication method not supported	AuthenticationNotSupportedException
8	Strong authentication required	AuthenticationNotSupportedException
9	Partial results being returned	If the environment property "java.naming.referral" is set to "ignore" or the contents of the error do not contain a referral, throw a PartialResultException. Otherwise, use contents to build a referral.
10	Referral encountered	If the environment property "java.naming.referral" is set to "ignore", then ignore. If the property is set to "throw", throw ReferralException. If the property is set to "follow", then the LDAP provider processes the referral. If the "java.naming.ldap.referral.limit" property has been exceeded, throw LimitExceededException.
11	Administrative limit exceeded	LimitExceededException
12	Unavailable critical extension requested	OperationNotSupportedException
13	Confidentiality required	AuthenticationNotSupportedException
14	SASL bind in progress	Used internally by the LDAP provider during authentication.
16	No such attribute exists	NoSuchAttributeException
17	An undefined attribute type	InvalidAttributeIdentifierException
18	Inappropriate matching	InvalidSearchFilterException
19	A constraint violation	InvalidAttributeValueException
20	An attribute or value already in use	AttributeInUseException
21	An invalid attribute syntax	InvalidAttributeValueException
32	No such object exists	NameNotFoundException
33	Alias problem	NamingException

LDAP Status Code	Meaning	Exception or Action
34	An invalid DN syntax	InvalidNameException
35	Is a leaf	Used by the LDAP provider; usually doesn't generate an exception.
36	Alias dereferencing problem	NamingException
48	Inappropriate authentication	AuthenticationNotSupportedException
49	Invalid credentials	AuthenticationException
50	Insufficient access rights	NoPermissionException
51	Busy	ServiceUnavailableException
52	Unavailable	ServiceUnavailableException
53	Unwilling to perform	OperationNotSupportedException
54	Loop detected	NamingException
64	Naming violation	InvalidNameException
65	Object class violation	SchemaViolationException
66	Not allowed on non-leaf	ContextNotEmptyException
67	Not allowed on RDN	SchemaViolationException
68	Entry already exists	NameAlreadyBoundException
69	Object class modifications prohibited	SchemaViolationException
71	Affects multiple DSAs	NamingException
80	Other	NamingException

Archive or Purge Audit Log Records

Audit logs are saved to the GigaVUE-FM database. Audit log records continues to grow over time. GigaVUE-FM allows you to archive these records based on a specific date. Records older than that date will be exported to an SFTP server.

The records are archived as a CSV file with a timestamp appended. For example, audit_20151005105607.csv. The file is compressed to a zip file before exporting to the server.

The archive and purge option for audit log records is available to the following user categories:

- Users with Write permission on Infrastructure Management, Traffic Control Management, FM Security Management, Whitelist Cups Management, Device Certificate, System Management, Others resource categories can archive their permitted audit logs.

- Users with Write permission on System Management category can purge audit logs.
- Super-admin users can perform all the activities mentioned above.

The archive and purge actions for audit logs are also recorded to the audit log. The Purge action for the audit log never purges the purge entry.

You can download the audit logs that are accessible to you. If Audit logs are empty either due to permissions or if no records are returned from the database, then you will not be able to download the .CSV file. The **Manage** button is disabled if there are no records to download.

Audit Logs									
All Audit Logs Manage Audit Logs									
Operations: Activate X Operations: Archive X Operations: Clear X Operations: Connect X Operations: Create X Filter Export									
Time	User	Operation Type	Entity Type	Source	Device IP	Hostname	Status	Description	Tags
2022-08-22 1...	admin	create uctTraf...	Kubernetes U...	container			SUCCESS		
2022-08-22 1...	admin	create fmUser ...	User	fm			FAILURE	GigaVUE-FM ...	
2022-08-22 1...	admin	create fmUser ...	User	fm			SUCCESS		
2022-08-19 1...	admin	create uctTraf...	Kubernetes U...	container			SUCCESS		
2022-08-18 1...	admin	create uctTraf...	Kubernetes U...	container			SUCCESS		
2022-08-18 1...	admin	create uctCon...	Kubernetes U...	vm			SUCCESS		
2022-08-18 1...	admin	create monitor...	Monitoring Do...	vm			SUCCESS		
2022-08-17 1...	admin	create tag value	Tag	fm			SUCCESS		

Go to page: 1 of 15 113 audit logs total

NOTE: Users with write permission to the System Management category can purge all audit logs. That is, the users audit logs as well as the audit logs of other users. Therefore, the manage button is enabled to purge even though the audit logs are empty for that user.

Manage Event Records

Event records can be purged by performing the following:

1. Select **Events** in the navigation pane.
2. Click **Manage Events**.
3. Click the Calendar icon and select a date. Records older than this date will be purged.

NOTE: The Purge operation removes the records from the database permanently.

Export Event Records

You can export the event records to an external server or download them as CSV or XLSX file to your local drive.

To export the event records to an external server:

1. Select **Events** in the navigation pane.
2. Click **Export > Export to Server**.
3. In the Export to Server pop-up that appears, click the Calendar icon and select a date. Records older than this date will be exported.
4. Specify the following details:
 - The address of the SFTP Server to which the records will be exported.
 - The user name and password for the SFTP server.
 - The file path on the server where the files will be archived.
4. Click **OK** to exported the records to the SFTP server, and then purge the records.

To download event records as a CSV or XLSX file:

1. Select **Events** in the navigation pane.
2. Click **Export > Export All** and specify the required format.

The Events file will get downloaded to the local folder.

System

The **System** pages provides a variety of options allowing you to set up key features of GigaVUE-FM. These pages allow you to configure licenses for GigaVUE-FM and GigaVUE-VM activation, set up notifications for events and their email recipients, and view event logs.

Go to **Settings** and click **System**, to access the system pages.

System provides access to the following pages:

- [Preferences](#)
- [SSH](#)
- [SNMP](#)
- [Port Packet Errors and Drops](#)
- [GigaStream Imbalance Notification](#)
- [Add New Template](#)
- [Node Details](#)
- [IP Resolver](#)
- [Backup/Restore](#)

- [Images](#)
- [Pre-requisites](#)
- [Event Notifications](#)
- [Export Data to External Data Server](#)
- [Licenses](#)
- [System Logs](#)
- [Storage Management](#)
- [Proxy Server Configuration](#)
- [Split DNS Configuration](#)

Preferences

The **Preferences** page displays the user profile and general settings for the current instance of GigaVUE-FM. Only users with administrative privileges can edit the Preferences.

Figure 15 Preferences for GigaVUE-FM

To change the GigaVUE-FM preferences:

Go to **Settings** and go to **System > Preferences**.

- Change the user name in the **Username** field.
- Click the **change password** link to change the password. (For more information about changing the password, refer to [Change Your Password](#).)

- Enter the Email address.
- Enter the Group name.

Under **Display & Session**:

- Toggle the **NOC View Mode** option, as required. If the **NOC View Mode** is set to on, then you cannot set the auto-logout time. Therefore, the session will never be logged-out and the following screens get refreshed continuously:
 - Alarm
 - All Audit Logs
 - Administrator/Events
 - High Availability
 - Flows
 - Backup Files
 - Image Servers
 - Internal Image Files
 - Licenses
 - Search Results pages
 - Tags
 - Tools
 - Chassis List & Topology View
 - GS Dump
 - Sys Dump
 - All the statistics pages
 - Map Groups
 - Circuit Groups
 - Circuit Tunnels
 - Ports Discovery
 - Virtual Nodes
 - Virtual Maps
 - Virtual Centers
 - Virtual Switches
 - NSX Virtual Nodes
 - NSX Virtual Maps
 - NSX Servers
 - Sys Logs
- Set the frequency of screen refresh using the **Screen Refresh Rate (min)** drop-down option. You can select from 0.5 to 5 minutes.

- Set the Idle logout time using the **Idle Logout Time (min)**¹ option. You can configure the idle logout time to a minimum of 5 minutes and a maximum of 300 minutes. The idle logout time becomes immediately effective. For more information, refer to [Idle Timeout Enforcement](#).
- Toggle the Session TTL option, as required. If the session TTL is enabled, sessions are terminated once their maximum lifespan is reached. For more information, refer to [Session Time-To-Live](#)
- Set the maximum number of concurrent session per user allowed to log into GigaVUE-FM. For more information, refer to [Maximum Sessions](#).
- The **NOC View Mode** must be set to off to configure the auto logout time.
- Starting from software version 6.3.00, the default value for the auto-logout time is set to 10 minutes.
- When upgrading from previous software version to 6.3.00, the default value is retained from the previous version of GigaVUE-FM. If you are installing GigaVUE-FM 6.3.00 directly, the default value is configured as 10 minutes.
- You will be logged out of GigaVUE-FM if the UI remained inactive for the period configured, and if you failed to respond to the inactive alert message prompted in the UI. The following processes will not be impacted (which usually take some time to complete):
 - GigaVUE-FM upgrade
 - Device upgrade
 - GigaVUE-FM HA deployment
 - GigaVUE-FM scale tasks

NOTE: When performing configurations in the UI, if you are inactive on the screen, then you may get logged out from GigaVUE-FM due to the idle time out configuration. If you had failed to save the configurations, then on logging in again, the configurations will be lost and you must reconfigure the settings again.

Under **General** Category:

- Enter a name for the GigaVUE-FM instance in the **FM Instance Name** box. The GigaVUE-FM instance name is displayed in the browser tab as well as beside the GigaVUE-FM logo. Refer to the “*Adding the GigaVUE-FM Instance Name*” section in the “*GigaVUE Fabric Management Guide*”.
- Configure a pre-login banner which states the security policy of your company or organization in the Login Infobox. For more information about configuring a custom banner, refer to the [Configure a Custom Banner](#) section in the “*GigaVUE Fabric Management Guide*”.

¹The maximum duration GigaVUE-FM can be inactive before it is logged out automatically.

Flows is disabled by default in GigaVUE-FM. You can change the status to enabled using the toggle option.

NOTE: Once you enable Flows you cannot disable it again. Contact Customer Support to disable Flows. Refer to the "Flows" section in the *GigaVUE-FM User's Guide* for detailed information.

GigaVUE-FM acts as the default syslog server. You can also use external syslog servers using the following options:

- **Syslog server:** Use the **Status** toggle option to enable or disable GigaVUE-FM to act as the syslog server. As you toggle between these options, the devices will be configured asynchronously in the background.
- **Forward Events to System Log:**
 - **Enable System Logs:** Turn on this option to forward events to external syslog servers.
 - **Event Category:** Category based on which the events GigaVUE-FM forwards it to the syslog level.
 - **Severity Level:** Severity level for the events.

NOTE: For optimized performance of GigaVUE-FM use an external syslog server, that is, disable GigaVUE-FM as syslog server. Instead, use an external syslog collector.

Based on the system memory, the following throttling options are available when GigaVUE-FM acts as the syslog server:

- less than or equal to 16GB -> 100 syslogs/minute
- less than or equal to 32GB -> 1000 syslogs/minute
- greater than 32GB -> 5000 syslogs/minute

Throttling will be audited in the Events page.

Security Settings: For Security Settings, refer to [Are all versions of GigaVUE-FM validated for FIPS compliance?](#)

Image Upgrade: For image upgrade, refer to [Upgrade from the UI](#).

API Request Limit (Number of Request): Enter the API request limit count range from 200 to 65536. Setting the API Request Limit above 5000 and a minimum value of 200 negatively affects GigaVUE-FM performance. It is recommended to enter a value more than 201 and less than 5000. If the API limit is exceeded, an event will be triggered. If the violations continue, GigaVUE-FM throttles the subsequent events. The throttled events

will have a default absorption window of 30 minutes. You can view these events on the Events page. Refer to [GigaVUE® Fabric Management Events](#) for more information on events.

API Limit Period: Enter the API limit duration from 30 to 60 Seconds.

Idle Timeout Enforcement

Sessions are automatically invalidated after inactivity, reducing the risk of unauthorized access from unattended sessions.

Session Time-To-Live

Sessions are terminated once their maximum lifespan is reached, regardless of activity, ensuring tighter control over session duration. When the **Session Time-To-Live** (TTL) option is enabled, sessions will end after the maximum lifespan specified in the **Session TTL Time** field is reached. The Session TTL time can be set from 1 to 24 hours. If the session TTL feature is disabled, GigaVUE-FM sessions will terminate based on the browser's cookie settings.

Maximum Sessions

You can configure your sessions to open concurrently, with a limit of 1 to 10 sessions. If you exceed this limit, GigaVUE-FM displays a screen with a message that you've reached the maximum number of login sessions. To continue, log out of any open sessions by selecting one from the list displayed in the screen and ending it.

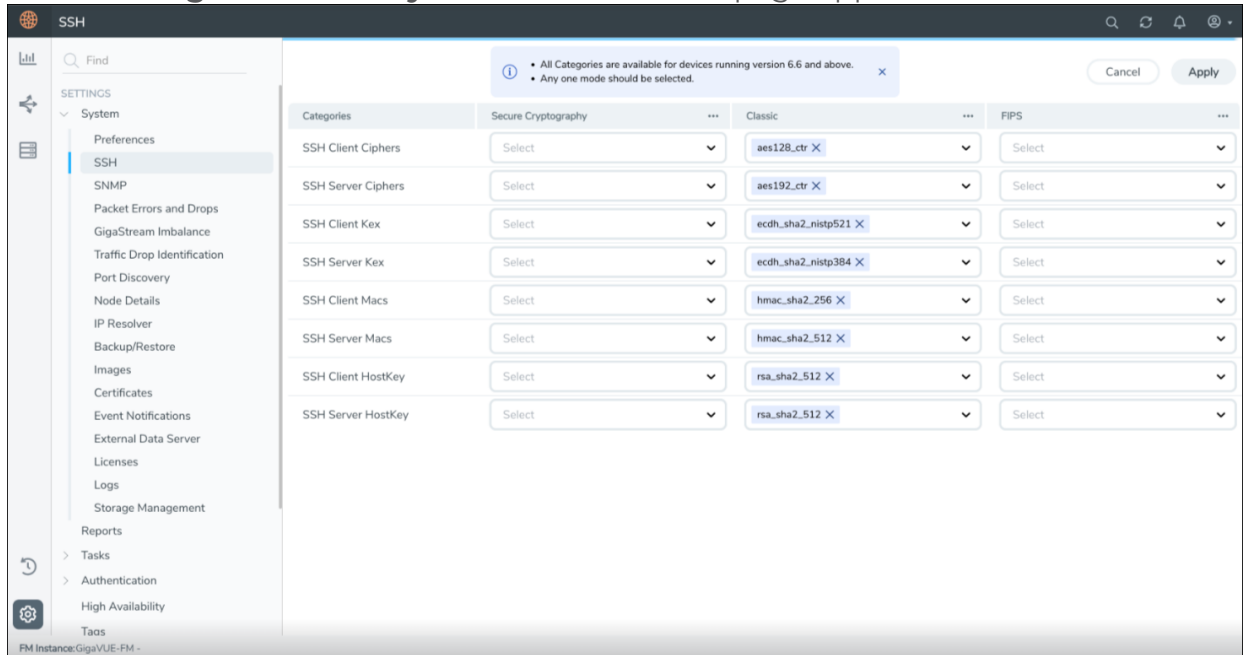
SSH

The SSH configuration page allows you to exclude less secure SSH cryptographic options, enabling you to configure only the most secure or preferred cryptographic settings. This provides greater control over the system's security. This page allows you to configure ciphers, key exchange algorithms (Kex), Message Authentication Codes (MACs), and HostKey algorithms for both the SSH client and server.

Configure SSH options

To configure SSH options:

1. Go to **Settings** and select **System**> **SSH**. The SSH page appears.



2. Click the **ellipses** next to the **secure cryptography**, **classic**, and **FIPS** fields. Select **Select All**, **De-select All**, and **Set as Default** as required.
 - a. Click **Select All** to select the supported values in the fields.
 - b. Click **De-select All** to remove the selected values in the fields. If values are not assigned to the fields, default values are automatically updated in the fields.
 - c. Click **Set as Default** to set the pre-defined values in the fields.

3. Select the following details:

Field	Description
SSH Client Ciphers	Select the ciphers to be used by the ssh client in the machine. The following ciphers are allowed in the secure cryptography field: • aes128-cbc • aes128-gcm@openssh.com • aes256-cbc • aes256-gcm@openssh.com The following ciphers are allowed in the classic field: • aes128-cbc * • aes128-ctr • aes128-gcm@openssh.com • aes192-ctr • aes256-cbc* • aes256-ctr • aes256-gcm@openssh.com • chacha20-poly1305@openssh.com The following ciphers are allowed in the FIPS field: • aes128-cbc • aes128-gcm@openssh.com • aes256-cbc • aes256-gcm@openssh.com
SSH Server Ciphers	Select the ciphers to be used by the ssh server in the machine. The following ciphers are allowed in the secure cryptography field: • aes128-cbc • aes128-gcm@openssh.com • aes256-cbc • aes256-gcm@openssh.com The following ciphers are allowed in the classic field: • aes128-cbc * • aes128-ctr • aes128-gcm@openssh.com • aes192-ctr • aes256-cbc* • aes256-ctr • aes256-gcm@openssh.com • chacha20-poly1305@openssh.com The following ciphers are allowed in the FIPS field: • aes128-cbc

Field	Description
	• aes128-gcm@openssh.com • aes256-cbc • aes256-gcm@openssh.com
SSH Client Kex	Select the kex to be used by the ssh client in the machine. The following kex are allowed in the secure cryptography field: • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 The following kex are allowed in the classic field: • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 • diffie-hellman-group14-sha256 • curve25519-sha256 • curve25519-sha256@libssh.org • diffie-hellman-group-exchange-sha256 • diffie-hellman-group16-sha512 • diffie-hellman-group18-sha512 The following kex are allowed in the FIPS field: • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521
SSH Server Kex	Select the kex to be used by the ssh server in the machine. The following kex are allowed in the secure cryptography field: • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 The following kex are allowed in the classic field: • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 • diffie-hellman-group14-sha256 • curve25519-sha256 • curve25519-sha256@libssh.org • diffie-hellman-group-exchange-sha256 • diffie-hellman-group16-sha512 • diffie-hellman-group18-sha512 The following kex are allowed in the FIPS field:

Field	Description
	• ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521
SSH Client Macs	Select the macs to be used by the ssh client in the machine. The following macs are allowed in the secure cryptography, classic, and FIPS field: • hmac-sha2-512 • hmac-sha2-256 • hmac-sha2-256-etm@openssh.com • hmac-sha2-512-etm@openssh.com • umac-128-etm@openssh.com

Field	Description
SSH Server Macs	Select the macs to be used by the ssh server in the machine. The following macs are allowed in the secure cryptography, classic, and FIPS field: • hmac-sha2-512 • hmac-sha2-256 • hmac-sha2-256-etm@openssh.com • hmac-sha2-512-etm@openssh.com • umac-128-etm@openssh.com
SSH Client Hostkey	Select the hostkey to be used by the ssh client in the machine. The following hostkeys are allowed in the secure cryptography field: • ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521 The following hostkeys are allowed in the classic field: • ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521 • rsa-sha2-512 • rsa-sha2-256 The following hostkeys are allowed in the FIPS field: • ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521
SSH Server Hostkey	Select the hostkey to be used by the ssh server in the machine. The following hostkey is allowed in the secure cryptography field: • ecdsa-sha2-nistp384 The following hostkeys are allowed in the classic field: • rsa-sha2-512 • rsa-sha2-256 The following hostkey is allowed in the FIPS field: • ecdsa-sha2-nistp384

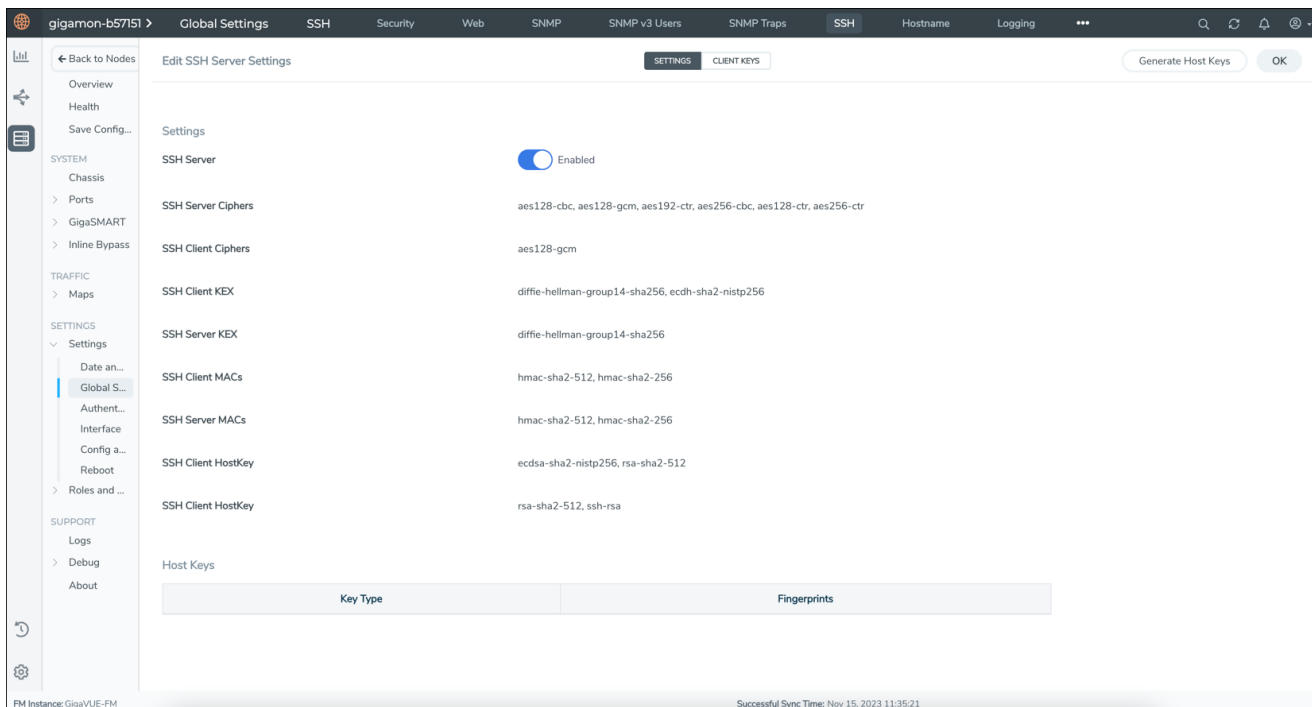
4. Click **Apply** to update the selected configurations.

View SSH options

Once the SSH management configurations are updated, you can view the applied configurations on the global settings page.

1. On the left navigation pane, go to **Inventory**  select **Nodes**.
2. In the Physical Nodes page, select the node for which you want to view the SSH configurations.

3. Go to **Settings > Global Settings > SSH**.
4. The selected ciphers, kex, macs, and hostkey algorithms for SSH client and server are listed on the settings page.



NOTE: For any settings or configurations outside the purview of GigaVUE-FM, please reach out to Gigamon Support at support@gigamon.com. You can also refer to <https://www.gigamon.com/support-and-services/contact-support> for Technical Support hours and contact information.

FIPS Compliance in GigaVUE-FM

GigaVUE-FM is compliant with the Federal Information Processing Standard (FIPS), a US government standard for security requirements of cryptographic modules. The FIPS module used in GigaVUE-FM is compliant with FIPS 140-3 and was validated by the National Institute of Standards and Technology (NIST). The certificate number is 4912. For more information, refer to [Cryptographic Module Validation Program – Certificate 4912](#).

Refer to the following sections for details:

Rules, Notes and Limitations

Refer to the following rules and notes for FIPS:

- After upgrading GigaVUE-FM instance from pre 5.16.00 to 5.16.00 or above, GigaVUE-FM boots in non-FIPS mode.

- FIPS is disabled by default in GigaVUE-FM. You can enable FIPS whenever needed. However, once enabled you cannot disable it.
- Only users with super admin privileges can enable FIPS.

Refer to the Frequently Asked Questions section for further details.

Configure FIPS in GigaVUE-FM

To configure FIPS in GigaVUE-FM:

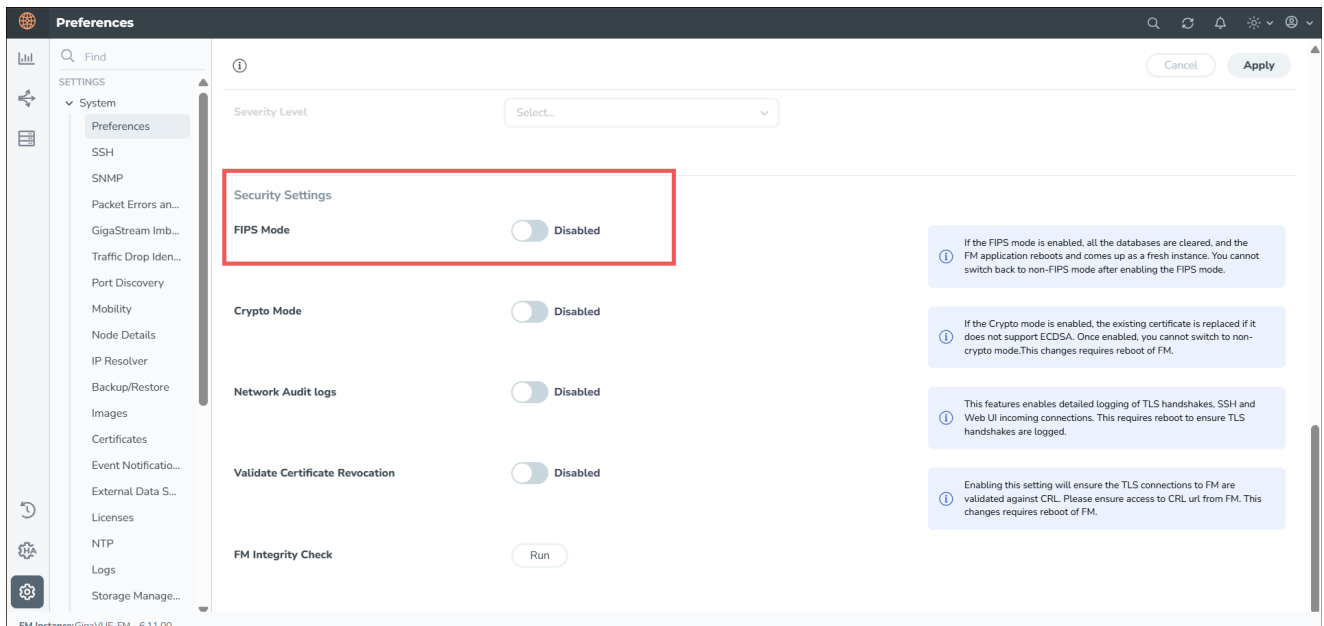
1. Go to **Settings** and go to **System > Preferences**.
2. Under **Security Settings**, enable the **FIPS Mode**.

NOTE:

- Do not enable FIPS Mode and Crypto Mode in the same request. Enable FIPS Mode first.
- After the system restarts, enable Crypto Mode in a separate request.

3. Click **Apply** to save the changes.
4. GigaVUE-FM will restart automatically after switching to FIPS Mode. Once the reboot completes, clear your browser cache and cookies to ensure the GigaVUE-FM IDP URL loads correctly.

NOTE: Once enabled, the toggle button is disabled. You cannot switch back to non-FIPS mode.



Configure FIPS in GigaVUE-FM High Availability Group

To form a FIPS enabled High Availability (HA) group:

- Enable FIPS in each of the standalone GigaVUE-FM instances.
- Assemble the HA group with FIPS enabled standalone GigaVUE-FM instances.

NOTE: You cannot add a GigaVUE-FM instance that is not FIPS enabled to a FIPS enabled High Availability group. Similarly, you cannot add a FIPS-enabled GigaVUE-FM instance to a High Availability group that is not FIPS enabled.

Enabled TLS Cipher Suites

GigaVUE-FM supports the commonly-supported TLS 1.2 and TLS 1.3 ciphers. The following ciphers are supported in TLS 1.2:

Supported TLS 1.2 Ciphers

Cipher Name	Key Exchange (Kx)	Authentication (Au)	Encryption (Enc)	MAC
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	ECDSA	AES256-GCM	SHA384
ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE	ECDSA	AES128-GCM	SHA256
ECDHE-ECDSA-AES256-SHA384	ECDHE	ECDSA	AES256	SHA384
ECDHE-ECDSA-AES128-SHA256	ECDHE	ECDSA	AES128	SHA256

Frequently Asked Questions

This page lists some of the most common issues and question related to FIPS.

Are all versions of GigaVUE-FM validated for FIPS compliance?

GigaVUE-FM versions 5.12.00.01 and 5.16.00 through 6.11 are compliant with FIPS 140-2. GigaVUE-FM version 6.11.01 and later are compliant with FIPS 140-3.

Can you enable FIPS using the fmctl command?

No. There is no support for enabling FIPS using the `fmctl` command. You can enable FIPS only using the GigaVUE-FM GUI.

Can you add a device that is not FIPS-compliant to a FIPS enabled GigaVUE-FM?

Yes. You can add a non FIPS compliant device to a FIPS enabled GigaVUE-FM.

What happens to the GigaVUE-FM database after you enable FIPS?

The GigaVUE-FM database is reset. GigaVUE-FM reboots and comes up as a new instance. You must reconfigure and setup GigaVUE-FM again.

How do I perform backup and restore operation on a FIPS enabled GigaVUE-FM?

A backup taken on a FIPS enabled GigaVUE-FM can only be restored on a GigaVUE-FM instance that is FIPS enabled. Similarly, backup taken on a non-FIPS GigaVUE-FM can be restored only on a non FIPS GigaVUE-FM.

Is the FIPS certification applicable for GigaVUE-FM instance irrespective of where it is deployed?

No. GigaVUE-FM Hardware appliance is only validated for FIPS certification.

SNMP

You can perform the following configurations from the SNMP Traps page:

- SNMP Traps
- SNMP Throttling
- Port Utilization Threshold
- Energy Saver
- SNMPv3 User

SNMP Traps

The SNMP Traps page shows the configuration settings applied to the devices managed by GigaVUE-FM. This page also allows you to configure the settings that need to be applied to all the devices managed by the GigaVUE-FM instance.

When the GigaVUE-FM instance starts, the following SNMP traps are enabled by default, for all the devices (indicated by → in the GUI):

- Link Status or Speed Change
- Module Change
- Fan Status Change
- Power Supply Status Change
- Inline Bypass Forwarding State Change

The traffic health state of the ports and devices is computed based on the SNMP traps. Therefore, in addition to the above traps, the SNMP traps that are used to determine the health status of the ports and devices are also enabled by default.

For more information about the traps supported, refer to [GigaVUE® Fabric Management Events](#)



For optimum performance of GigaVUE-FM, SNMP trap processing is disabled during the first config refresh cycle, as in the following cases:

- When GigaVUE-FM starts or restarts.
- When node comes back after being down.

NOTE: You must audit the SNMP trap list again to ensure that the System Reset Trap is enabled on all devices.

Traffic Health State Based on SNMP Traps

GigaVUE-FM determines the traffic health state of the devices and ports as follows:

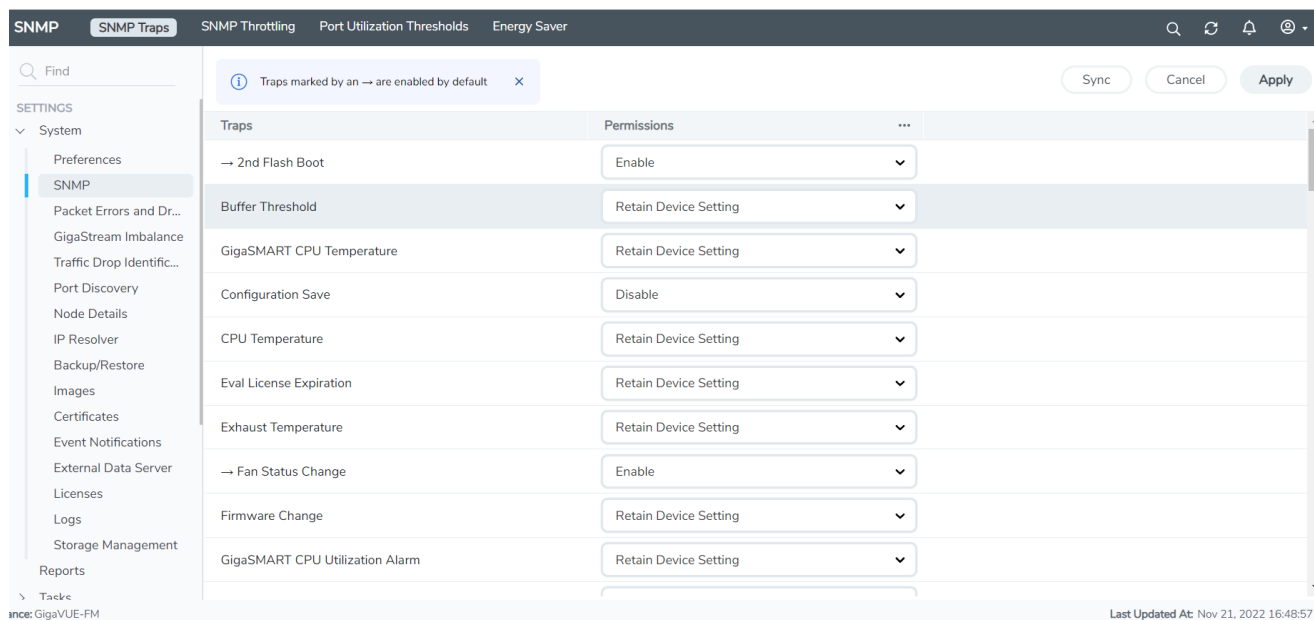
- If GigaVUE-FM receives any of the traffic health related traps mentioned above: Port state is set to yellow or red.
- If no further traps are received within the configured interval, which is 5 minutes: Port state is set to green.
 - For utilization thresholds, the health status will be reset as soon as GigaVUE-FM receives clear trap from the device.



- When a new device is added to GigaVUE-FM, the traps that determine the health status of the ports and devices are enabled, by default. However, if some of these traps are disabled in the device, then GigaVUE-FM cannot determine the health status.
- When GigaVUE-FM reboots, the traffic health status of all the devices will be cleared and will be recomputed based on the subsequent traps received by GigaVUE-FM.

Configure SNMP Traps

Go to **Settings** to access SNMP Traps and select **System > SNMP Traps**.



The SNMP Traps page allows you to perform the following configurations:

- Enable, disable or retain device settings for all the traps for all the devices: Click the **ellipses** next to the **Permissions** field. Select **Enable All**, **Disable All** or **Retain Device Settings for All Traps** as required.
- Enable, disable or retain device settings for specific traps for all the devices using the **Enable**, **Disable**, **Retain Device Settings** drop-down against each of the traps.

After making the required configurations:

1. Click **Apply** to apply the configuration.
2. Click the **Sync** button to synchronize the global SNMP settings to all the devices.

With this functionality, the following configuration settings are applied to all the devices:

- Specific configuration type changes
- Audit configuration changes

NOTE: If a new device is added to GigaVUE-FM, then the global configuration setting is applied to the new device. If for some reason, the configuration setting is not applied to a device, then an event is raised with the appropriate details in the Events page.

If a trap has been forcefully enabled/disabled on a device because of the global configuration setting, then an event is raised with the appropriate details in the Events page.

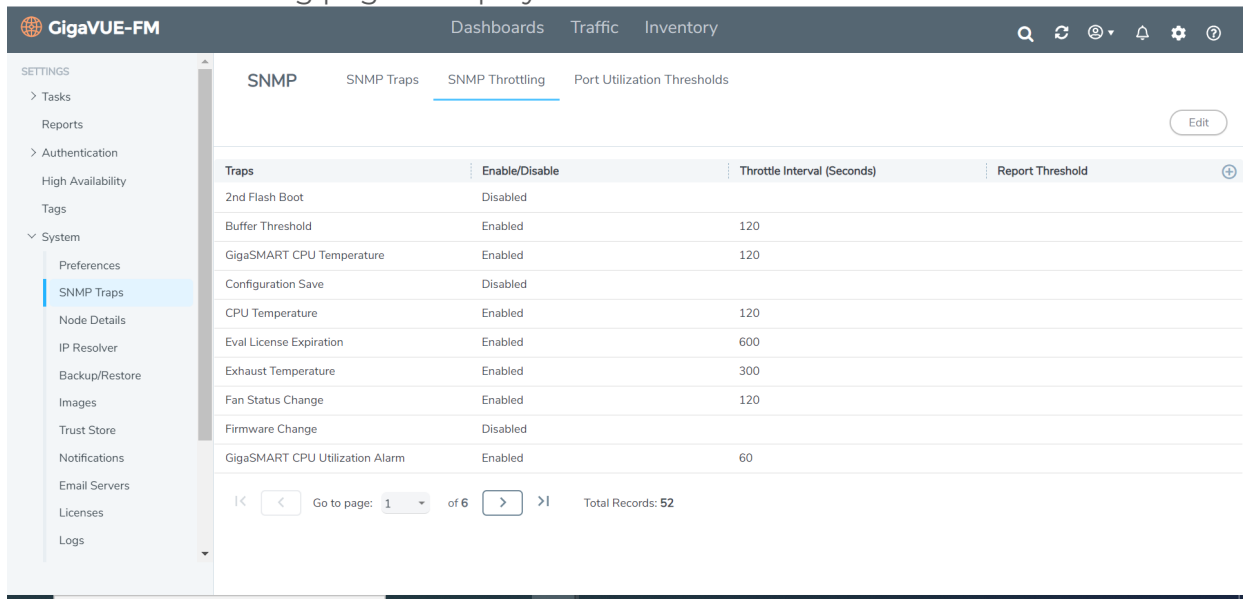
SNMP Throttling

Using SNMP Throttling, you can reduce the flooding of SNMP traps. You can manage the flooding by configuring the nodes with appropriate parameters for the trap events.

It is recommended that you enable SNMP Throttle for your SNMP Traps.

To configure SNMP Throttling:

1. On the right side of the top navigation bar, click .
2. On the left navigation pane, go to **System**, click **SNMP Traps** > **SNMP Throttling**. The SNMP Throttling page is displayed.



Traps	Enable/Disable	Throttle Interval (Seconds)	Report Threshold
2nd Flash Boot	Disabled		
Buffer Threshold	Enabled	120	
GigaSMART CPU Temperature	Enabled	120	
Configuration Save	Disabled		
CPU Temperature	Enabled	120	
Eval License Expiration	Enabled	600	
Exhaust Temperature	Enabled	300	
Fan Status Change	Enabled	120	
Firmware Change	Disabled		
GigaSMART CPU Utilization Alarm	Enabled	60	

3. Click **Edit**. For each of the traps configure the following:
 - **Permissions:** Enable or disable the throttle. Click the Ellipses at the top to enable or disable throttle for all the traps.
 - **Throttling Interval:** Configure the throttling interval. The throttling interval is configured by default for some of the traps (which is displayed in the page).
 - **Report Threshold:** Configure the threshold limit for each of the traps based on which a throttle report trap is sent at the end of the interval. You can view the report in the Alarms and Events page.
4. Click **Apply** to apply the configuration.

NOTE: SNMP throttling is available for all traps for all devices running software version 5.5.00 and above. For devices running earlier versions, SNMP throttling is available only for the following three traps:

- Link Status or Speed Change
- Packet Drop
- Packet Rx/Tx Error

SNMP throttling from device is different from throttling Near-Real Time status notification from GigaVUE-FM to GigaVUE-FM GUI. GigaVUE-FM throttles all the events (SNMP events sent by the device, state changes performed by the user, and status updates through GigaVUE-FM), and the events are pushed at the cluster level, summary level and global level. Refer to the following table for more details:

Throttle Level	GUI Screens	Count and Interval	Description
Cluster	GUI screens related to cluster	2 events per 5 second	Events to the particular cluster will be throttled
Summary	Dashboard, Physical nodes		Events across all the cluster will be throttled
Global	GUI screens related to solutions		Events across all the solutions will be throttled

Port Utilization Threshold

You can configure the utilization threshold for ports from this page. You can configure both the upper (high) and lower threshold limits based on which an alarm is triggered.

To configure port utilization:

1. Go to **Settings** and select **System > SNMP Traps > Port Utilization Threshold**.

The screenshot displays the 'Port Utilization Thresholds' configuration page in the GigaVUE-FM GUI. The left sidebar shows the navigation menu with 'SETTINGS' expanded and 'SNMP' selected. The main content area features a header with 'SNMP', 'SNMP Traps', 'SNMP Throttling', 'Port Utilization Thresholds', and 'Energy Saver'. A notification bar states 'All form elements are mandatory unless indicated as optional.' Below this, a message indicates 'Port utilization thresholds configuration is applied to device clusters version 5.10 and above.' The configuration includes two input fields: 'High Utilization Threshold (%)' and 'Low Utilization Threshold (%)', both currently set to '1-100'. At the bottom, the status bar shows 'FM Instance: GigaVUE-FM' and 'Last Updated At: Nov 21, 2022 19:49:45'.

2. Configure the high and lower utilization threshold values. Click **Apply**.
3. The configured port utilization threshold values will be applied for devices running software version 5.10.00 and higher.

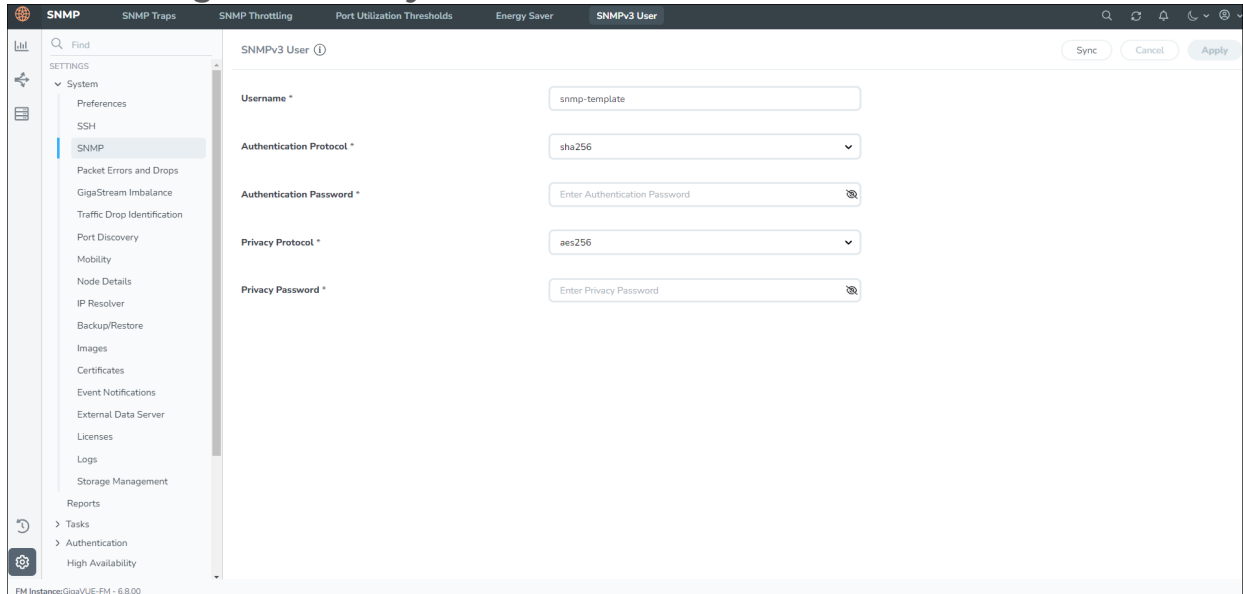
NOTE: GigaVUE-FM allows you to create the threshold values when you first access the GigaVUE-FM instance. Once the values are configured, you can only edit the values using the Edit option. When a new device is added to GigaVUE-FM, then the port utilization threshold setting is applied to the new device. If for some reason, the threshold setting is not applied to a device, then an event is raised with the appropriate details in the Events page.

SNMPv3 User

You can manage the SNMPv3 user template from this page. GigaVUE-FM uses this SNMPv3 user configuration to register an SNMPv3 target on the GigaVUE-OS nodes. This setting applies to all nodes running GigaVUE-OS with version 6.8 and above.

To configure an SNMPv3 user, do the following:

1. Go to **Settings** and select **System > SNMP > SNMPv3 User**.



2. Enter the information for the SNMPv3 user.
 - **Username**—the name of the global template SNMPv3 user.
 - **Authentication Protocol**—the authentication type is either **md5** or **sha1** or **sha256** or **sha384** or **sha512**, which specifies the mechanism to use for password hashing.
 - **Authentication Password**—the password used to authenticate the user specified by **Username**.
 - **Privacy Protocol**—the privacy type specifies the level of encryption for the password, which is either **des** or **aes-128** or **aes-256**.
 - **Privacy Password**—When the privacy type is selected, a privacy password can be configured and linked to a specific user by their **Username**. If no privacy type is specified but a privacy password is entered, the default privacy type will be set to **aes-128**.
3. Click **Apply** to apply the configuration.
4. Click the **Sync** button to synchronize the global SNMPv3 user configuration to all the applicable devices.

Port Packet Errors and Drops

GigaVUE HC Series and GigaVUE TA Series devices generate SNMP traps for packet drops and packet errors that occur in the port for both ingress and egress traffic. The traps are sent to GigaVUE-FM based on which alarms are often triggered, even for a single packet drop or error. Starting in software version 5.14.00, GigaVUE-FM allows you to configure threshold values for port packet drop/error based on which the number of traps and alarms can be controlled.

NOTE: Configuring SNMP throttling (see [SNMP Throttling](#) section) only reduces the number of traps. However, with SNMP throttling it is possible for significant traps to get dropped and unwanted traps to get through the throttling process. Use the Port Packet Drop/Error configuration to generate traps that are of significance.

G-TAP A Series Equipment	Power Type	Description
GTP-ATX01	AC	G-TAP A-TX Copper. Taps one 10/100/1000 Base-T (UTP) Ethernet link.
GTP-ATX02	DC	
GTP-ATX00	PST	G-TAP A-TX Copper for use with PST-GTA01 Power Supply Tray (no AC adapter).
GTP-ASF01	AC	G-TAP A-SF. Accepts fiber and copper SFP/SFP+ transceivers to tap a single 10G/1G link.
GTP-ASF02	DC	
GTP-ASF00	PST	G-TAP A-SF for use with PST-GTA01 Power Supply Tray (no AC adapter).
PST-GTA01	AC	1U Power Supply Tray. Powers up to 24 A Series taps.
PST-GTA02	DC	
GTP-ATX01-UN	AC	G-TAP A Series, Always on Copper TAP, AC Power (EU, UK, NA/JP, AU plugs).
GTP-ASF01-UN	AC	G-TAP A Series, Always on SFP/SFP+ TAP, AC Power (EU, UK, NA/JP, AU plugs).

GigaVUE-FM allows you configure threshold values for packet drop/error for the port at the following three levels:

Configuration Level	Description	Notes
Port Level Configuration	Applies to a specific port.	Has the highest priority and overrides the port level and global level configuration.
Port Type Level Configuration	Applies to all ports of a particular port type.	Has the second highest priority and overrides the global level configuration.
Global Level Configuration	Applies to all ports.	Has the lowest priority.

Packet Drop/Error threshold for a port can be configured for both Rx and Tx, and consists of setting up the following values:

- Percentage of packets dropped/has error.
- Number of packets dropped/has error in a given interval

Traps are generated in the devices only if:

Packet Drop/Error % > Drop/Error Threshold % Configured

AND

Number of Packets Dropped/Error > Drop/Error Threshold Count Configured

Allowable range:

- **For percentage:** 0 to 100. Percentage value can be configured as low as 0.0001%
- **For count:** >0

NOTE: If you configure '-1', the feature will be disabled for those ports, and traps will be generated for every packet drop and error.

You can configure the threshold from the device settings page or from global settings page of GigaVUE-FM. Refer to the following sections for details:

- [Configure Port Packet Drop/Error in Devices](#)
- [Configure Port Packet Drop/Error in GigaVUE-FM](#)

Refer to the GigaVUE CLI Reference guide for the corresponding CLI commands for configuring the port packet drop/error threshold values.

Configure Port Packet Drop/Error in GigaVUE-FM

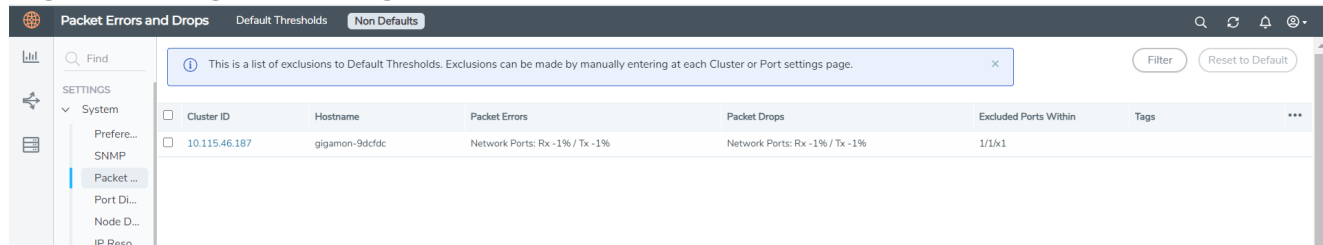
You can configure the port packet drop/error threshold globally for all the devices managed by GigaVUE-FM. To configure the port packet drop/error in GigaVUE-FM:

1. On the left navigation bar, click .
2. Select **System > Packet Errors and Drops**. The Packet Errors and Drops page is displayed:

Configuration Level	Description
Packet Drop Threshold	Percentage and count value for packet drop threshold configuration for Rx and Tx.
Packet Error Threshold	Percentage and count value for packet error threshold configuration for Rx and Tx.
Port Type	Port type for which the threshold is to be configured. Configuration for <i>All Ports</i> will be applied to all the ports (this is equivalent to the global level in device CLI).

If the device configuration is different from the global level configuration or the device has port-level configuration, then those devices will be listed in the Non Defaults page. Configurations changes at the global level will not be applied to the devices in the Non Defaults page.

Use the **Reset** button to remove the current device-level configuration and to apply the GigaVUE-FM global configuration.



Related topics

- [Port Packet Errors and Drops](#)
- [Configure Port Packet Drop/Error in Devices](#)

GigaStream Imbalance Notification

In GigaVUE-OS nodes, traffic is distributed across the ports in a GigaStream based on the following criteria:

- Type and volume of the incoming traffic
- Configurations defined in the Advanced Hash Settings page for the selected line card or chassis. Refer to the Advanced Hashing section in the Fabric Management guide for more details.

Consider a scenario in which **ip4src** and **ip4dst** are configured as advanced hash methods. Accordingly, traffic is distributed based on the matching IP source and IP destination addresses.

- In case of high traffic volume on a particular IP address or subnet, one or more ports within the GigaStream group will receive more traffic compared to the other ports.
- Alternatively, if there is a low traffic volume on a particular IP address or subnet, one or more ports within the GigaStream group will receive lower traffic compared to the other ports.

A small variation in traffic volumes across the ports in a GigaStream is expected and is acceptable. Large variation in traffic volume causes packet drops due to over subscription or under subscription of ports. With the GigaStream imbalance notification functionality, the port statistics of the member ports in a GigaStream are validated to determine if the variation in traffic distribution across the ports does not exceed or fall

below a user-defined threshold value limit. If traffic distribution is not within the allowed variance limit, the GigaVUE HC Series and TA Series devices generate SNMP traps that are sent to GigaVUE-FM based on which GigaStream imbalance alarms are triggered.

SNMP traps are generated in the devices based on the following criteria:

- Variance threshold % configured either through GigaVUE-FM or CLI (refer to the [Example](#) for more details)
- Distribution of traffic between the ports (on a 30 second interval)



If GigaStream port group has a persistent imbalance in traffic, it is recommended to:

- Change the Advanced Hash settings
- Use a Weighted GigaStream to apply more hashing buckets to under utilized ports and lesser hashing buckets to over utilized ports

The following SNMP traps are triggered in the devices:

- For imbalanced traffic distribution: gigamonSnmpGigastreamImbalanceNotification
- On recovery of balanced traffic: gigamonSnmpGigastreamRecoveryNotification

To manage the SNMP traps, you can either use the SNMP throttling feature or the GigaStream Imbalance notification feature. With SNMP throttling, it is possible for some of the recovery traps to get throttled resulting in inappropriate health status of the ports in the GigaVUE-FM GUI. Use the GigaStream Imbalance Notification feature to generate traps and trigger appropriate alarms.

NOTE: GigaStream Unhealthy alarm is raised to signify the imbalance in traffic distribution (alarm description includes all the affected ports).

GigaStream Imbalance Threshold Priority Levels

Threshold values for GigaStream imbalance can be configured at the following levels:

Configuration Level	Description	Notes
Per GigaStream Level Configuration	Applies to a specific GigaStream in a device.	Has the highest priority and overrides the type level and global level configuration.
Type Level Configuration	Applies to all GigaStreams of a particular type.	Has the second highest priority and overrides the global level configuration .
Global Level Configuration	Applies to all GigaStreams.	Has the lowest priority.

The following table shows the various configurations that can be performed from the GUI:

Configuration Level	Details	Refer to
Per GigaStream Level Configuration	Allows you to configure GigaStream Imbalance notification for a specific GigaStream in a device.	Configure GigaStream Imbalance per GigaStream
Device Level Configuration	Allows you to configure GigaStream Imbalance notification for all the GigaStreams in a device.	Configure GigaStream Imbalance per GigaStream
GigaVUE-FM Level Configuration	Allows you to configure GigaStream Imbalance notification for all the GigaStreams in all devices managed by GigaVUE-FM.	Configure GigaStream Imbalance Threshold in GigaVUE-FM

NOTE: For configuration using CLI, refer to the GigaVUE-OS CLI Reference Guide.

You can configure threshold values for GigaStream imbalance for the following GigaStream types:

- All GigaStreams
- Tool GigaStream
- Circuit GigaStream
- Hybrid GigaStream
- Stack GigaStream

NOTE: GigaStream Imbalance threshold notification functionality is applicable only for regular GigaStreams. Controlled GigaStreams and weighed GigaStreams are not within the scope of this functionality as traffic distribution is uneven within the ports.

Example

Consider a GigaStream GS1 consisting of three member ports P1, P2, P3. Let the threshold variance be configured as **10%**. Refer to the following table for details on how the threshold limits are calculated, based on which traps are triggered.

Time	Port Utilization of Member Ports	Average Port Utilization	Allowed variance based on configured threshold value	Upper and lower limits	Is SNMP Trap Triggered?
T1	- P1 - 55 - P2 - 60 - P3 - 65	60	6	Upper limit: $60+6 = 66$ Lower limit: $60-6 = 54$ The port utilization in all the ports in the GigaStream is within the threshold limit.	No
T2 (T1+30 seconds)	- P1 - 10 - P2 - 20 - P3 - 30	20	2	Upper limit: $20+2 = 22$ Lower limit: $0-2 = 18$ The port utilization in port P2 is within the threshold limit, whereas port utilization in ports P1 and P3 is not within the threshold limit.	GigaStream Imbalance trap is triggered in the device and sent to GigaVUE-FM and the corresponding GigaStream Imbalance Threshold alarm is triggered.
T3 (T1+60)	- P1 - 19 - P2 - 20 - P3 - 21	20	2	Upper limit is $20+2 = 22$ Lower limit is $20-2 = 18$	Trap is cleared.

Time	Port Utilization of Member Ports	Average Port Utilization	Allowed variance based on configured threshold value	Upper and lower limits	Is SNMP Trap Triggered?
				The port utilization in all the ports in the GigaStream is within the threshold limit.	

Rules, Notes and Limitations

- If you configure the threshold value to '0', higher level threshold is applied to the GigaStream. For example, if you configure the threshold of a particular GigaStream to '0', it inherits its type-level threshold configuration. If type-level threshold is also configured as '0' then global-level threshold is applied to the GigaStream.
- If you configure the threshold value to -1, the feature is disabled on the given GigaStream. The GigaStream will no longer inherit its type-level/global-level threshold values and trap will also not be generated on account of variation in traffic distribution.
- You can configure email notifications for GigaStream Imbalance event occurrence. Refer to the Event Notification section for details.
- Supported polling interval is 30s only.

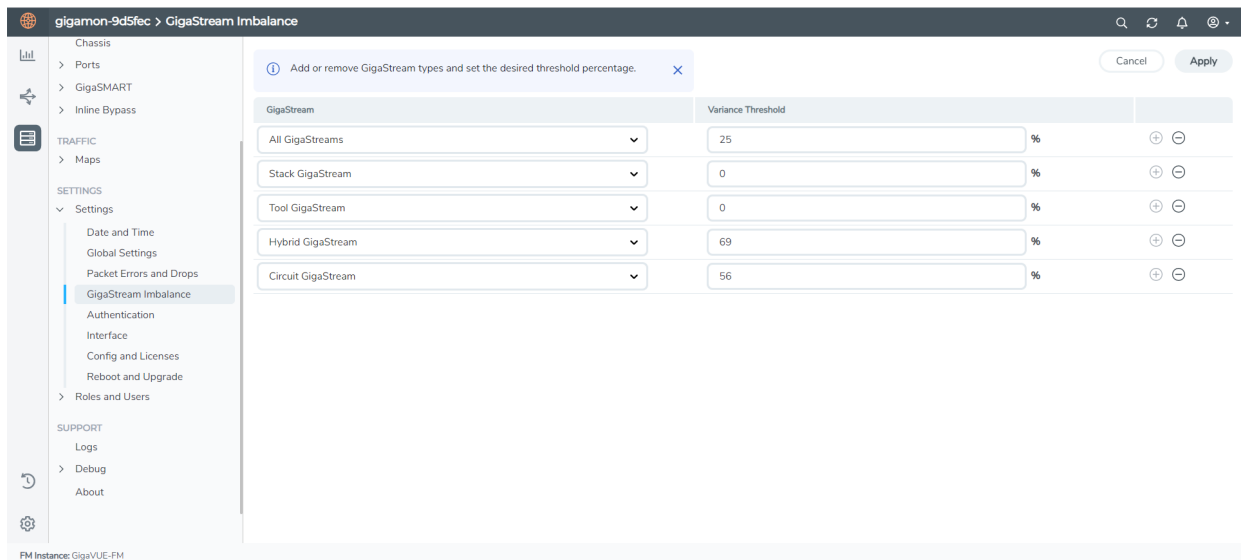
Configure GigaStream Imbalance Threshold in Devices

To configure GigaStream Imbalance threshold through the device settings page:

1. On the left navigation pane, go to **Inventory**  and under **Physical**, select the required device or cluster.
2. Click **Settings > GigaStream Imbalance**. The GigaStream page is displayed.

3. Select or enter the following values:

Field	Description
GigaStream	GigaStream type for which the threshold is to be configured. Configuration for <i>All GigaStreams</i> will be applied to all the GigaStreams (this is equivalent to the global level in device CLI). Use the +/- buttons to configure for the various GigaStream types.
Variance Threshold	Variance threshold value in %. If the threshold is above or below the Variance threshold and if the traffic distribution is not uniform across the ports in the GigaStream, traps will be sent from the devices to GigaVUE-FM.



4. Click **Save** and **Apply** to save and apply the configuration.

Configure GigaStream Imbalance per GigaStream

To configure GigaStream Imbalance for a specific GigaStream:

1. Select **Ports > Port Groups > GigaStream**. Select the GigaStream for which you want to configure the GigaStream Imbalance threshold.
2. Click **Edit** to open the port editor.

- Under **Variance Threshold**, configure the **GigaStream Imbalance Threshold** in %.

The screenshot shows the GigaStream configuration interface. On the left is a navigation menu with categories like SYSTEM, TRAFFIC, and SETTINGS. The 'Settings' option is selected. The main panel is titled 'GigaStream™' and contains fields for Alias, Description, Type, Controlled GigaStream, Ports, Weighting, Variance Threshold, and Tags. The 'Variance Threshold' field is highlighted with a red rectangle, showing a value of 25 and a percentage sign (%). The 'Type' field has four radio buttons: Tool GigaStream (selected), Hybrid GigaStream, Stack GigaStream, and Circuit GigaStream. The 'Ports' field shows two ports: 4/1/1/1 and 4/1/1/2. The 'Weighting' field is set to 'Equal'. The 'Tags' field has a 'TagKey' dropdown and a 'Values' input field with add and remove icons. At the bottom, it says 'FM Instance: GigaVUE-FM' and 'Node Sync Time: Jul 15, 2022 13:58:47'.

- Click **OK** to save the configuration.

The configuration is applied to that specific GigaStream.

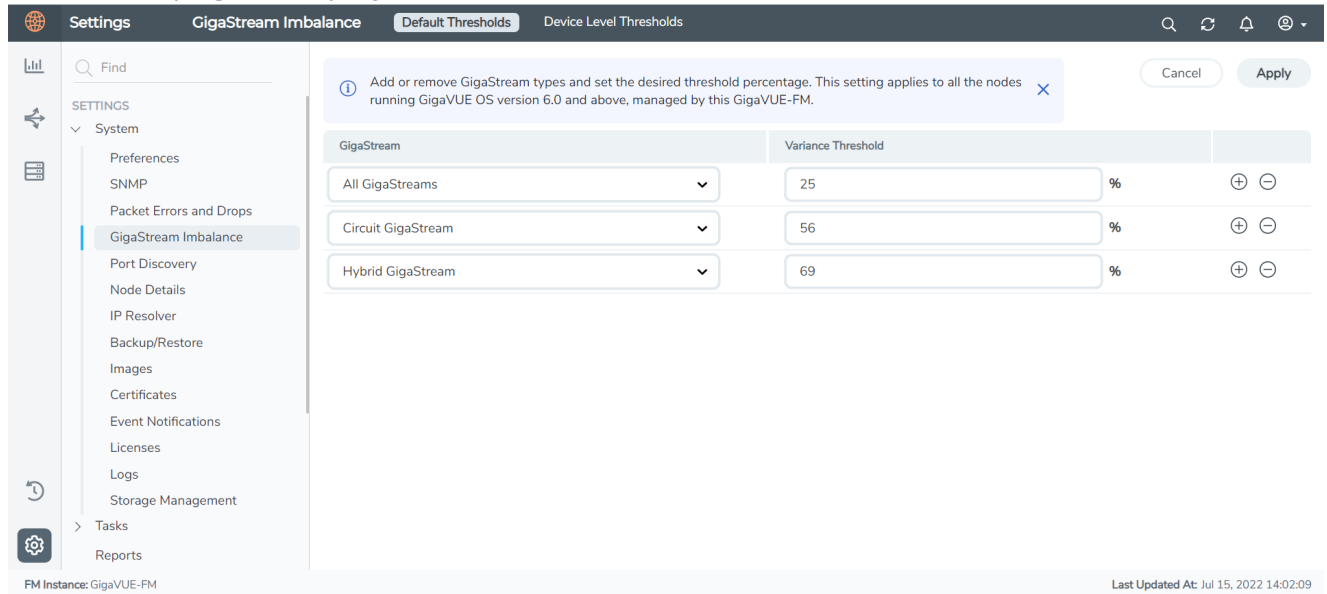
NOTE: To configure the threshold values globally for all the devices managed by GigaVUE-FM refer to [Configure GigaStream Imbalance Threshold in GigaVUE-FM](#).

Configure GigaStream Imbalance Threshold in GigaVUE-FM

You can configure the GigaStream Imbalance threshold globally for all the devices managed by GigaVUE-FM. To do this:

- On the left navigation bar, click .

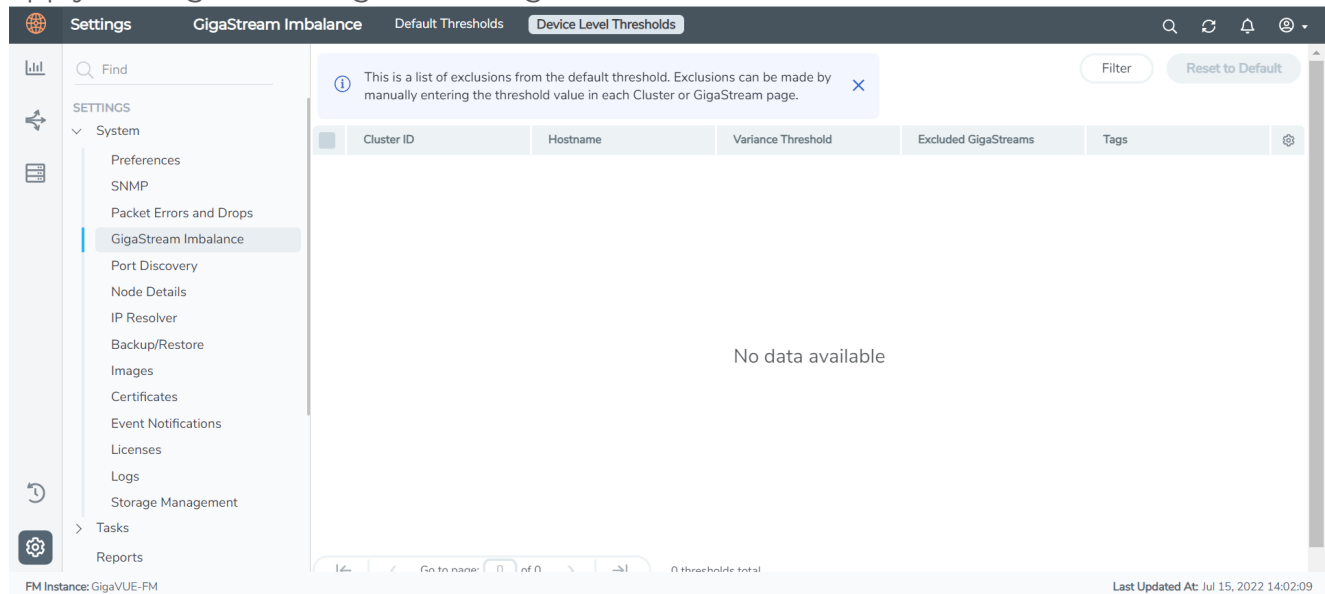
2. Select **System > GigaStream Imbalance > Default Thresholds**. The GigaStream Imbalance page is displayed:



Field	Description
GigaStream	GigaStream type for which the threshold is to be configured. Configuration for <i>All GigaStreams</i> will be applied to all the GigaStreams in all the devices managed by GigaVUE-FM. Use the +/- buttons to configure for the various GigaStream types.
Variance Threshold	Variance threshold value in %. If the threshold is above or below the Variance threshold and if the traffic distribution is not uniform across the ports in the GigaStream, traps will be sent from the devices to GigaVUE-FM.

If the device configuration is different from the global level configuration or the device has per GigaStream level configuration, then those devices will be listed in the Device Level Thresholds page. Configurations changes at the global level will not be applied to the devices in the Device Level Thresholds page.

Use the **Reset to Default** button to remove the current device-level configuration and to apply the GigaVUE-FM global configuration.



Port Discovery

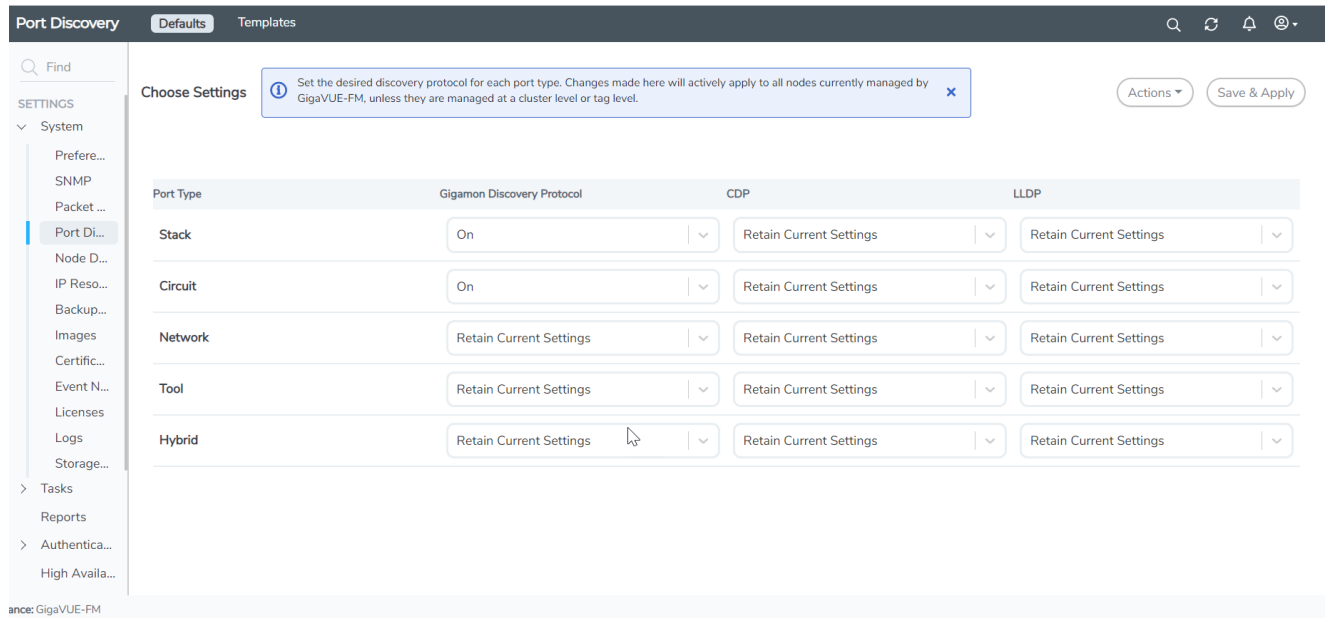
GigaVUE-FM allows you to configure the discovery protocols (CDP, LLDP and GDP) on each of the individual ports. However, in a scaled environment, where GigaVUE-FM manages a large number of devices, it is difficult and time-consuming to configure the protocols on each and every individual port. The Port Discovery page allows you to bulk configure the discovery protocols (GDP, CDP and LLDP) on the ports across the devices.

To access the Port Discovery page, on the left navigation pane, click  and select **System > Port Discovery**. The following pages appear:

- Defaults
- Template

Defaults

The Defaults page displays the discovery protocol configuration applied by default to the port in the devices managed by GigaVUE-FM. On upgrading GigaVUE-FM to software version 5.14.00 or later, the global configuration is applied on the clusters that are already upgraded to 5.14.00 or greater.



By default, GDP is enabled on the stack and circuit type ports. For the other port types, you can click the drop-down to either:

- Retain the current settings for the protocol configuration:
- Configure the required protocol configuration to 'On' or 'Off'.

Click **Save & Apply** to save the changes performed on this page. The changes will be applied to all the devices managed by GigaVUE-FM.

NOTE: The global template will not be applied on the clusters where the custom template is applied. At any point in time, a cluster can be associated with only one template.

Templates

The Templates page allows you to create custom templates from global configuration. You can perform the following tasks from this page:

- [Add New Template](#)
- [Edit Custom Template](#)
- Delete Custom Template: Select Actions and click Delete a Custom Template

Add New Template

To create a custom template:

1. Click **New** from the templates page. The New Port Neighbor Discovery Config page is displayed. Alternatively, you can also select the **New** option from the **Actions** drop-down.

2. Edit the required discovery protocol configurations for the required port types.
3. Under Apply Settings, you can either choose:
 - **Cluster:** Select the required cluster ids for which the configurations will be applied.
 - **Tags:** Select the required tag ids and tag values. The configurations will be applied for the ports that have the tag key and tag value configured.
4. Click **Save**. In the dialog box that appears, enter a name for the template and click **Save**.

The newly created template will be added to the list view.

You can also create template from the Defaults page.

1. Edit the configurations displayed in the Defaults page.
2. Click the **Actions** drop-down and select **Save as Template**.
3. In the dialog box that appears, enter a name for the template and click **Save**.

Edit Custom Template

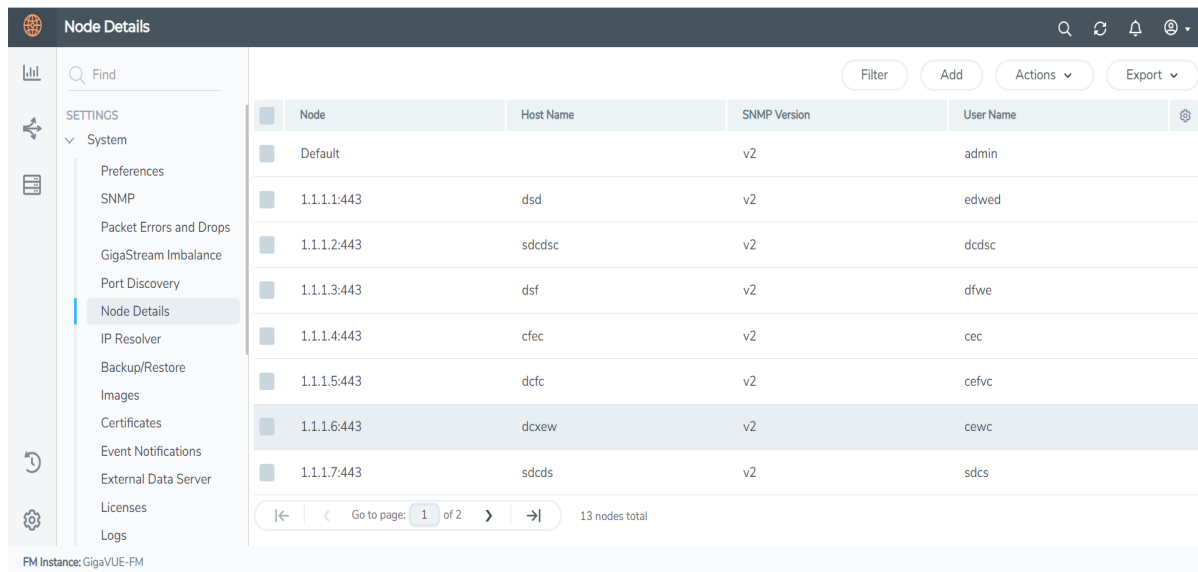
To edit a custom template:

1. Select the required custom template that you need to edit.
2. Click the **Actions** drop-down and select **Edit**.
3. Change the required configurations.
4. Click **Save**.

Node Details

The **Node Details** page includes the details of every node managed by GigaVUE-FM. The figure shows an example. For each node, you need to provide a user name and password that allow administrator privileges on the node.

To access the Node Details page, Go to **Settings** and select **System > Node Details**.



Node	Host Name	SNMP Version	User Name
Default		v2	admin
1.1.1.1:443	dsd	v2	edwed
1.1.1.2:443	sdcsc	v2	dcsc
1.1.1.3:443	dsf	v2	dfwe
1.1.1.4:443	cfec	v2	cec
1.1.1.5:443	dcfc	v2	cefc
1.1.1.6:443	dcxew	v2	cewc
1.1.1.7:443	sdcsc	v2	sdcsc

Go to page: 1 of 2 13 nodes total

Figure 16 Credentials for Physical Nodes.

The list of node credentials is maintained in a local database and is accessed whenever GigaVUE-FM needs to connect to a node. Also, GigaVUE-FM will use the credentials in this page to log into any node added with the **Add** button in the **Physical Node** page.

Using the “Default” Credentials Effectively

The **Node Details** page includes both a **Default** entry as well as entries for specific IP addresses. The **Default** credentials make it easier to add multiple GigaVUE nodes that use the same username/password quickly. Instead of adding node-specific credentials for each system, you can just set the **Default** credentials to match the username/password in use on multiple nodes, and then add all the IP addresses that use those credentials in the same **Add Node(s)** dialog box.

Node Details Fields and Page Controls

Node Details page has following buttons that allow you to manage the information that appears in the table:

Controls	Description
Add	Allows you to add a node and its login credentials. - Clicking Add opens a dialog where you specify the following details: - Node IP address and port number - Host Name - User name - Password and Confirm Password options - SNMP Version - Only one node can be added each time. - The user name and password you provide must have administrator privileges on the node.
Filter	Allows you to filter the nodes based on the required fields.
Actions	Allows you to perform the following operations: Edit: Allows you to change the credentials for a node. - Select a node. Click Actions > Edit to open a dialog where you make the changes. - Multiple IP addresses cannot be selected for editing. Delete Allows you to delete a node and its credentials. - A confirmation message pops-up prior to deleting a node. - Multiple IP addresses can be selected for deletion.
Export	Allows you to export the details of all the nodes or only the selected nodes either in CSV or XLSX format.

IP Resolver

GigaVUE-FM must be configured with DNS server and default search domains in order to add and manage the nodes by their Fully Qualified Domain Names (FQDN).

This configuration is not mandatory to manage normal nodes/clusters. However, to manage the clusters behind NAT, this configuration is required. This is because GigaVUE-FM does not know the NAT IP of the member nodes of the cluster behind NAT. It can only learn the private IP and hostname through the device APIs. GigaVUE-FM cannot reach the nodes behind NAT with their private address. GigaVUE-FM uses the hostname to contact the nodes in the cluster. Host names must therefore be resolved to NAT IP using the IP Resolver page, failure to do so will result in failure in node specific operations.

You can configure the domain name server and search domains from the IP Resolver page.

Refer to the following sections for details.

NOTE: IP Resolver configuration is not applicable for GigaVUE-FM deployed on cloud platforms.

DNS Servers

To configure the DNS servers for the interfaces:

1. Go to **Settings** and select **System > IP Resolver**. The DNS Servers page appears.
2. Enter the following details, as required.

Field	Description
Interface Name	Interface name for which DNS is to be configured. All the associated interfaces will be listed.
DNS Server	IP address of the domain name server. Use the +/- icon to add the additional servers. GigaVUE-FM allows you to configure only three name servers. The + option is disabled once you have configured three name servers. NOTE: If GigaVUE-FM is configured with DHCP and three or more nameservers are assigned from DHCP itself, then the Add Server option is disabled in the UI.

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

Default Search Domain

To configure the default search domain:

1. Go to **Settings** and select **System > IP Resolver > Default Search Domain**. The Default Search Domain page appears.

Field	Description
Default Search Domain	Default search domain. You can configure only a maximum of 6 search domains from the GigaVUE-FM GUI.

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

Traffic Drop Identification

GigaVUE-FM periodically collects statistical data of the physical and logical resources from the devices. The Traffic Drop Identification feature utilizes the historical statistical data to identify any significant traffic drop in the components. For software version 6.1.00, the traffic drop at the decapsulation side of the tunnel can be identified.

To enable this feature, you must define Alert Policies based on which alarms get triggered if there is a significant throughput change in traffic volume. An alert policy binds the resources such as a tunnel and the required conditions to identify the drop in traffic volume. Refer to the [How Alert Policies Work](#) for details.

How Alert Policies Work

An alert policy consists of the following sections:

- **Overview:** Name and description of the alert policy.
- **Monitoring Resources:** Resource such as Tunnels (for software version 6.1.00).
- **Threshold Conditions:** Criteria for detecting the traffic drop.
- **Clear Condition:** Conditions based on which alarms will be cleared.

The Alert Policies work based on the threshold conditions that define the criteria for creating the alarm. It consists of the time duration to average the metrics, drop threshold percentage, and severity of the alarm.

When the computed traffic drop value exceeds the configured threshold value, an alarm is triggered with the configured severity. Alarm gets cleared based on the clear condition defined.

Alert policy supports both single threshold and multiple thresholds configuration. In multiple threshold configuration, up to three levels of drop thresholds and associated severity can be configured. Consider an alert policy that is configured with multiple threshold values such as:

- Minor - 2%
- Major - 5%
- Critical - 8%

GigaVUE-FM calculates the threshold value at periodic intervals:

Intervals	Calculated Drop %	Alarms Severity
1	Computed drop is 4% Exceeds the 2% configured value for severity state Minor and is lower than the 5% configured value for severity state Major	An alarm with severity 'Minor' is triggered.
2	Drop further increases to 7% exceeds the 5% configured value for severity state Major and is lower than 8% configured for severity state Critical	Alarm is updated with severity as 'Major'
3	Drop goes beyond 8%.	Alarm is updated with severity as 'Critical'
4	Drop is identified as 4%	Alarm severity will not be lowered. Instead alarm will be cleared based on the clear criteria.

Alarms get cleared based on the clear condition. The following options are provided:

- **Time based:** Alarms will be cleared after the configured time (10-30 minutes interval)
- **Threshold based:** Alarms will be cleared based on the following criteria:
 - **Threshold value:** Denotes the threshold value to clear the alarm when the computed traffic drop value goes below this configured value
 - **Duration:** Duration for how long the computed traffic drop should be maintained below the threshold value (10-30 minutes duration).

Therefore, the alarms do not get cleared immediately after the drop goes below the threshold value. It is ensured that the drop is consistently maintained below the threshold value for the given duration. Refer to the [Configure Alert Policy](#) section for the various fields required for creating the policy.

Tunnel Traffic Drop Identification

For tunnels, traffic drop is calculated based on the traffic sent over the tunnel versus the traffic received at the decapsulation side of the tunnel. That is, the average processed traffic is computed for configured duration for both encapsulation and decapsulation

sides separately and the drop is computed using these two values.

GigaVUE-FM supports configuring various tunnel types and each tunnel type has its own source and destination components. The following table lists the components considered for computing the total traffic for the different tunnel types:

Tunnel Type	Encapsulation side Component	Decapsulation Side Component
GigaSMART L2GRE	GSOP General Stats Rx Packets	GSOP General Stats Tx Packets
Embedded L2GRE	Encap Map Source Ports Rx Packets	Decap Map Rule Stats (Rules with L2GRE ID)
Embedded VxLAN	Encap Map Source Ports Rx Packets	Decap Map Rule Stats (Rules with VxLAN ID)
Circuit Tunnel	Encap Map Packets	Decap Map Rule Stats (Rules with Circuit ID)
Hybrid Tunnel (configured between GigaVUE V Series Nodes and physical nodes)	Egress TEP Tx Packets	Ingress TEP Rx Packets

NOTE: The source and destination of the tunnels may reside in different clusters. As stats collection for the clusters happen at different time intervals, the encapsulation and decapsulation statistics may not always match exactly. Consider this while configuring the tunnel drop threshold in an Alert Policy for the tunnels.

Rules, Notes, and Limitations

Refer to the following rules, notes and limitation for traffic drop identification for the tunnels:

- For software version 6.1.00, traffic drop alert policies can be created only for tunnels discovered by GigaVUE-FM. Refer to [Tunnel Monitoring](#) section for details.
- For the tunnels discovered and listed in the Tunnel Monitoring page, Alert Policies can be configured only if the Tunnel Discovery State is 'Complete'.
- For Alert Policies with multiple alarms, severity can be configured only up to three levels.
- Traffic drop computation is not performed in the following scenarios:
 - when any one or both of the participating nodes are unreachable.
 - when the number of statistical points at the encapsulation and decapsulation side are not equal.

- Traffic drop identification will not work for tunnels with multiple sources and single destination with decap key 0. If monitoring is required for such tunnels, it is recommended to configure a higher drop threshold value. Alarms generated for these types of tunnels can be used as a starting point for troubleshooting exact problem.
- Traffic drop identification will not work if the traffic at the decapsulation side of the tunnel is very high than at the encapsulation side (that occurs due to any misconfiguration or any other symptoms).
- **For embedded tunnels:** Source post statistics is considered for computing the drop threshold value. Therefore, if an alert policy is configured for these tunnels and there is a packet drop on the encapsulation map and the packet drop value is exceeding the drop threshold, an alarm will be triggered.
- Alert Policies are updated based on the state change of the tunnels:
 - Consider an Alert Policy created for a tunnel. During the next config sync cycle, if the state of tunnel changes to incomplete, then traffic drop computation is suspended for the tunnel. Traffic drop computation resumes once the state changes to complete.
 - Consider an Alert Policy with only one tunnel. If the tunnel is deleted then the Alert Policy also gets deleted. Deletion of Alert Policies is captured in the Events page.
 - Consider an Alert Policy with more than one tunnel. If one of the tunnels is deleted, then the deleted tunnel is also removed from the policy. Update to the Alert Policies is captured in the Events page.
- If monitoring is disabled for a tunnel (in the Tunnels Monitoring page) and if there is an Alert Policy configured for the tunnel, the traffic drop computation is suspended. Traffic drop computation resumes once monitoring is enabled for the tunnel.

Configure Alert Policy

To configure Alert Policies:

1. Go to **Settings** and select **System> Traffic Drop Identification**. The Traffic Drop Identification page appears.
2. Click **New Policy**.

The screenshot displays the 'Traffic Drop Identification' interface. On the left, a sidebar menu under 'SETTINGS' shows 'System' expanded, with 'Traffic Drop Ide...' highlighted. The main area features a table with the following data:

Policy Name	Description	Status	Resources	Metric	Alert Condition
p1	—	Active		TUNNEL_TRAFFI...	Single Threshold
policy1	—	Active	CIRCUIT:2301:FM-TLG-4ed56021-ba54-4124-af0c-041c...	TUNNEL_TRAFFI...	Single Threshold

At the bottom, a pagination bar shows 'Go to page: 1 of 1' and '2 policies total'. The footer includes 'FM Instance: GigaVUE-FM' and 'Last Updated At: Oct 8, 2022 00:04:11'.

3. Select or enter the following details:

Field	Description
Policy Name	Name of the policy
Description	Detailed description about the policy
Monitoring Resources	
- Metric	Metric for the various resource types. For software version 6.1.00, Tunnel Traffic Monitoring is the only metric supported.
- Resources	List of tunnels identified in the Tunnel Monitoring page.
Conditions	
- Alert Condition	Alert condition. You can configure this as Single Threshold or Multiple Thresholds.
- Average Duration	Period during which the metric is to be monitored.
- Threshold	Threshold value in %. If you select Alert Condition as Multiple, you can configure up to three threshold values with varying severity levels.
Clear Alarm Condition	
Clear Type	You can clear the alerts based on: • Time • Threshold
Clear Alarm After	If Clear Type is selected as Time , configure the Duration after which the alarm should be cleared.
Clear alarm when traffic drop is maintained below	If Clear Type is selected as Threshold , configure the threshold percentage for the required minutes.

4. Click **Apply** to apply the Alert Policy.

5. The policy is added to the list view. The Alarm column lists the alarm count for each policy. Click on the alarms and you will be redirected to the Alarms page.

Once the Alert Policy is created with the required details, the policy is scheduled and runs periodically every 5 minutes to compute the traffic drop based on the conditions. If the traffic drop exceeds the configured threshold values for the specified duration, alarms are triggered.

Use the following buttons to manage the Alert Policies:

Button	Description
New Policy	Use to create a new Alert Policy
Actions	Use the Actions drop-down button to perform the following tasks. You can select either a single policy or multiple policy, as required. • Edit - Use to edit the policy details.

Button	Description
	- Delete - Use to delete the policy details - Activate - Use to enable the policy. - Deactivate - Use to disable the policy
Filter	Use to filter the Alert Policies based on the policy name or the status of the Policy.
Export	Use to export the Alert Policies (either all or the selected Alert Policies) in CSV or XLSX format.

Backup/Restore

The Backup/Restore page allows you to backup and restore the configuration data for GigaVUE-FM, Physical Nodes, and add Archive Servers used for back up.

NOTE: GigaVUE-FM allows you to restore the backup files of the earlier two software versions. For example, if your GigaVUE-FM is running software version 6.2.00, you can back up and restore the following software versions: 6.1.00 and 6.0.00.

GigaVUE-FM Appliance Backup and Restore

GigaVUE-FM includes a backup-and-restore feature for saving configuration data. You can use the saved data to restore an instance of GigaVUE-FM or provide a copy of the configuration data and have it available for a new instance of GigaVUE-FM. This is useful for restoring the configuration on an appliance or when migrating to a GigaVUE-FM hardware appliance.

You can schedule GigaVUE-FM for an immediate backup or schedule a backup to occur once at a specified time or on a reoccurring basis. For example, you can schedule a backup for a particular day, week, month, or date at regular intervals.

NOTE: GigaVUE-FM backup and restore is not supported for cloud solutions.

Rules and Notes

GigaVUE-FM Backup

- Backup is only supported for users with super admin privileges.
- When you backup GigaVUE-FM, it will be in maintenance mode, and you cannot perform any operations such as create, update and delete. You can only view the data in GigaVUE-FM.
- If you perform a GigaVUE-FM backup in parallel with another backup that is already in progress, you will be notified about the status and instructed to perform the second backup at a later time.
- After the backup operation is completed an event is received in the Events page.

- When creating a backup file, do not include the following special characters: **space * " ? ; : , / % @** in the alias.
- Backup of GigaVUE-FM is only supported from GigaVUE-FM version 5.13.00.

GigaVUE-FM Restore Process

- Restore of GigaVUE-FM is only supported for users with super admin privileges.
- During the restoration process, the database is restored from the backup while retaining the previously active GigaVUE-FM licenses.
- If you destroy the existing GigaVUE-FM and deploy a new one with the same MAC address, the backup will be restored and the same GigaVUE-FM license will be reinstalled on the destroyed unit.
- Restore operation will only add the licenses for that GigaVUE-FM instance. Ensure to have the licenses for the nodes and other GigaVUE-FM instances (in case of High Availability) before the restore operation. Add the licenses after the restore operation is completed.
- After restore, you must reconfigure the RADIUS and TACACS+ passwords.
- Restore of GigaVUE-FM is only supported from GigaVUE-FM version 5.13.00.
- GigaVUE-FM logs out all active sessions after a restore.

Recovery Process

- If the GVOS backup in GigaVUE-FM has not changed, it can be restored to bring both GigaVUE-FM and GigaVUE-OS back into parity.
- If the GigaVUE-OS backup has changed, delete and recreate the solution in GigaVUE-FM.
- To avoid issues, it is recommended to have daily or scheduled periodic backups of both GVOS and FM.

Data Saved When Backing Up GigaVUE-FM

When you back up GigaVUE-FM, the following information is saved:

- List of standalone nodes and clusters that are directly under the management of the GigaVUE-FM.
- User credentials needed to access the nodes
- Node level user account and RBAC configurations
- vMaps
- GigaVUE-FM credentials and preferences
- GigaVUE-FM database dump
- GigaVUE-OS backups maintained by GigaVUE-FM
- Certificates of Fabrics (GVOS, GigaVUE V Series Node, Controller)
- FHA Settings

- Solution configuration data
- Solution level metadata
- Intent collections
- Other information, such as node level Radius, TACACS, SSH servers and SNMP or email notification configurations

The backup does not include the following data:

- GigaVUE-FM appliance host/IP configuration
- System configuration of GigaVUE-FM. For example, DHCP, NTP, DNS configurations, FMHA Tunnel Operation mode, etc.,

These are configured through the [fmctl](#) configuration when configuring a new GigaVUE-FM.

Backup Immediately

To do an immediate back up of a GigaVUE-FM, do the following:

1. On the right side of the top navigation bar, click .
2. On the left navigation pane, select **System > Backup/Restore > GigaVUE FM Appliance**.
3. Click **Backup**.
4. Select **Immediate**.
5. Select the archive server for the backup file. Refer to [Figure 17 Immediate Backup to an Archive Server](#).

To add an archive server, refer to [Add an Archive Server](#).

6. Click **OK**.

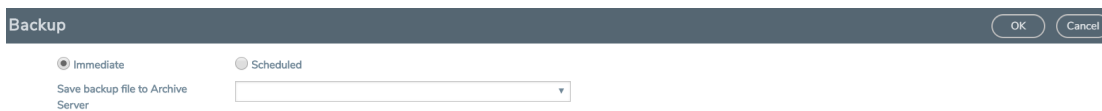


Figure 17 Immediate Backup to an Archive Server

Schedule Backups

To create a schedule for backing up GigaVUE-FM, do the following:

1. On the right side of the top navigation bar, click .
2. On the left navigation pane, select **System > Backup/Restore > GigaVUE FM Appliance**.
 - a. Click **Backup**.

b. Select **Scheduled**.

The GigaVUE-FM time clock is based on ESX host time. Make sure that you have synchronized clock before any scheduling operation.

- To repeat backups, use **Recurrences**, **Start Date**, and **Start Time** to set how often the backup occurs, at what time, and when the backup schedule will end.

If you want to schedule a single backup for a specific data and time, select Once Only for **Recurrence**.

Figure 18 Scheduled Backup for GigaVUE-FM shows an example scheduled backup. In this example, the weekly backup to archive server Archive Server 1 starts on March 17 and occurs every Saturday at 9:00 pm until March 31.

The screenshot shows a 'Backup' dialog box with the following settings:

- Backup Type:** Scheduled (selected over Immediate)
- Recurrence:** Once Only (selected from a dropdown)
- Start Date:** March 17, 2017 (selected from a calendar icon)
- Start Time:** 12:00 PM (selected from time dropdowns)
- Save backup file to Archive Server:** Archive Server 1 (selected from a dropdown)

Figure 18 Scheduled Backup for GigaVUE-FM

- Click **OK**. To monitor the progress of the event, select All Alarms/Events in the left navigation pane.

Once you have scheduled a recurring backup, the scheduled backup appears as a scheduled task on the Scheduled Tasks page. To view tasks, select **Tasks > Scheduled Tasks**. After the backup has completed the outcome of the task is displayed on the Alarm/Events page.

Restore GigaVUE-FM Configuration Files

To restore a GigaVUE-FM configuration from a backup file, do the following:

- On the right side of the top navigation bar, click .
- On the left navigation pane, select **System > Backup/Restore > GigaVUE-FM Appliance**.
- Click **Restore**.
The Restore page displays, showing the file names from which to restore.
- Select the Archive Server from which to retrieve the backup file.
- Select the configuration to restore by clicking the check box next to the file name. Only one configuration can be selected with an restore action.
- Click **OK**.

NOTE: GigaVUE-FM will reboot once after successful restore operation. Logs will be recorded in the Audit Logs page with Restore Complete/Success Message.

After successful restoration, the configuration available in the backup file will be persisted. Restore Success Event is recorded in the Events page. If Restore Failure Event appears after GigaVUE-FM restore operation, then the configuration that existed before the restore operation will remain.

Archive Servers

The Archive Servers page displays the archive servers currently available for backing up GigaVUE-FM. The page displays the following information:

- The alias to help identify the server
- The IP address of the server
- The type of server, either SCP or SFTP
- The username for logging in to the server
- The path on the server to the backup files

NOTE: GigaVUE-FM does not support Windows as an archive server.

For information on archive server requirements for Linux machine, refer to [Archive Server Requirements for Linux machine](#)

Add an Archive Server

The Backup/Restore feature of GigaVUE-FM requires an archive server for saving and restoring the configuration files. To add an archiver server to GigaVUE-FM, do the following:

1. On the right side of the top navigation bar, click .
2. On the left navigation pane, select **System > Backup/Restore > Archive Servers**.
3. Click **Add**.
4. Enter the following information about the server:
 - Alias—An name to help identify the archive server.
 - Server Address—The IP address of the server.
 - Type—The type of archive server. The only type available is SCP.
 - File Path—The path to the backup files on the server
 - Username—The login user name for the server.
 - Password—The login password for the server.
5. Click **Save**.

Edit an Archive Server

To make changes to an archive server, do the following:

1. On the right side of the top navigation bar, click .
2. On the left navigation pane, select **System > Backup/Restore > Archive Servers**.
3. Click **Edit**.
4. On the Edit Archive Servers page, make changes to the server information.
5. Click **Save**.

Delete an Archive Server

To delete an archive serve, do the following:

1. On the right side of the top navigation bar, click .
2. On the left navigation pane, select **System > Backup/Restore > Archive Servers**.
3. On the Archive Servers page, select the server to delete.
4. Click **Delete**.

Archive Server Requirements for Linux machine

You can use the archive server as a Linux machine. To use an archive server as Linux machine, you must meet the following requirements:

- The GigaVUE-FM user must have an account to copy the backup to the archive server (Linux machine). You can create a new user account or use an existing one.
- The user must create a directory in the archive server to save the backup.
- The user must have the read-write privilege to access the backup directory.
- The user must provide necessary port access between the GigaVUE-FM and the Linux server.

You must meet the following requirements in the GigaVUE-FM:

- Configure the archive server with the Linux server IP, location, and user credentials.
- The location provided in the configuration must match the directory created in Linux.
- The user credentials provided in the configuration must exist on the Linux server and must have read-write access to the backup directory.

Physical Nodes

The **Physical Nodes** page lists the backup files currently saved in local storage on the machine where GigaVUE-FM is installed. You can also change the Do not Purge setting for the file and down load the files.

NOTE: You can backup multiple configuration files. The default is 10 per cluster. This file will be kept during automatic purge.

Backup/Restore

GigaVUE-FM Appliance

Physical Nodes

Archive Servers

Total Backup Files: 6 | Filtered By : none

Actions

Edit

Delete

Filter

Expand All Collapse All

☐	Clus...	File Name	B...	Comments	Date	SW Version	Do no...	Config Snapshot	Device Summary	Restore Repor...	
☐	▼ 1...										
☐			T...	Device back...	2019-...	5.8.00_Beta	Disabl...	Show_Config	Summary	Restore Log Files	
☐			T...		2019-...	5.8.00	Disabl...	Show_Config	Summary	Restore Log Files	
☐	▼ 1...										
☐			i...	Device back...	2019-...	5.7.01	Disabl...	Show_Config	Summary	Restore Log Files	
☐			i...	Device back...	2019-...	5.8.00	Disabl...	Show_Config	Summary	Restore Log Files	
☐	▼ 1...										
☐			u...	Device back...	2019-...	5.8.00_Beta	Disabl...	Show_Config	Summary	Restore Log Files	
☐			2...	Device back...	2019-...	5.8.00_Beta	Disabl...	Show_Config	Summary	Restore Log Files	

<

<

Go to page: 1

of 1

>

>

Total Records: 9

Figure 19 Backup Files Page

Enable Do Not Purge

To set Do Not Purge for a backup file, do the following:

1. On the right side of the top navigation bar, click .
2. On the left navigation pane, select **System > Backup/Restore > Physical Nodes**.
3. On the **Backup Files** page, select the backup file or files.
4. Click **Actions**, and then select **Enable Do Not Purge**.

The Do Not Purge column will display a check mark for each backup file that has Do Not Purge enabled.

Disable Do Not Purge

To disable Do Not Purge for a backup file, do the following:

1. On the right side of the top navigation bar, click .
2. On the left navigation pane, select **System > Backup/Restore > Physical Nodes**.
3. On the **Backup Files** page, select the backup file or files.
4. Click **Actions**, and then select **Disable Do Not Purge**.

Download Backup Files.

You can also download the backup files by doing the following:

1. On the right side of the top navigation bar, click .
2. On the left navigation pane, select **System > Backup/Restore > Physical Nodes**.
3. On the **Backup Files** page, click **Show_Config** for the file to download the backup.
4. Click **Download**.
5. GigaVUE-FM downloads the file. The filename includes the node's IP address and a timestamp.

Device Configuration Backup

GigaVUE-FM retrieves and stores the device configuration in binary and text formats. GigaVUE-FM restores the device configurations in binary format and allows you to view the configurations in text format. The advantage of the binary format is that it backs up all state parameters, including system parameters.

Version Compatibility

- For GigaVUE devices 5.1 version onwards, GigaVUE-FM will take a binary backup of those devices. For devices prior to version 5.1, GigaVUE-FM will continue to take text-based backups.
- For backups taken in text format in GigaVUE-FM v5.4.01 or above, GigaVUE-FM will allow those configurations to be restored.
- Before GigaVUE-FM v5.500, the configuration backup was text based, which was intended to backup only traffic related configs.

Points to Remember

- **Describe your backup:** Provide a meaningful name and comments while taking the backup, to help track the configuration while restoring.
- **View your backup:** You can view and download the text format of binary contents for readability. Some details in the binary content might not appear in text format.
- **View the restore report:** After performing a restore operation, a restore report displays the results of the restore operation such as the success or failure as well as all the logs from the leader device.

Restore Configuration (RMA'ed device)

The following are the steps to be performed for Standalone and Cluster Nodes:

Standalone Devices (RMA):

1. Make a backup on Device A, which will contain Device A details (Serial Number, chassis ID, GUID, etc.)
2. Device A has now failed.
3. Order and get a new device, Device B (identical hardware inventory, except all the hardware serial numbers are different).
4. Power up Device B and assign it a hostname and IP address.
5. The hostname should be the same as the previous device.
6. The IP address should be the same. (Different IP addresses are supported, but not recommended.)
7. On GigaVUE-FM, restore the backup of Device A onto this device:
 - a. If the IP address is the same, then it will get discovered as Device A.
 - b. If the IP address is not the same, restore the Device A data onto the Device B (IP address, etc.)
 - c. Now the backup taken on device A is pushed to device B.
 - d. When the backup is complete, GigaVUE-FM invokes a new “Migration” API from the node.
 - e. When the process is complete, Device B is restored to Device A’s configuration.

A node of the cluster (RMA):

1. The binary backup of the cluster is available in GigaVUE-FM.
2. Node A fails.
3. Replace with node B.
4. Configure the node B with the IP address, hostname, cluster ID, cluster VIP etc.
5. Node B joins into the cluster.
6. Cluster leader will push the config to the new node, which will not apply to its hardware since its serial number does not match.
7. GigaVUE-FM will now discover node B back in the inventory.
8. Instruct GigaVUE-FM to migrate the configuration of node B, from the old serial number to the new one.
9. This will be sent to the Leader of the cluster (and new API that will be provided same as 7 above).
10. Cluster leader will do the migration and push the configuration to the new node

**Notes:**

- GigaVUE-FM handles the UUID stored in GigaVUE-FM.
- GigaVUE-FM has a dependency on the device API to migrate configuration of RMA box to a new serial number.

Restore Devices and GigaVUE-FM for Traffic Management Solutions

This section provides instructions to restore devices and GigaVUE-FM for the traffic management solutions, such as Application Intelligence, Flexible Inline Flows, and Fabric Maps.

Before you restore devices and GigaVUE-FM, keep in mind the following:

- Ensure that you backup the devices and GigaVUE-FM at the same time.
- Perform the restore operation during a maintenance window.
- Do not restore devices that are in operation. It will affect the packet flow.

To restore devices and GigaVUE-FM:

1. Restore the devices. You can choose to restore devices in any order. Refer to [Restore Nodes and Clusters](#).
2. Verify that the restore operation on the devices are completed successfully. Refer to [View Restore Logs](#).
3. Restore GigaVUE-FM from the required archive server. Refer to [Restore GigaVUE-FM Configuration Files](#).
4. Verify that the GigaVUE-FM is restored successfully.
 - a. On the right side of the top navigation bar, click .
 - b. On the left navigation pane, select **Events**.

NOTE: You can either wait for the devices to synchronize completely or re-discover the devices in GigaVUE-FM.

5. If the GVOS backup in GigaVUE-FM has not changed, it can be restored to bring both GigaVUE-FM and GigaVUE-OS back into parity. If the GigaVUE-OS backup has changed, delete and recreate the solution in GigaVUE-FM. For more information to recreate the solutions, refer to:
 - [Application Intelligence Solutions](#)
 - [Fabric Maps](#)
 - [Flexible Inline Arrangements](#)
 - [Traffic Policy](#)

Images

The Images page is used to specify the servers where you will store image files for upgrading your nodes. You obtain images for your nodes by contacting Technical Support. Once you have the images, you can use an external server or use GigaVUE-FM as the image server.

Go to **Settings** to access Images and select **System > Images**.

Internal Image Files

If you use GigaVUE-FM for the image files, the files used to upgrade the physical nodes to the latest software version are stored on your local system and uploaded to GigaVUE-FM from the Upload Internal Image Files page. To access this page, go to **System > Images > Internal Image Files**.

After obtaining the image files, copy them to your local system. Use the **Browse** button to upload the files. The figure shows an image file for a Gigamon-HC3 node selected for uploading. To upload the file, click **OK**.

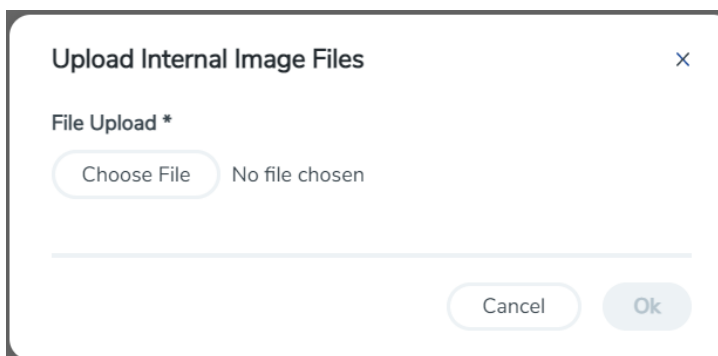


Figure 20 Image File Uploaded

After the uploading has completed, the image file is shown on the Internal Image Files page. Use the **Download** button to download images stored on GigaVUE-FM to your local system. Use the **Delete** button to remove image files.

In case of GigaVUE-FM High Availability group, always use GigaVUE-FM GUI (API) to upload the image files. Use GigaVUE-FM CLI only as a fallback mechanism and upload the image files only from the GigaVUE-FM instance with Active status.

External Servers

The External Servers page allows you to add the external servers that stores the image files used for upgrading the physical nodes or GigaVUE-FM to the latest software version.

To access the External Servers page, go to **System > Images > External Servers**. The External Servers page has buttons to set up and manage external image servers. These buttons are described in [Table 2: Controls on External Servers Page](#). For information on how to upgrade from an external server, refer to the *Upgrading from an External Image Server* section in the *GigaVUE Fabric Management Guide*.

Table 2: Controls on External Servers Page

Add	Allows you to specify where image files will be stored. Clicking Add opens the Image Server Details dialog, where you specify: • Alias — A name to identify the server. • Server IP/Host Name — The IP address of the server or the host name. • Type — Images can be updated using SCP. • Username and Password — The user name and password that will be used to log into the server to store the image file. NOTE: Starting from software version 6.1.00, you cannot add a TFTP server. If TFTP servers were added in previous software versions, then after upgrading to software version 6.1.00, the added TFTP servers will not be available.
Actions	Allows you to perform the following operations: • Select a server and click Actions > Edit to open the Image Server Details dialog, where you can modify the values specified for the server. Same options are to be filled as noted for Add. • Select a server and click Actions > Delete to delete the server specified. The Delete Option will have a validation option to select as a pop-up prior to deleting a node.
Export	Allows you to export the details of all the nodes or only the selected nodes either in CSV or XLSX format.

Certificates

The Certificates Page provides access to the following pages:

- [Updating Trust Store](#)
- [Certificate Issuance](#)
- [Certificate Issuance](#)
- [Notes](#)
- [CA List](#)

The Automated Certification Management Environment protocol is used for automatic certification of devices and GigaVUE-FM. Refer to the following sections for details.

Automated Certification Management Environment (ACME Configuration)

To enable secure and confidential communication between GigaVUE-FM, GigaVUE-OS devices and other network entities, it is important to deploy, manage and update the required certificates. By default, GigaVUE-FM and the GigaVUE-OS devices come up with self-signed certificates. However, you can also deploy custom certificates signed by the Certificate Authorities (CA). This requires you to manually install the certificates and map the certificates to the web.

Starting in software version 5.13.01, GigaVUE-FM and the devices support Automated Certificate Management Environment (ACME) protocol that allows automatic certificate signing and deployment between Certificate Authorities (CAs) and GigaVUE-FM, GigaVUE-OS devices web servers. If your devices and GigaVUE-FM instances are running software version 5.13.00 or lower, ensure to add all the devices to GigaVUE-FM, upgrade the devices and GigaVUE-FM to software version 5.13.01 for the ACME protocol to be functional.

How ACME Works

The ACME protocol is based on the principle of client-server communication:

- **ACME Server:** Runs at a Certificate Authority, for example, Step-ca . The ACME server responds to the client requests and executes the requested actions (issue, renew, revoke) once the client is authorized.
- **ACME Client:** Runs on the user's server or device that needs to be protected by the PKI certificate. The ACME client uses the ACME protocol to request the ACME server running in CA to perform the certificate management tasks such as issue, renew, revoke of certificates.

An ACME server and a client must be appropriately configured. The client sends requests to the server and the server receives the requests and issues certificates for the client. The ACME server and the client communicate over a secure HTTPS connection using JSON messages.

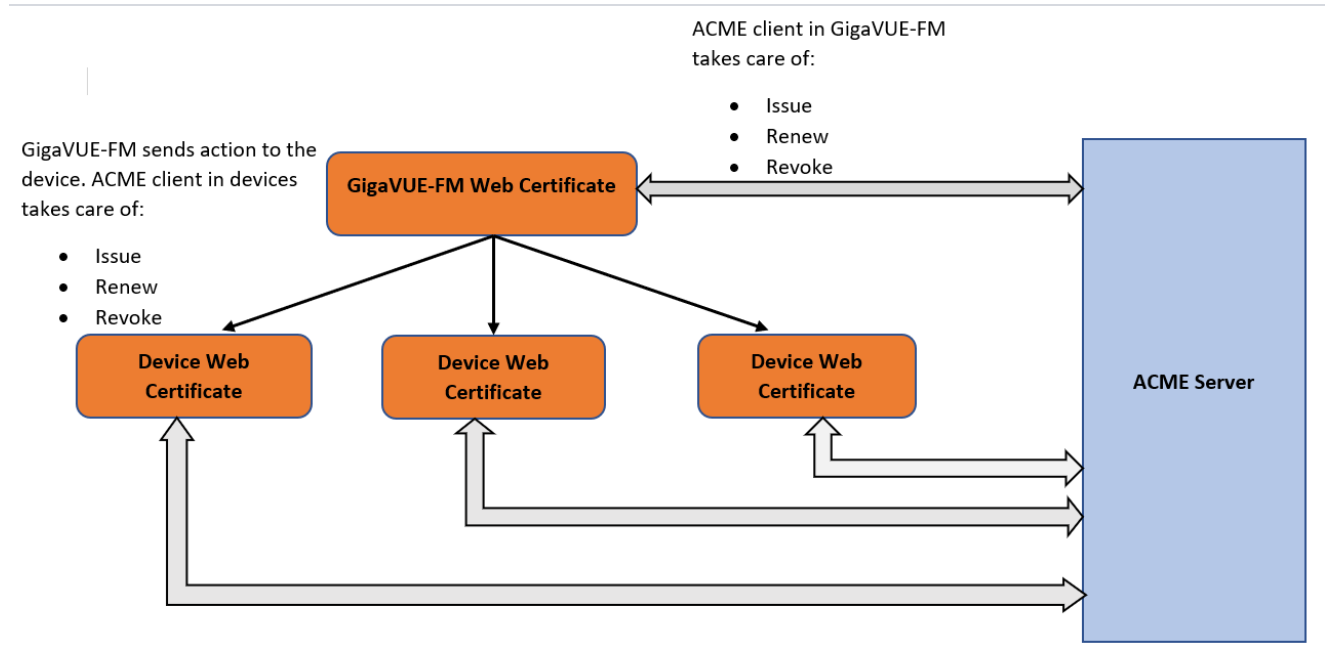
NOTE: For more details about the Automatic Certificate Management Environment protocol, refer to RFC 8555.

ACME Configuration in GigaVUE-FM and the Devices

ACME client is configured in both **GigaVUE-FM** and the GigaVUE-OS devices, and takes care of the following operations by contacting the ACME server that runs in a Certificate Authority:

- Issue of Certificates
- Renewal of Certificates
- Certificate Revocation

The following diagram shows how ACME works in GigaVUE-FM and the devices:



Refer to the following table for a summary of the ACME process in devices and GigaVUE-FM:

Task	In Device	In GigaVUE-FM
Certificate Issuance and Renewal	The ACME Client is installed in the devices and takes care of automatic issue/renew/revoke of the HTTPS certification of the devices. Issuance: After the certificate is downloaded, the device will automatically update the ACME issued certificate for web operation. Renewal: • Both manual and automatic renewals are supported. • Auto renewal timers are started in the device based on the configured value (default is 1/3rd days before the certification expiry).	The ACME client is installed in GigaVUE-FM and takes care of automatic issue/renew/revoke of the HTTPS certification of GigaVUE-FM (standalone GigaVUE-FM instances and also instances in a HA group). Issuance: After the certificate is downloaded, GigaVUE-FM will automatically update the ACME issued certificate for web operation. Renewal: • Both manual and automatic renewals are supported.

	Note: If the user provided auto renew days is > (expiry date – today date), then default renewal days will be calculated (1/3rd days before expiry). Both public and private keys are renewed.	Auto renewal timers are started in GigaVUE-FM based on the configured value (default is 1/3rd days before the certification expiry).
Certificate Revocation	Upon receiving revoke command (from GigaVUE-FM), the device: - Re-issues a new certificate and maps it for the HTTPS operations. - Sends a revocation request to the ACME server and deletes the same from the device cache. Note: The certificate revocation process renews the certificate first followed by the revocation. This is to avoid the down time of the web server .	Revoke operation in GigaVUE-FM: - Initiates re-issue of new certificate - Followed by revocation of the existing certificate. Once the re-issue and revoke operation is successful, the newly issued ACME certificate will be activated as the Web certificate. If revoke fails, GigaVUE-FM will fall back to default certification mode.
Clear Certificate	Clear operation clears the ACME issued certificate from the devices and maps the web certificate to the default certificate. This command also cancels the auto-renewal timers that are started by the ACME client in the device	Deleting the ACME issued certificate results in GigaVUE-FM falling back to the default certification mechanism.

ACME Configuration in Devices

The ACME client configured in the device takes care of certificate issuance, renewal and revocation for the devices.

Pre-requisites

The following are the pre-requisites for ACME configuration:

- DNS must be configured.
- Root of ACME server and intermediate certificates must have been installed and added to the CA list (Refer to [CA List](#) page).

Notes

- Device uses its domain name to download (Issue) a certificate from a CA.
- Certificate revocation and renewal (manual renewal) requires domain name and box id as input.
- Classic mode supports rsa-2048 and rsa-4096 certificate algorithms. Secured crypto & FIPS mode support prime256v1 and secp384r1 certificate algorithm.

Limitations

The following are the limitations:

- ACME certificate can be issued only for single domain. Multiple domain name as Subject Alt name is not allowed.
- It is not possible to issue a new certificate based on CSR.
- Command to modify the renewal-period for the already issued certificate is not available.
- Managing multiple server certificate using ACME is not supported.
- Only web certificates used in the device will be managed by ACME.

Add Root CA Certificate of ACME Server

You must add the root CA certificate before using the ACME protocol for certificate issuance and renewal.

CLI Command

Invoke the following command to add the root CA certificate of the ACME server to the nodes:

```
config# crypto certificate name <cert name> public-cert pem <PEM string>
```

Invoke the following command to add the root CA certificate of the ACME server to all the nodes in a cluster:

```
config# crypto certificate ca-list default-ca-list name <cert name>
```

Certificate Issuance

Gigamon devices handle the issuance of web server certificate as per the ACME protocol.

CLI Command

Invoke the following command from CLI to generate a fresh certificate and its corresponding private key:

```
config# crypto certificate acme issue box-id <box-id> domain <xyz.gigamon.com> ca-  
url <url> {algorithm <rsa-2048 | rsa-4096 | ec-prime256v1 | ec-secp384r1>}  
{renew-days <1-365> } {root-cert <cert_name>}
```

You can specify the number of days (1 to 365 days), when the device should contact the ACME server to renew the certificate before its expiration (default is 1/3rd of the number of days before expiry).

NOTE: Certificate issuance process is a time consuming process (because of authorization/challenge involved). After user executes issue command, a message "Issuance in progress. Check status using `show crypto acme client info {box-id <box-id>}`" is displayed.

If the command is successful:

- The device generates a private key and downloads the signed certificate from the CA server.
- The certificate is installed in the default certificate location. The certificate will be renamed as acme-https-crt.
- The new certificate is used only for web communications.
- SNMP traps will be sent to syslog-server and GigaVUE-FM. The traps are sent before start of an operation (issue, renew and revoke) and after the operation is completed, (success / failure).
- Use `Show crypto certificate` to view the newly downloaded certificate.
- Use `show crypto acme client info` to view the status of the certificate.

If the command fails:

- The existing certificate (previously used on the system) will be used for web communication.
- If the challenge process takes a longer time, the acme-client will be timed out and appropriate error messages will be displayed. This is also reflected in `show crypto acme client info`.
- In case of failures in downloading the certificate from ACME server, you must correct the errors and execute the certificate issue command again to download the certificate.

Refer to the GigaVUE CLI Reference Guide for details about the command.

Certificate Renewal

Renewal of web server certificate is handled in the device as follows:

- The device periodically auto-renews the certificates based on the auto renew interval configured during the issue of certificate. By default, auto-renewal happens one-third of the days before expiry.
- You can also manually renew the certificate using the domain name that is used during the certificate issuance phase.

NOTE: The ACME client in the device takes care of renewing certificates that are issued only by ACME. Other user provided certificates (eg., LDAP, TACACS) will not be auto-renewed by the ACME client.

CLI Command

Invoke the following command to renew a certificate:

```
config# crypto certificate acme renew {box-id <box-id>} domain <domain-name>
```

If the command is successful:

- The CA renews the certificate and its corresponding private key as well.
- The device replaces the certificates in the HTTPS certificate path.
- SNMP trap is sent to GigaVUE-FM to indicate that the certificate has been successfully renewed. Syslogs will be sent to syslog server and GigaVUE-FM.

Certificate Revocation

To revoke a certificate, the device sends a signed revocation request indicating the certificate to be revoked. If the request is valid, the server will revoke the certificate. To avoid the downtime of the devices' web server, the revoke CLI command:

- Internally renews the certificate
- Followed by revoking the compromised certificate.

If the renew operation fails, the device will switch to default certificate.

CLI Command

Invoke the following command to revoke a certificate:

```
config# crypto certificate acme revoke {box-id <box-id>} domain  
xyz.gigamon.com
```

If the command execution is successful, SNMP trap is sent to GigaVUE-FM to indicate that the certificate has been revoked.

Clear ACME

Clear operation clears the ACME issued certificate from the devices and maps the web certificate to the default certificate. This command also cancels the auto-renewal timers that are started by the ACME client in the device.

CLI Command

```
crypto acme client clear
```

You cannot switch to another certificate for web communication when ACME certificate is used for web. This is to avoid unnecessary auto-renewals.

View Certificate Status

The ACME operations such as issue, renew and revoke are time-consuming. Therefore, to know the status of the ACME operations use the following command:

```
show crypto acme client info box-id <box-id>
```

Example for Certificate Issuance

```
show crypto acme client info box-id 4
```

Box Id 4:

=====

ACME Issued Certificate Info

=====

https:

Domain : 10.60.95.2

Cert Name : acme-https.crt

Acme-Server : https://10.115.72.233:8080/acme/acme/directory

First-Issued : 2021/10/11 16:14:46

Next Renewal : 2021/12/10 23:26:47

Expires : 2022/01/09 16:14:48

Renewal Days : System Computed

Last Succesful Renewal : n/a

Last Failed Renewal : n/a

Last Request Status Since Bootup

=====

Domain : 10.60.95.2

Acme-Server : https://10.115.72.233:8080/acme/acme/directory

Request-Status : Success

Type of Request : Issue

Troubleshooting Scenarios

Use the following table to troubleshoot issue(s) that you might encounter during the ACME certification process:

Problem	Solution
Failure in ACME certification renew/revoke operation	- Check the device log/GigaVUE-FM events and see if this is due to wrong account registration. - Clear the ACME issued certificate and issue a fresh certificate.

Configuration from GigaVUE-FM GUI

You can configure ACME certification for the devices from GigaVUE-FM GUI or from the respective device GUI.

- Global configuration from the GigaVUE-FM GUI allows you to configure the ACME certificate for all the devices managed by GigaVUE-FM.

- Configuration of ACME from the devices allows you to configure the ACME certificate for the specific devices.

NOTE: For global configuration of ACME for devices from GigaVUE-FM, root/intermediate certificate of CA must be configured in the Trust Store page of GigaVUE-FM.

Refer to the following GUI screens for details:

- [Certificate Issuance](#)
- [CA List](#)

ACME Configuration in GigaVUE-FM

ACME configuration in GigaVUE-FM is required for the following:

- Web certification of GigaVUE-FM
- Communication between the individual GigaVUE-FM instances in case of High Availability.

Pre-requisites

The following are the pre-requisites for ACME configuration:

- Only super-admin users and admin users can Issue, Renew, Revoke and Delete certificates.
- DNS must be configured. GigaVUE-FM and the devices will perform DNS look up for fetching the DNS name.
- The trust chain of CA authority must be configured in both GigaVUE-FM and devices.
- Root certificate for a CA must be installed as a prerequisite for requesting the certificate.

The following table summarizes about ACME implementation in GigaVUE-FM:

Task	Description	Refer to...
Certificate Issuance	GigaVUE-FM uses the rootca and the user specified ACME server address along with its domain name or user provided CSR to download the requested certificate. After the CA issues the certificate, GigaVUE-FM: - Copies the certificate to the HTTPS certificate path - Generates cms.p12 file using the following command: <pre>openssl pkcs12 -export -name CMS -out cms.p12 -inkey localhost.key -in localhost.crt -passout pass:cms123</pre> - Uploads the cms.p12 generated file in the directory. NOTE: Appropriate error message will be displayed if downloading the certificate from the CA server times out. The tomcat and httpd will be restarted for the new certificates to take effect.	- To configure the ACME Server, refer to Notes for details. - Refer to Certificate Issuance section for details.
Certificate Renewal	GigaVUE-FM supports both manual and automatic renewal of ACME certificates. Renewal of GigaVUE-FM web certificate server certificate is handled as follows: Manual Renewal: You can manually renew the certificate using the domain name that is used during issuance phase. Automatic Renewal: You can configure the auto-renewal period during the certificate Issuance phase. However, you can modify the renewal days. NOTE: By default, auto-renewal is 1/3rd of the certificate validity period.	Refer to Certificate Renewal .

Task	Description	Refer to...
	- Once the CA renews the certificate, the device will replace the certificates in the certificate path. - GigaVUE-FM generates the cms.p12 file and once cms.p12 is generated, it would be uploaded in the directory. NOTE: If downloading the certificate from the CA server times out, appropriate error messages will be displayed. You must retry renewal of the certificates. The tomcat and httpd will be restarted for the new certificates to take effect.	
Certificate Revocation	To revoke a certificate, GigaVUE-FM sends a signed revocation request indicating the certificate to be revoked. If the request is valid, server will revoke the certificate. NOTE: The revoke operation will internally perform a re-issue of new certificate first and then it will initiate the revoke of old certificate. If the operation fails, GigaVUE-FM will fall back to default certificate.	Refer to Certificate Revocation .
Certificate Deletion	Once the certificate is deleted, GigaVUE-FM will fall back to the default certification mechanism.	

NOTE: If DHCP is enabled in GigaVUE-FM and if the IP address of GigaVUE-FM changes, you must re-issue the certificate because the manual renewal and revoke operations will not work. This is because, GigaVUE-FM GUI passes the old IP address as the domain name instead of the new IP address during the first manual renew and revoke after the change in IP address (due to which DNS resolution fails). Therefore, to re-issue the certificate you must provide the Fully Qualified Domain Name (FQDN) of the new IP address and issue the new certificate. GigaVUE-FM then updates the new IP with FQDN in the database and deletes the old entry.

Trust Store

The SSL Certificate Enhancement feature in GigaVUE-FM ensures secure communication between GigaVUE-FM and the devices added to GigaVUE-FM. The Trust Store page in GigaVUE-FM enables security by maintaining a list of certificates provided by the devices. To add new devices to GigaVUE-FM and to manage the existing devices, you must add the root CA certificate of the respective devices to the Trust Store.

Click the **Enable Secure Access** button in the Trust Store page to enable and disable secure access:

- If you enable security, GigaVUE-FM performs the following:
 - Verifies if the root CA certificate of the device is available in GigaVUE-FM.
 - Adds the device only if the certificate is signed by an authorized CA.
 - Verifies the chain of custom certificates, as required.
- If you disable security, GigaVUE-FM adds the devices without any validation.

IMPORTANT RECOMMENDATION: Prior to adding the public certificates of the devices to the Trust Store, you must ensure that:

- Login to the devices and add the private key and certificate of the devices through CLI/Console into each of the devices. Use the **crypto** CLI command for adding the keys and certificates. Refer to the *GigaVUE-OS CLI Reference Guide* for detailed information.

Cloud Solution

NOTE: The following configuration is not applicable for FMHA mode.

The GigaVUE-FM communicates with cloud platforms like OpenStack, and Nutanix through an encrypted connection secured by Secure Sockets Layer (SSL). To ensure that SSL certificates provided by these platforms are valid and trusted, you must enable the Trust Store on your GigaVUE-FM and add the certificate of Root Certificate Authority (Root CA) to the Trust Store. This process helps your GigaVUE-FM verify the authenticity and integrity of SSL certificates, ensuring secure data transmission. Any updates to the Trust Store, require a GigaVUE-FM process (CMS) restart.

To access the Trust Store Page, click  and select **Certificates > Trust Store**.

To add a certificate to GigaVUE-FM:

1. Click **Add** on the Trust Store page. The Add Certificate page appears.
2. Enter an **Alias** for the certificate.
3. Click **Choose File** to upload the certificate.
4. Click **Add**.

The certificate is added to the list view.

You can also perform the following operations:

- **Filter:** Click the **Filter** button to filter the records based on the selected criteria.
- **Delete:** Click **Actions** > **Delete** to delete the selected entry.
- **Export:** Click the **Export** button to export all or only the selected records in CSV or XLSX file format.

NOTE: Revoked certificates can be removed using the delete operation.

Updating Trust Store

With software version 5.12.xx, the default iSSL trust stores have been updated from Mozilla Firefox. Refer to [apps inline-ssl](#) in GigaVUE-OS CLI Reference Guide for more information on the commands that update or replace trust store.

If you do not wish to upgrade GigaVUE-OS to the software version 5.12. xx, follow the below instructions on how and where to download the latest Mozilla Firefox trust store, and how to append their additions to override the default trust store during the update.

The default iSSL trust stores are automatically updated with each GigaVUE release.

GigaVUE-OS Version	Customer Trust Store	Gigamon Trust Store (CC*) <i>with Custom Certificates</i>	Gigamon Trust Store
Prior 5.12.00	No action	- Fetch replace trust store. - Fetch append customer's trust store with custom certs	Fetch replace trust store
With 5.12.00	No action	Fetch reset trust store	Fetch reset trust store
With 6.5.00	No action	No action	No action

GigaVUE-FM

The ACME client configured in GigaVUE-FM contacts the ACME server to issue, renew, revoke and delete certificates for the standalone GigaVUE-FM instances or for the GigaVUE-FM instances that belong to the High Availability group. In case of HA, the ACME operations must be implemented in each of the GigaVUE-FM instances.

Refer to the following sections for details.

Certificate Issuance

For certificate issuance by the ACME server:

NOTE: Ensure to configure the ACME server before performing these steps.

1. Go to **Settings** and select **Certificates** > **GigaVUE-FM**. The **GigaVUE-FM** page is displayed.
2. Select the IP address of the GigaVUE-FM instance for which you need the certificate to be issued.

3. Click **Actions** and select **Issue**. Enter the following details:

Field	Description
IP Address/FQDN Name	The IP address or FQDN using which the GigaVUE-FM instance can be reached externally. If this is not entered, DNS will be resolved for the selected IP address and certificate request will be initiated for the resolved FQDN. NOTE: This field is optional.
ACME Server Alias	The ACME server. Click Add ACME Server, if the ACME server is not already added. NOTE: This is a mandatory field.
Algorithm	The required Algorithm. The default algorithm for GigaVUE-FM is rsa-4096 NOTE: This field is optional.
Renewal days	The number of days after which the certificate must be renewed. The default renewal days is 1/3rd of certificate validity period. NOTE: This field is optional.

4. Click **OK**.

The ACME certificate is added to the list view and the following fields are included in the list:

- Expiry Date
- Certificate Status
- Certificate Request Status

Certificate Renewal

1. Go to **Settings** and select **Certificates** > **GigaVUE-FM**. The **GigaVUE-FM** page is displayed.
2. Select the IP address of the GigaVUE-FM for which you need the certificate to be renewed.
3. Click **Actions** and select **Renew**.

The renewed certificate is downloaded and activated with the new expiry date.

Auto renewal is initiated with respect to the user configured renewal Days. If the user configured renewal days is invalid or if the user is not configured the renewal days during issue, Auto renewal will initiate on 1/3rd of cert validity period

Certificate Revocation

To revoke a certificate:

1. Go to **Settings** and select **Certificates** > **GigaVUE-FM**. The **GigaVUE-FM** page is displayed.
2. Select the IP address of the GigaVUE-FM for which you need the certificate to be revoked.
3. Click **Actions** and select **Revoke**.

Revoke operation in GigaVUE-FM initiates re-issue of new certificate followed by revocation of the existing certificate. Once the re-issue and revoke operation is successful, the newly issued ACME certificate will be activated as the Web certificate. If revoke fails, GigaVUE-FM will fall back to default certification mode.

Certificate Deletion

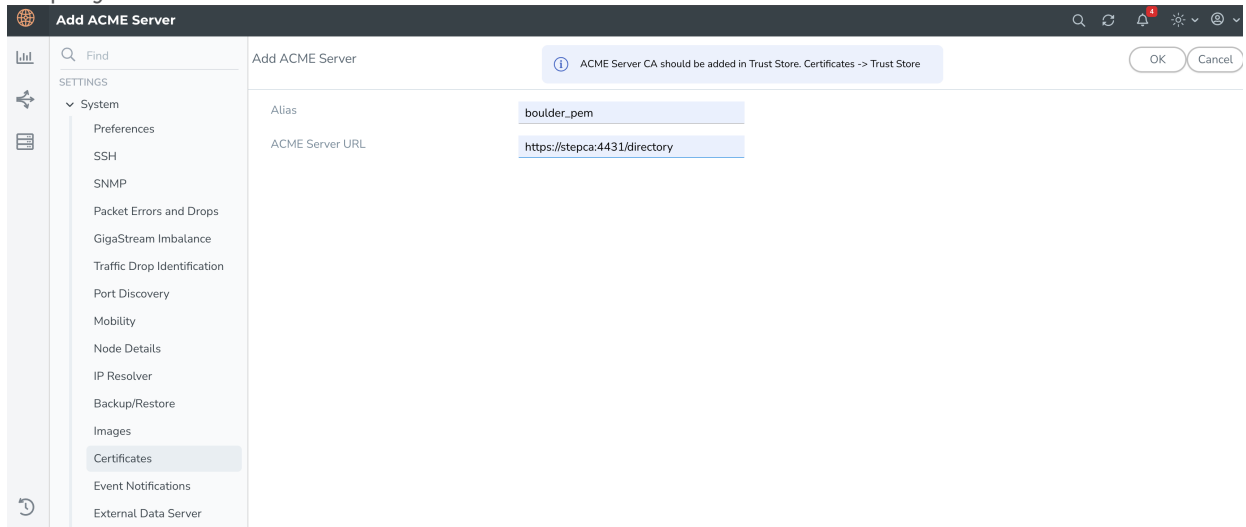
Click Delete Certificates to delete a certificate. GigaVUE-FM will fall back to the default certificate process.

Configure ACME Server

The ACME server page allows you to configure the ACME server details in GigaVUE-FM.

To add a server:

1. Go to **Settings** and select **Certificates** > **ACME Server**. The **ACME Server** page is displayed.



2. Click **Actions** and select **Add Server**. Enter or select the following details:

Field	Description
Alias	Alias name of the ACME server
ACME Server URL	ACME Server URL

3. Click **OK**. The server will get added to the list view.

To edit server details:

1. Go to **Settings** and select **Certificates** > **ACME Server**. The **ACME Server** page is displayed.
2. Select the server from the list view.
3. Click **Actions** and select **Edit**. You can edit the **ACME server URL**.

Notes

Refer to the following notes:

- You must add the certificates (ACME server CA files) in the trust store before configuring the ACME certificates. To configure the certificates, refer to [Updating Trust Store](#).
You can add multiple servers to the ACME Server page. However, you can configure only one server for GigaVUE-FM.
- If GigaVUE-FM uses self-signed certificates, the **Certificate Issued** field will be set to 'No'.
- You cannot delete a server without deleting the ACME Certificates issued by the server.

CA List

The CA List page allows you to add the root CA certificate for the devices. You can access the CA List page from GigaVUE-FM as well the devices:

From GigaVUE-FM	Go to Settings > System > Certificate > CA List	Use this for global configuration of all the devices managed by GigaVUE-FM.
From Devices	Go to Inventory > Node > Settings > Global Settings > CA List	Use this for configuration of individual devices and clusters.

To add a CA for all the devices managed by GigaVUE-FM:

1. Go to **Settings** and select **Certificates > CA List**.
2. Click **Add**.

3. Select or enter the following details:

Field	Description
Alias	Alias name of the CA. NOTE: At Global level the certificate name can have up to 28 characters. At the node level, the certificate name can have up to 40 characters.
Description	Description of the CA.
Choose Certificate	Choose the certificate from the desired location.

4. Click **Save**.

The CA will be added to the list view and displays the following details:

- Alias
- Description
- Issuer Name
- Algorithm
- Subject Name

- Valid From
- Valid To

The CA List page allows you to perform the following tasks:

- **Delete:** To delete a certificate.
- **Filter:** To filter the certificates based on specific criteria.
- **Export:** To export the details in the CA List page to a CSV file.
- **Audit:** To audit the actions performed in the CA List page.

ACME Certificate

The ACME Certificate page allows you to configure the ACME Server URL, thus enabling you to perform the following tasks on the devices managed by GigaVUE-FM:

- Issue and renew certificates
- Delete Certificates
- Audit

You can access the ACME certificate page from GigaVUE-FM as well the devices:

From GigaVUE-FM	Go to Settings > System > Certificate > ACME Certificate	Use this for global configuration of all the devices managed by GigaVUE-FM
From Devices	Go to Inventory > Node > Settings > Global Settings > ACME Certificate	Use this for configuration of individual devices and clusters.

Certificate Issuance

To issue a certificate:

NOTE: You must add the root CA certificate of the ACME server using the CA List page.

1. Go to **Settings** and select **Certificates > ACME Certificate**. The **ACME Certificate** page is displayed.

2. Click **Actions** and select **Issue**. Enter or select the following details:

Field	Description
ACME Server URL	The ACME server URL. NOTE: This field is mandatory.
Algorithm	Algorithm. The default algorithm for device in classic mode is rsa-2048. The default algorithm for device in FIPS mode is prime256v1. NOTE: This field is optional.
Renewal Days	The next renewal date. The default renewal days is 1/3rd of the certificate validity period. NOTE: This field is optional.

3. Click **Save**.

The ACME certificate is added to the list view and displays the following details:

Field	Description
Cluster Name	The name of the cluster.
Box Id	The box identifier of the node for which the certificate is issued.
Domain	The domain name, which will be used as subject name as well as subject alternate name in the certificate.
ACME URL	ACME URL
Algorithm	Algorithm
Next renewal date	The next renewal data.
Expiry date	The expiry date of the certificate.

Field	Description
Last request ACME URL	The last request status of the ACME URL.
Last Request Type	The type of request.
Last Request Status	The type of status.

Certificate Renewal

To renew a certificate:

1. Go to **Settings** and select **Certificates** > **ACME Certificate**. The **ACME Certificate** page is displayed.
2. Click **Actions** and select **Renew**.

Certificate Deletion

Click **Delete Certificate** to delete the certificate. The devices will fall back to the default certificate process.

Audit

Appropriate events are captured in the Events page for certificates issuance and renewal process using the ACME client configured in GigaVUE-FM and the devices managed by GigaVUE-FM. The same is added as audit log.

Integrate Private CA

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

Rules and Notes

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

To integrate private CA

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

- Upload CA Certificate to GigaVUE-FM.

Generate CSR

To create an intermediate CA certificate:

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

The CSR is downloaded successfully.

Upload CA Certificate

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

To upload the signed CA certificate to GigaVUE-FM:

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

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

Event Notifications

GigaVUE-FM provides powerful email notification capabilities, automatically sending emails to specified addresses when a wide variety of events take place on the node. Gigamon strongly recommends that you configure this feature so that you have immediate visibility of the events affecting node health.

Some of these events are detected by GigaVUE HC Series and GigaVUE TA Series, and the notifications are forwarded to the GigaVUE-FM. For a node to be able to send notifications to the GigaVUE-FM, the node's SNMP notifications must be configured with the IP address of GigaVUE-FM. For information about adding a destination for SNMP notifications, refer to Configuring SNMP Notifications in *GigaVUE-OS CLI Reference Guide*.

Notes

- Before configuring the notifications, ensure to configure the Email Server and send a test email for confirmation. Refer to [Send Test Email](#).
- When upgrading from earlier versions, the notification tasks are migrated as follows:

Upgrade Path	Task Status after Migration
From 5.11.00 to 5.13.00	Instant notification tasks are migrated as one task per user.
From 5.12.00 to 5.13.00	• Instant notification tasks are migrated as one task per user. • Batch notification tasks are migrated as one task per user and the tasks will be in disabled state. You must enable the tasks for notification.

Configure Email Notifications

To configure the email notification of events:

On the left navigation pane, click  and select **System > Event Notifications**. The following pages appear :

- **Notifications:** Use to configure automatic email notification schedule for the events.
- **Permitted Recipients:** Use to configure the recipient email addresses and domain names.
- **Configuration:** Use to configure the event notification and data notification interfaces.
- **SNMP Server:** Use to configure the receivers for SNMP Trap notifications sent from the GigaVUE-FM.

Refer to the following sections for details:

- [Event Notifications](#)
- [Permitted Recipients](#)

- [Configure SNMP Traps Notification](#)

Event Notifications

The Event Notifications page allows you to schedule the notification of events to the users, either as:

- **Instant:** Events will be notified instantly.
- **Digest:** Events generated within a pre-defined time interval will be consolidated into a batch and sent as a single email.
- **SNMP Trap:** Events generated within a pre-defined time interval will be consolidated into a batch and sent as a single email.

You can schedule notifications for :

- single events or a collection of events consolidated into templates.
- multiple users or domains by adding the email addresses or domain names to the Permitted Recipients page.

To add a new schedule:

1. Select  > **System** > **Event Notifications** > **Notifications**.
2. Click **New**. Enter the following details:

Field	Description
Overview	
Name	The name of the notification
Description	A brief description about the notification
Notification Type	Select as Instant or Digest

For Batch Notification:

Field	Description
Overview	
Email Subject Prefix	The email subject prefix for the email notifications sent to the user. You can key in a maximum of 12 characters. The default prefix is 'GVFM-Events'. The email prefix is added to both instant and digest emails.
Frequency	The frequency of the schedule. The following frequencies are available: • Minutes: 15, 30

Field	Description
	• Hours: 1, 2, 3, 4, 6, 8, and 12 • Daily: For daily schedule, configure the required time, which is the local time of the GigaVUE-FM instance.
If No Events Occur	If there are no events triggered, you can choose to: • Send Email Anyway • Don't Send Email
Enable	Enable or disable the schedule for sending batch notifications. NOTE: You can enable a maximum of 20 schedules at a time.
Include Attachment	Enable this to include the attachment in the email. NOTE: The size of the attachment can vary from 0 to 5000.

For Instant Notifications:

Field	Description
Overview	
Email Subject Prefix	The email subject prefix for the email notifications sent to the user. You can key in a maximum of 12 characters. The default prefix is 'GVFM-Events'. The email prefix is added to both instant and digest emails.
Rate Limit	The number of events that will be sent in a defined time. The rate limit configuration is applicable globally for all the schedulers. The valid range is between 1 and 20, and the default value is 10.

3. Configure the following:

Option	Description	Reference
Tags	Get notified about the events based on the tags (both RBAC and Aggregation tags)	Tags
Recipients	Add the email addresses of the recipients or the domain names	Recipients
Events	List of events for which the notification should be sent.	Events

For SNMP Trap

To enable SNMP Trap notifications:

1. Select  > **System** > **Event Notifications** > **Notifications**.
2. Click **New**. Enter the following details:

Field	Description
Overview	
Name	The name of the notification
Description	A brief description about the notification
Notification type	SNMP Trap
External Trap Receiver	Select the Trap Receiver from the drop-down list. To add a new trap receiver refer to Configure Notification Receivers
Events	List of events for which the notification should be sent. Refer to Events

Tags

The **Tags** option allows you to get notified about the events depending on the tags assigned. This includes the subscribed events with resource type as taggable and meets the tag condition, and the events for non-taggable resources.

Tag type can be access-control or aggregation tag type, based on which the events will be notified.

To add tags:

1. Click the + symbol under tags. The Add Tags dialog box appears.
2. Select the required **TagKey** and the associated **Tag Values**.
3. Click **Add Tag(s)**.

Refer to the *Tags* section in the *GigaVUE Administration Guide* for details.

Recipients

The **Recipients** option allows you to add the email addresses of the recipients or domain names to send the scheduled notifications. The email recipients must already be added to the Permitted Recipients page. Refer to the [Permitted Recipients](#) section for details.

Events

The **Events** option allows you to add the events for which the notification will be scheduled. To add Events to the notification, you can:

1. Choose a pre-defined template category. All related events are grouped in the respective category types. The following template types are available:
 - IP Interface Events
 - License Events
 - GigaSMART Events
 - Card Events
 - Trap Events
 - Node Events
 - Port Events
 - Chassis Events
 - Cluster Events
 - Configuration Events
 - Cloud Monitoring Session Events
 - Cloud Fabric Node 3PO Events
 - Cloud Fabric Node Events
2. Add new event or events. Click **Add Event** and enter the following details:
 - **Scope:** Scope of the events to be notified, such as Physical Node, Inline, etc.
 - **Sub Type:** Type of events based on the scope selected.
 - **Event:** List of individual events under the sub type.
 - **Severity:** Severity level of the events that need to be notified.
3. Click **Add Event(s)**. The events will be added to the Events section.

NOTE: Click **Clear All Events** to clear all the events. Use the Delete option to delete specific events.

Buttons

The Scheduler page has the following buttons:

Button	Description
Actions	Use the Actions button to perform the following operations: • Enable: Enable multiple digest notifications • Disable: Disable multiple digest notifications • Clone: To clone an existing notification. Enter a new name and description for the cloned notification. You can also edit other fields, as required. • Edit/Delete: To edit and delete the existing notifications.
Filter	Use the Filter button to filter the notifications based on the following criteria: • Task Name • Type • Events • Recipients • Tags
Export	Use to export the notifications.

Refer to the following image for sample digest notification configuration:

The screenshot displays the 'Edit Notification' configuration interface. On the left is a sidebar with a search bar and a 'SETTINGS' menu. The 'System' category is expanded, showing options like Preferences, SNMP, Packet Errors and Drops, GigaStream Imbalance, Port Discovery, Node Details, IP Resolver, Backup/Restore, Images, Certificates, Event Notifications (highlighted), External Data Server, Licenses, Logs, Storage Management, and Reports. The main area is titled 'Edit Notification' and contains the following fields:

- Name ***: A text input field containing 'Notification'.
- Description (optional)**: A text input field containing 'Notify License Expiry'.
- Notification Type ***: A dropdown menu set to 'Instant'.
- Email Subject Prefix ***: A text input field containing 'Licenses'.
- Rate Limit**: A text input field containing '10', with an information icon (i) to its right.
- Recipients**: A section containing a 'Recipients List *' with a list box showing 'krithika.jeelaraman@gigamon.com' and a close button (X). To the right of the list box is a light blue help box that says 'Enter the email IDs separated by comma.'

At the top right of the configuration area are 'Cancel' and 'Apply' buttons.

Permitted Recipients

The **Permitted Recipients** page displays the list of email addresses/domain names along with the notifications subscribed for that email address.

From the **Permitted Recipients** page, you can add the email addresses of the recipients or the domains to which the notifications must be scheduled and sent. To add the email addresses/domain name:

1. Select  > **System** > **Event Notifications** > **Permitted Recipients**.
2. Click **New**. In the **Add Permitted Recipients** dialog that appears enter the following details:
 - **Type**: Can either be email or Domain.
 - **Address**: Email address or the domain name.
 - **Alias**: Alias for the email address or domain name
3. Click **Save**.

NOTE: You can add permitted recipients only if you are a user with read-write access to the GigaVUE-FM security Management category.

To filter the email addresses/domain:

1. Click **Filter**.
2. Select the required combination of Type, Address or Alias.
3. Click **Apply Filter**.

Use the **Clear** button to clear the existing filters.

You can also:

- Delete the email addresses/domain: Select the required records, click **Actions** > **Delete**.
- Export the records in the Permitted Recipients page in CSV or XLSX format, using the **Export/Export All** buttons.

Email Format

The email subject will have the configured prefix together with the severity details of the events generated over a period of time. Use the email subject prefix to filter the event notification emails.

In case of email digest, the email body has the following format:

- **Summary table**: Lists the events based on the severity details of the events.
- **Event digest table**: Provides a detailed breakup of the top ten events in terms of the severity, event type, source, hostname, entity type, entity id and number of occurrences.

Click on the links provided in the email:

- If you are already logged in to GigaVUE-FM, you will be navigated to the Events page with the applied filters.
- If you have not already logged into GigaVUE-FM, you will be navigated to the login page. Login to access the Events page with the applied filters.

NOTE: The list of events displayed on the Events page depends on your user role and access rights. Refer to the [Events](#) section for details.

Based on the **Include Attachment** configuration, an event digest attachment is also included in the email.

The email and the attachment include a hyperlink that will navigate you back to the Scheduler table in the GigaVUE-FM GUI from where you can create/edit/delete/view schedulers and also update the permitted recipients.

Configure SNMP Traps Notification

GigaVUE-FM sends SNMP Trap notification for the GigaVUE-FM events such as Image Upgrade Status, Backup operation Status to the configured SNMP trap receivers. GigaVUE-FM sends SNMP v2c/v3 trap notifications to specified receivers.

NOTE: You can configure a maximum of 10 SNMP receivers.

Configuring SNMP traps notification consists of the following steps:

- Configure Notification Receivers
- Enable SNMP Trap and Events

Configure Notification Receivers

To configure a notification receiver and enable the SNMP sever, do the following:

1. Select **Settings > Event Notification > SNMP Server**.
2. Click **Add**. The **Add SNMP Server** dialog appears.
3. Configure the notification receivers by doing the following:
 - a. Enter the alias name of the SNMP server.
 - a. Enter the IP address of the trap receivers in the **Hostname / IP Address** field.
 - b. Click in the **SNMP Version** field and select **v2c** or **v3** from the drop-down list.

If you select v3, you should enter the **User Name** and select any of the following **Security Level** in the drop-down list:

- **noAuthNoPriv** – Does not provide authentication or encryption.

- **AuthNoPriv** – Provides authentication but does not provide encryption. When you select this security level, you should also select the required Authentication protocol and should also provide its password. The authentication type is either **md5** or **sha1** or **sha256** or **sha384** or **sha512**, which specifies the mechanism to use for password hashing.
- **AuthPriv** – Provides both authentication and encryption. When you select this security level, you should also select the required Authentication and Encryption protocols, and should also provide their passwords. The authentication type is either **md5** or **sha1** or **sha256** or **sha384** or **sha512**, which specifies the mechanism to use for password hashing. The privacy type specifies the level of encryption for the password, which is either **des** or **aes-128** or **aes-256**.

The following table provides information about the field or fields that should be selected for the above mentioned security levels:

Security Level	Auth Protocol and Auth Password	Priv Protocol and Priv Password
noAuthNoPriv	No	No
AuthNoPriv	Yes.	No
AuthPriv	Yes	Yes

- Enter the server port number in the **SNMP Port** field. The default port number is **162**.
 - Enter the community string in the **Community** field for SNMP Version v2c. For example, public.
- Click **Ok**.

SNMP server details is added to the list view.

The SNMP Server page has the following buttons:

Button	Description
Add	Use to add SNMP server details.
Filter	Use to filter the SNMP Server based on the selected criteria.
Actions	Use the Actions button to perform the following operations: • Clone: To clone an existing SNMP server. Enter a new name for the cloned SNMP server. You can also edit other fields, as required. • Edit/Delete: To edit and delete the existing notifications.
Export/Export All	Use to export the SNMP server details in CSV or XLSX format.

Validate SNMP Receiver Configuration

To validate the SNMP Receiver Configuration, do the following:

1. Select **Settings > Event Notification > SNMP Server**.
2. Select the receiver and click **Send Test SNMP Trap** to send a test trap to the selected SNMP receiver.

Enable SNMP Trap and Events

To enable events for SNMP Server Trap notifications, refer to [Event Notifications](#)

Configuration Settings

When a node is added, GigaVUE-FM registers itself as follows:

- Notification target for SNMP Traps, Events and Syslog.
- Metadata exporter for receiving JSON records for Application Visualization.

By default, eth0 IP of GigaVUE-FM is used as the target address.

NOTE: Traps, events and Syslogs will not be received by GigaVUE-FM when eth0 IP is registered as target address in the following cases:

- Either GigaVUE-FM is behind NAT, or the node being added is behind NAT or both.
- Cloud deployment such as AWS: If AWS and customer infrastructure are isolated, then nodes in the customer infrastructure will not be able to reach GigaVUE-FM via eth0. Public IP of GigaVUE-FM must be used to register the target address.

Traffic received in GigaVUE-FM can be of the following two types:

- Management Traffic
- Data Traffic

Using the **Configuration** page you can configure any other interface as the default interface. To do this:

1. Go to **Settings** and select **System > Event Notifications > Configuration**.
2. Enter the following details:

Field	Description
Events Notification Interface	Used for receiving SNMP traps, events, syslogs, etc.
Data Notification Interface	Used for receiving application metadata from devices.

For both the interfaces, you can choose one of the following options:

- **Target Address:** Specify a valid DNS Server Name, Fully Qualified Domain Name of GigaVUE-FM, Static IPv4 address like Public IP, or IPv6 address.

NOTE: When using DNS Server Name, you must configure IP Resolver, refer to [IP Resolver](#) for more detailed and step-by-step instructions.

- **Interface Name:** Choose the interface that should be used while registering GigaVUE-FM as a notification address

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

Email Servers

Use the Email Servers page to configure the Email hosts for sending notification emails. To access the Email Servers page:

1. Go to **Settings** and select **System > Event Notifications > Email Servers**.
2. Click the **Configure** button on the Email Server page to open the configuration page.

The following table describes the fields on the Configure Email Server page.

Field	Description
Enable SMTP Authentication	The user's credentials are used for SMTP authentication when this option is selected. When the option is not selected, SMTP authentication is disabled. Note: When SMTP authentication is enabled, data is transferred only over TLS.
Email Host	The email server to be used for sending notification emails.
Username	The user name to login to the email server.
Password	The password for the user name.
From Email	The address that you want to be displayed in the From field of the notification emails.
Port	If SMTP authentication is enabled, port is set to 587 by default. If SMTP authentication is disabled, port is set to 25 by default.



Note: For SMTP-based authentication, emails will be sent only if you perform the following steps:

- Configure a valid email address (with valid domain name) in your SMTP Server.
- Enter the configured email address in the **From Email** field.

Send Test Email

The **Send Test Email** button in the Email Server page is used to send a test email to the email address before adding it to the **Permitted Recipients** page.

NOTE: The **Send Test Email** button is enabled only when the email host is configured.

You can also:

- Reset the email server: use the **Reset** button
- Export the email server details in CSV or XLSX format: use the **Export/Export All** buttons.

Export Data to External Data Server

The GigaVUE-FM allows you to export statistical data from GigaVUE-FM to an external data server for analysis and visualization. The following data is exported from GigaVUE-FM (including the tags associated with the ports and maps) to an external data server:

- Port Statistics
- Map Statistics
- Map Rule Statistics

Rules, Notes and Limitations

Refer to the following rules and notes:

- You must be a user with write access to the GigaVUE-FM Security Management category to configure an external data server. To view the external data server details, you must be a user with read access to the GigaVUE-FM Security Management category.
- You can configure only one external data server at a time.
- KAFKA is the only message broker supported.
- An event is triggered every 5 minutes if there is a failure in sending of stats from GigaVUE-FM.

Configure External Data Server

Pre-requisite: The port that is configured must be open in the external data server.

To configure an external data server:

1. Go to **Settings** and select **System > External Data Server**.

2. Click **Add**.

< Add External Server

ⓘ Alias, Hostname / IP Address, Port should not be empty×

CancelOk

Alias *

test

Message Broker *

KAFKA

IP Address / Hostname *

10.115.210.249

Port *

9092

Authentication Type *

PASSWORD_AUTH

3. Select or enter the following details, as required.

Field	Description
Alias Name	Alias name of the external data server.
Message Broker	Message broker used by the external data server. - KAFKA is the only supported message broker. - KAFKA Client version used in GigaVUE-FM is 3.2.0¹. - The KAFKA topic name in which the port, map and map rule stats are sent is “fm-physical-stats”. You can listen to this topic from external servers to receive the data.

¹Use KAFKA receiver compatible with the mentioned version.

Field	Description
IP address/Host name of the external server	IP address/host name of the external data server.
Port	Port number on which the external data server is listening. The default port is 9092.
Authentication Type	The authentication type used by the external data server. Can be either: • NO_AUTH: This is the default. • PASSWORD_AUTH: If you select this, you must enter the user name and password configured on the external data server. NOTE: PASSWORD_AUTH in GigaVUE-FM relates to the SASL_PLAINTEXT option in the KAFKA configuration, where in the SASL_PLAINTEXT is used as the security protocol along with the username and password details.

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

Up on successful configuration, for every stats cycle, the following statistical data is sent to the external data server.

- Port
- Map
- Map rule

Use the following buttons to manage the external data server details.

Button	Description
Validate Server	Use to validate the external data server after adding the external server details in GigaVUE-FM: • Upon successful validation, the following message pops-up: <i>Successfully sent the test message to the selected Kafka server</i> • Upon failure of validation, the following message pops-up: <i>Unable to send message via the configured Kafka broker</i>
Add	Use to add an external data server.
Actions	Use the actions drop-down to perform the following actions: • Edit: Edit the external data server details. • Delete: Delete the external data server details.

NOTE: If the Kafka server is no longer needed, it can be deleted. However, if the Kafka server was set up before GigaVUE-FM version 6.9, you must delete it, reconfigure it, and then delete it again to ensure no further data is sent.

Licenses

The Licenses page lets you review and apply licenses for the various products. Refer to the GigaVUE Licensing Guide for details.

System Logs

You can generate log files that contain information about the system. Gigamon support can use these files for root cause analysis.

- Go to **Settings** and select **System > Logs**, to access Logs.
- Click the **Download** button to download the compressed files.

Create a Log file

To create a log file that Gigamon can use for analysis, do the following:

1. Select **System > Logs**.

The Logs page displays, which shows a list of log files.

Logs		Generate	Download	Delete
☐	File Name	Date Created		
☐	sysdump-gigavue-fm-5800-20191202-105...	2019-12-02 4:24:14 PM		

< < Go to page: 1 of 1 > > Total Records: 1

Figure 21 Logs Page

2. Click **Generate**.

The system generates a new log file and displays an event message.

NOTE: You can view a maximum of 5 log files in the screen. GigaVUE-FM automatically deletes the older log file and displays the new log file when you click **Generate** to generate log files for more than 5 times.

3. Select the log file to download, and then click **Download**.

The system downloads the file to your local environment. The file is in a compressed and encrypted format that you can provide to Gigamon.

Delete a Log File

To delete the log files for clearing up the disk space:

1. Select **System > Logs**.

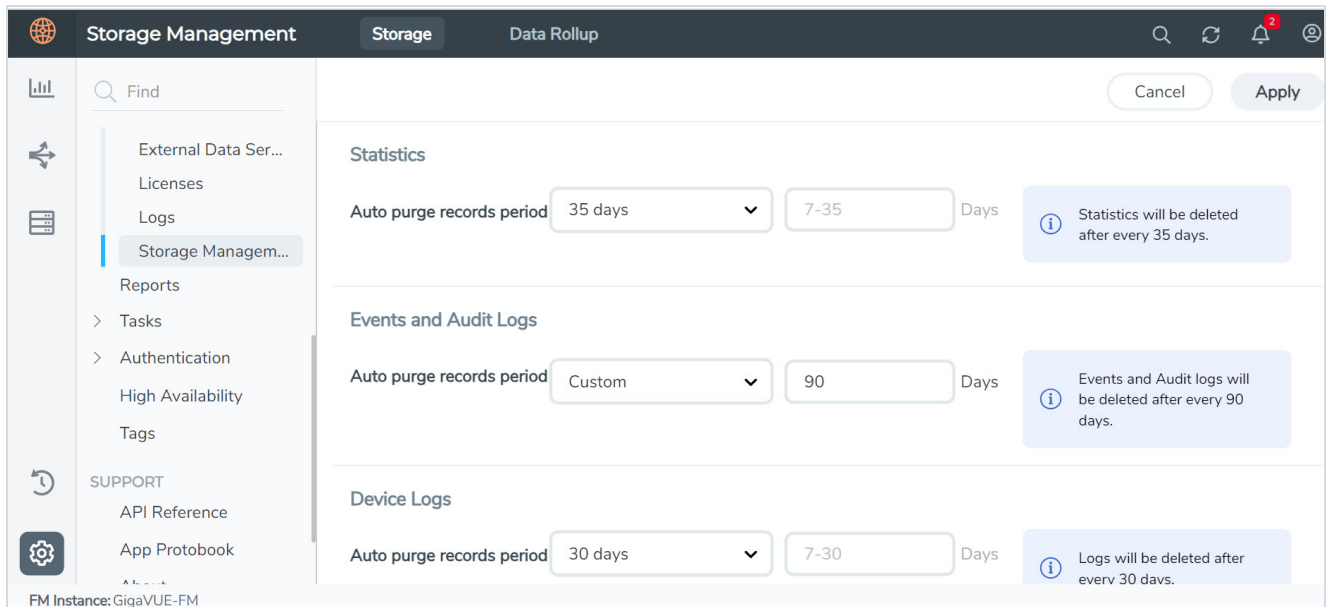
The Logs page displays a list of log files. Refer to [Create a Log file](#).

2. Select the Logs that you want to delete and click **Actions > Delete**.

Storage Management

GigaVUE-FM Storage Management allows you to define how the stored logs are managed. You can specify a schedule for purging old device logs. Storage Management is used for all storage settings, including device logs, event notifications, and statistics. Refer to [Events](#) section.

Go to **Settings** to access Storage Management and select **System > Storage Management**.



To free the used storage older than specified period:

1. Go to **Settings** and navigate to **System > Storage Management**.
2. Configure the Storage Management settings for Storage and Data Rollup.
3. Click **Apply** to apply the settings.

Storage Management Settings

The following are the settings that you can configure from Store Management page.

Storage	
Setting	Description
Statistics	
Auto purge records period	Select the purge period, which is the number of days after which the records will be for deleted. Options are • 7 days • 35 days • custom (between 7 and 35 days) 35 days is the default. Important: The records will be permanently deleted from the database based on the period. NOTE: If you have configured the purge period to a specific value, then after upgrading to software version 6.1.00, the same value is retained. You must manually update the number of days to 35 days, if required.
Events and Audit Logs	
Auto purge records period	Specify how often to delete the Events and Audit Log records. Options are • 7 days • 30 days • 90 days (Default value) • custom (between 7 and 30 days). 90 days is the default. Records will be purged regularly while maintaining records for the specified duration. This means that, at any given time, records of the specified duration will be available to view from the GigaVUE-FM Events page.
Device Logs	
Auto purge records period	Specify how often to delete Device Log records. Options are • 7 days • 30 days (Default value) • custom (in days). 30 days is the default. Records will be purged regularly while maintaining records for the specified duration. This means that, at any given time, records of the

Storage	
	specified duration will be available to view from the GigaVUE-FM Logs page for the node.
Data Rollup	
Allows you to browse and evaluate the performance of the statistics for a duration of up to 120 days for the following fields: • Ports • Maps • Map Rules	Rollup is enabled by default. Use the toggle option to disable Rollup. Once Rollup is disabled you cannot browse 120 days of data. Refer to the Fabric Health Analytics section in the Fabric Management Guide for details. NOTE: Associated Map Rule Visualization will only show the latest map rule count of 35 days.

Caution: There is no undo. Statistics records prior to the days specified will be immediately and permanently deleted from the database when you click **OK**. Event records will be permanently deleted from the database at the specified scheduled interval.

Rules and Notes

- You can edit the purge period after you have configured it to a specified interval. However, if you change the purge period, the records will be purged only after the initial set period expires for the specific record. For example, if the purge period for statistics was initially set to 30 days, and after 5 days, if you change the purge period to 7 days, the first record will be purged only after 30 days and the subsequent records will be purged when the 30 days period expires for the records.
- After you upgrade GigaVUE-FM to 5.11.00, the purge period specified for the storage management settings will be configured to the default values. You must reconfigure the purge period to the required values.
- For optimum performance of GigaVUE-FM:
 - Configure an external syslog server, or
 - If GigaVUE-FM is configured as the syslog server, use minimum time interval for the purge periods.

- If the used size of the config folder exceeds 75%, the disk reclaim script will start to run in the GigaVUE-FM background:
 - GigaVUE-FM maintains a maximum threshold value for the disk space. The default value is 75%. You can configure this to the required value.
 - If the default value is reached, a defender script runs in the background to check if there are any indices beyond the purge policy. If any exist, it will be cleared. An alarm with severity level Warning with a description stating to contact GigaVUE-FM support is triggered. An event notification that captures the indices being removed is created.
 - If the disk space is not reclaimed, GigaVUE-FM stops the stats collection and disables Syslog. The severity level of the alarm is changed to Critical. Another event log is created indicating the disabling of syslog and stats.
 - If the disk space is recovered by manual cleanup, and threshold falls below 75%, disk reclaim will auto enable the stats collection (applicable from software version 6.0.00).

NOTE: Contact Gigamon technical support team to enable stats collection and syslog.

Proxy Server Configuration

The Proxy Server configuration page enables users to create proxy server profiles that can be utilized for URL categorization and certificate revocation status updates thus enhancing network security. The proxy profile is then attached to a device by configuring it in the Inline SSL application. This is applicable only for Gen 3 cards.

Supported Platforms

Proxy Server Profile can only be associated with Gen 3 cards such as:

- SMT-HC1-S module on GigaVUE-HC1 and GigaVUE-HC1-Plus.
- SMT-HC3-C08 module on GigaVUE-HC3.

Configure Proxy Server Profile

1. Go to **Settings>Setting> Proxy Server Configuration > New**. Configure the following field attributes:
 - **Alias**- This is the proxy server profile alias. Once configured, this field cannot be modified.
 - **Description** - Enter a description for the Proxy Server Profile.
 - **Protocol**-Only HTTP protocol is supported.
 - **Proxy Address**- Enter the proxy server address. This could be either the IP address or the domain name of the proxy Server profile .
 - **L4 Port**- Specify the L4 port for the proxy server profile.
 - **Authentication Type**- Only Basic and None authentication types are currently supported. If you select Basic then the following fields will be enabled :
 - **User name** -Enter the User name.

- **Password**- Enter the Password. If you upgraded your device from GigaVUE-OS version 6.8.xx to 6.9.xx, the Proxy Server Profiles configured through GigaVUE-OS CLI will be migrated to GigaVUE-FM. However, to use the Proxy server Profile in a new Inline SSL application you will need to reconfigure your password in GigaVUE-FM.
 - **Periodic Ping**- You can enable or disable Periodic Ping which checks the status of the proxy server profile at regular intervals. If it is enabled configure the following fields:
 - **Periodic Ping Type**-This indicates the type of Periodic ping that would be sent. Only http-connect is supported.
 - **Periodic Ping Interval**-Configure the interval at which the periodic ping should be initiated. You can enter a value from 1-10.
 - **Periodic Ping Failure Retry**- Configure the number of attempts that a periodic ping can be sent. You can enter a value from 1-3.
2. Click on **Save**.

A new Proxy Server profile can also be created from the Inline SSL app configuration page by using the '**Create Proxy**' button. The created Proxy Server profiles will be listed and managed under the **Proxy Server Configuration** page.

The configured Proxy profile is maintained in GigaVUE-FM and is not attached to a node until explicitly done so through an Inline SSL deployment. A unique alias can be used to reuse and attach a proxy server profile configuration to multiple nodes.

Proxy Server Configuration

ALIAS	PROXY ADDRESS	DESCRIPTION	L4 PORT	AUTHENTICATION ...	APP TYPE	APP HEALTH	APP ALIAS
proxy1	1.1.1.1		8888	None	2 Apps		
					Flex Inline SSL ...	Proxy Server...	sslappnew
					Flex Inline SSL ...	Healthy	sslapp1
proxy2	10.114.11.22		7777	None	1 App		
					Flex Inline SSL ...	Proxy Server...	sslapp2

Go to page: 1 of 1 Total Records: 2

FM Instance: GigaVUE-FM - 6.9.00

Editing a Proxy Server Profile

To edit an existing Proxy Server Profile:

3. Go to **Settings>Setting> Proxy Server Configuration**.
4. Select the Proxy Server profile that you want to edit and click on the **Actions> Edit**, the edit Proxy Server profile page appears.
5. You can edit all attributes of your profile, except for the Alias.
6. Click on **Apply** to save your changes.

Any edits made to the Proxy Server Profile will also be reflected in the associated Inline SSL Solution.

Delete a Proxy Server Profile

To delete an existing Proxy Server profile:

1. Go to **Settings>Setting> Proxy Server Configuration**.
2. Select the Proxy Server profile that you want to edit and click on the **Actions> Delete**. The Proxy Server profile is deleted.

NOTE: If your Proxy Server profile is associated with an Inline SSL application, choose 'None' in the Proxy Server profile field on the Inline SSL configuration page to disconnect the proxy server profile prior to deleting the profile.

Configure Proxy Server profile in an Inline SSL Deployment

To successfully attach the Proxy Server profile to the Inline SSL Deployment, follow the below steps:

1. Go to  > **Physical > Orchestrated Flows > Inline Flows > Configuration Canvas** **Inline Flows**.
2. Select the required device with your configured flexible inline decryption solution.
3. Click the '+' icon next to the **Inline SSL APP** option to create a new flexible inline decryption solution or to open the configured solution.
4. Under **Network Access** section, select a **Proxy Server** profile from the drop-down. You can select Proxy Server profiles for each of your GigaSMART engines. Refer [Inline SSL APP—Field References](#) in GigaVUE Fabric Management Guide for details.
5. Click on **OK** to save your configurations. You can assign the configured proxy server profiles to each of your GigaSMART engines.

6. You can view the health of the proxy server profile on the **Proxy Server Configuration** page and on the Inline SSL application page, as shown in the screen below
7. The health of the proxy server profile would have the following states:

-  - This icon indicates that the connection is a success.
-  - This icon can indicate any of the following states of the connection :
 - Authentication Failure
 - Domain Name Lookup Failure
 - Connection Failure
 - Internal Error
 - Disabled

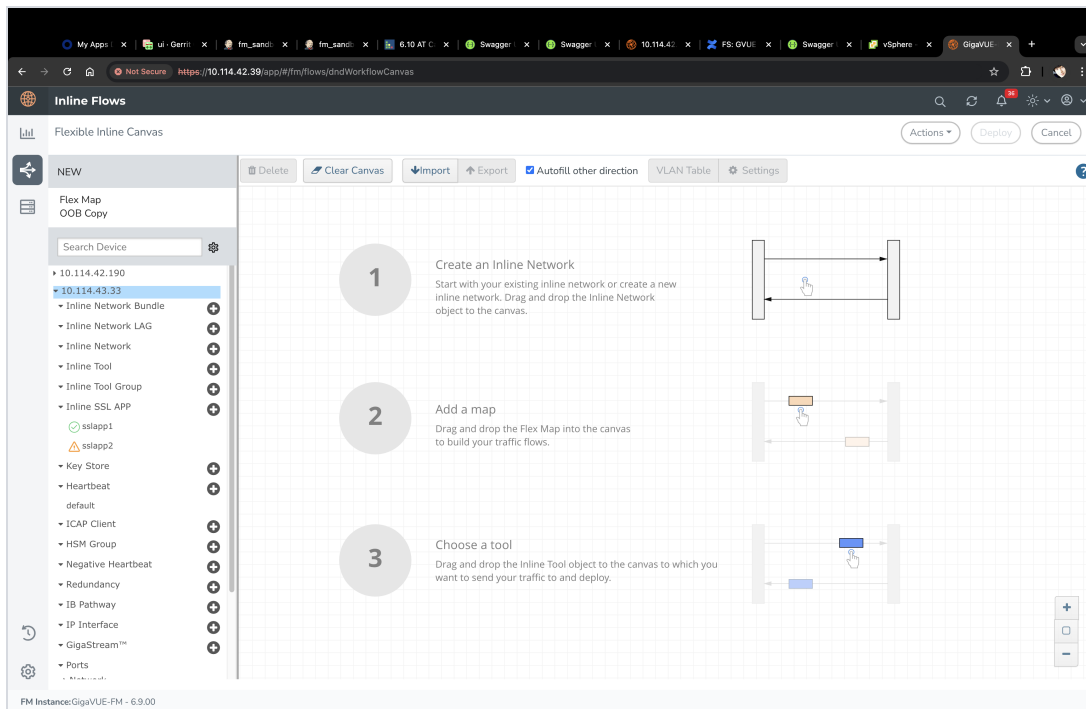


Figure 22  - Connection is a Success,  - Connection is ; Authentication Failure or Domain Name Lookup Failure or Connection Failure or Internal Error or Disabled

Proxy Server Profile Limitations

The following are limitations while configuring Proxy Server Profile:

- Access to only HTTP proxy servers are supported.
- This feature is not available on Gen 2 devices.

- This feature is compatible only with IPv4 proxy servers.
- Other GigaSMART applications, such as HSM or Application Intelligence, that utilize the GigaSMART engine port will not adhere to proxy settings.
- Migration of proxy servers from the device to GigaVUE-FM is not supported if the device is running version 6.8.xx.
- For Resilient Inline Arrangement, the proxy server option will only be displayed when both devices are running version 6.9.xx or higher.

Upgrade Considerations

- If a device upgrades from version 6.8.xx to 6.9.xx and has a proxy profile with an alias that already exists in GigaVUE-FM but with different configuration, an error will occur. The user will need to manually edit the configurations as necessary.
- If you upgraded your device from GigaVUE-OS version 6.8.xx to 6.9.xx, the Proxy Server profiles configured through GigaVUE-OS CLI will be migrated to GigaVUE-FM. However, you will need to reconfigure your password in GigaVUE-FM if you intend to use this proxy server profile in a new solution. Any existing solutions will be migrated successfully along with the password.

Split DNS Configuration

The Split DNS configuration page enables users to create Split DNS profiles. Split Domain Name System (Split DNS) functionality enables the use of different DNS servers for internal and external networks, enhancing security and privacy by preventing the same domain name server from being used for resources accessible both internally and externally.

Supported Platforms

Split DNS Profile can only be associated with GigaVUE HC Series Gen 3 and Gen 2 modules of the following devices:

- GigaVUE-HC1
- GigaVUE-HC1-Plus.
- GigaVUE-HC3.

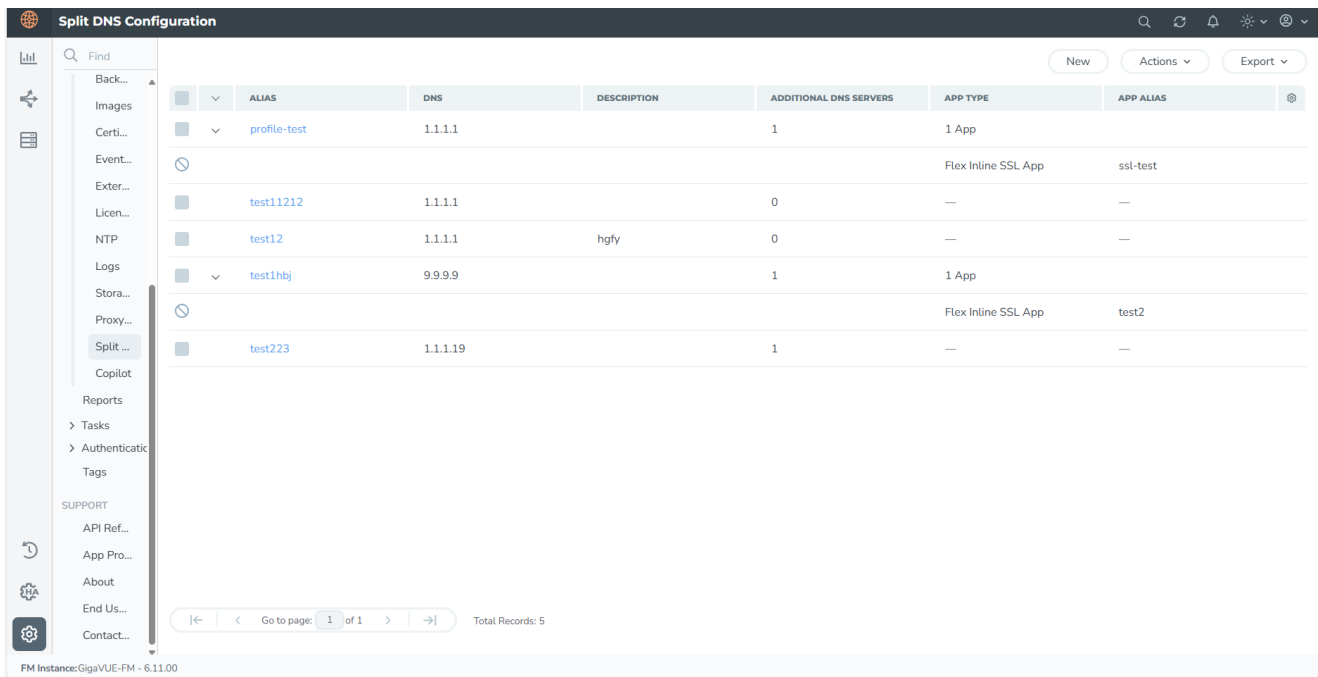
Configure Split DNS Profile

1. Go to **Settings>Setting> Split DNS Configuration > New**. Configure the following field attributes:
 - **Alias**- This is the DNS server profile alias. Once configured, this field cannot be modified.
 - **Default DNS Server**- The default DNS Server is the collector DNS server which would resolve domain names if none of the domains in additional DNS server matched. Configure the Default DNS Server profile by providing the following details:
 - **DNS**- Enter the DNS server address
 - **Description** - Enter a description for the DNS server Profile.

- **Additional DNS Servers**-This is an optional configuration. Import or add manually other internal DNS Servers to be queried based on domain name. To import an additional DNS server configuration, upload or drop the XLS or XLSX configuration file. While adding the additional DNS Server manually enter the following:
 - **DNS**- Enter the DNS server address
 - **Description** - Enter a description for the DNS server Profile.
 - **Domain**- .Domain name for which the DNS server needs to be used.
- 2. Click on **Save**.

A new Split DNS Server profile can also be created from the Inline SSL app configuration page (from the left navigation pane, go to **Physical > Orchestrated Flows > Inline Flows> Inline SSL APP**) by using the '**Create new Split DNS**' button. The created Split DNS Profiles will be listed and managed under the  **Setting> Split DNS Configuration>Split DNS Configuration** page.

The configured Split DNS Server profile is maintained in GigaVUE-FM and is not attached to a node until explicitly done so through an Inline SSL deployment.



ALIAS	DNS	DESCRIPTION	ADDITIONAL DNS SERVERS	APP TYPE	APP ALIAS
profile-test	1.1.1.1		1	1 App	
test11212	1.1.1.1		0	Flex Inline SSL App	ssl-test
test12	1.1.1.1	hgfy	0	—	—
test1hbj	9.9.9.9		1	1 App	
test223	1.1.1.19		1	Flex Inline SSL App	test2

Editing a Split DNS Profile

To edit an existing Split DNS Server Profile

1. Go to **Settings>Setting> Split DNS Configuration**.
2. Select the Split DNS Server profile that you want to edit and click on the **Actions> Edit**, the edit Split DNS Server profile page appears.

3. You can edit all attributes of your profile, except for the Alias.
4. Click on **Apply** to save your changes.

Any edits made to the Split DNS Server Profile will also be reflected in the associated Inline SSL Solution.

Delete a Split DNS Server Profile

To delete an existing Split DNS Server profile:

1. Go to **Settings>Setting>Split DNS Server Configuration**.
2. Select the Split DNS Server profile that you want to edit and click on the **Actions>Delete**. The Split DNS Server profile is deleted.

NOTE: If your Split DNS Server profile is associated with an Inline SSL application, you will not be allowed to delete and an error for the same will be thrown.

Configure Split DNS Server Profile in an Inline SSL Deployment

To successfully attach a Split DNS Server profile to the Inline SSL Deployment, follow the below steps:

1. Go to  > **Physical > Orchestrated Flows > Inline Flows > Configuration Canvas Inline Flows**.
2. Select the required device with your configured flexible inline decryption solution.
3. Click the '+' icon next to the **Inline SSL APP** option to create a new flexible inline decryption solution or to open the configured solution.
4. Under **Network Access** section, select the **Split DNS** option. From the drop-down select Split DNS Server profiles for each of your GigaSMART engines. Refer [Inline SSL APP—Field References](#) in GigaVUE Fabric Management Guide for details.
5. Click on **OK** to save your configurations. You can assign the configured Split DNS Server profile to each of your GigaSMART engines.

Tasks

The Tasks page provides access to the Admin Tasks and Scheduled Tasks pages. The Admin Task page displays any administrative tasks waiting to occur on the nodes managed by GigaVUE-FM. The Scheduled Tasks page displays the scheduled reoccurring task on the nodes

This section covers the following topics:

- [Admin Tasks](#)
- [Scheduled Tasks](#)

Admin Tasks

Currently, the only tasks that can be scheduled are node image installs, node upgrades, and node reboots. Once a task listed in this table executes, it also appears in the Events list.

Go to **Settings**, to view the **Admin Tasks** and click **Tasks**.

Admin Tasks								Delete	Filter
Total Tasks : 2 Filtered By : none									
☐	Name	Type	Status	Node Summary	Start Time	End Time	Log		
☐	FM Upgrade	ImageInstall	Success	-	2019-12-16 17:06:00	-	-		
☐	FM Upgrade	ImageInstall	Success	-	2019-11-27 12:11:00	-	-		

Figure 23 Admin Tasks Page

The Admin Tasks page displays the following information:

Parameters	Description
Name	The name of the task.
Type	The type of task that is scheduled, for example, Node Reboot .
Status	The status of the task. They are In Progress , Success , or Failure .
Node Summary	The total number of nodes available in the clusters. Click Details to view the post upgrade sanity check of all the available configuration objects in the cluster. For more information, refer to View the Upgrade Sanity Check .
Start Time	The start time of the scheduled task.
End Time	The end time of the scheduled task. IMPORTANT: Timestamps are shown in the time zone of the client browser's computer and not the timezone of the node where the task is scheduled. The timestamp is based on the correctly configured clock on the GigaVUE-FM server and converted from UTC to the client computer's configured timezone.
Log	The log records every step performed with the timestamps. Click Log for a detailed view of every step that occurred during the upgrade process. Refer to View the Upgrade Sanity Check .

NOTE: Click the heading cell of any column to sort the field values based on that attribute. However, if you try to sort based on **Start Time** or **End Time** columns, then it might not fetch accurate results (as the fields are not populated for older records).

View the Upgrade Sanity Check

The information in the Node Summary Details page is grouped based on clusters. Each cluster displays the configuration objects and their state before and after the upgrade. For example, if cards are down after the upgrade, the number of cards that are down are displayed in the Result column. Click the number to view more details about the cards that are down.

To view the upgrade sanity check:

1. Go to **Settings** select **Tasks**.
2. In the Admin Tasks page, click the Detail link in the Node Summary column. Refer to [View the Upgrade Sanity Check](#).
3. In the Result column, click the number and view the detailed information about the configuration objects.

Delete an Admin Task

To delete a scheduled task from the Admin Tasks, do the following:

1. Go to **Settings** select **Tasks**.
2. From the Admin Tasks page, select a task from the list.
3. Click **Delete**.

The task is unscheduled and stopped from happening.

Scheduled Tasks

The Scheduled Tasks page displays tasks that have been set to reoccur at scheduled times. Currently, the only tasks that can be scheduled are device backups, GigaVUE nodes upgrade, and GigaVUE-FM configuration data.

Schedule					
Filtered By : none					
☐	Name	Type	Scheduled Time	Due In	Recurrence
No Records Found					

Figure 24 Scheduled Tasks Page

The Scheduled Task page displays the following information.

Parameters	Description
Name	The name of the scheduled task.
Type	The type of the scheduled task.
Scheduled Time	The timestamp when the task is scheduled to begin.
Due In	The time left for the scheduled task to begin.
Recurrence	The frequency of the scheduled task. For example, daily at 4 hours 35 minutes.

Delete a Scheduled Task

To reschedule a task, do the following:

1. Go to **Settings** select **Tasks > Scheduled Task**.
2. Select a task from the list.

The task is either a configuration data backup of GigaVUE-FM (FMServerConfigBackUp) or a backup of a device (configBackup).

3. Click **Delete**.

Clicking Delete unschedules and stops the task from happening.

Reports

The Reports page displays the lists of reports generated, allows you to generate new reports, download reports and delete reports that you no longer need. You can also export the reports generated in CSV and XLSX.

The screenshot displays the 'Reports' page in the GigaVUE-FM interface. The page has a dark header with the title 'Reports' and a search bar. Below the header, there is a sidebar with navigation options: SETTINGS (System, Tasks, Reports, Authentication, High Availability, Tags), SUPPORT (API Reference, App Protocols, About, Contact Support), and a Refresh button. The main content area shows a table of reports with the following data:

Report Name	Creation Date	Created By
gigamon_GigaVBL_20220313024712_admin.pdf	2022-03-13 08:17:12	admin
gigamon_physical_inv_20220218070110_admin.pdf	2022-02-18 12:31:10	admin
gigamon_GigaVBL_20220113000531_null.pdf	2022-01-13 05:35:31	null

At the top right of the table, there are buttons for 'Generate New', 'Download', 'Delete', and 'Export'. At the bottom of the page, there is a pagination bar that says 'Go to page: 1 of 1' and 'Total Records: 3'.

Refer to the following sections for details:

- [Overview of Reports](#)
- [Generate Reports](#)
- [NetFlow Format Support on Exporters](#)

Overview of Reports

The Reports page allows you to create the following types of reports:

- [GigaSMART Performance Report](#) provides a summary of GigaSMART performance for all GigaVUE HC Series nodes with GigaSMART functionality.
- [Visibility Fabric Inventory Report](#) provides a summary of all physical inventory (includes GigaVUE HC Series and GigaVUE TA Series) that is visible on GigaVUE-FM.
- [Visibility Fabric Node Details Report](#) provides specific details relating to the physical nodes (includes GigaVUE HC Series, GigaVUE TA Series).
- [Visibility Fabric Performance Report](#) provides traffic analysis information.
- [Volume Based License Usage Reports](#) provides volume based license usage report.

Generate Reports

To generate reports:

1. Go to **Settings** to view the Reports page.
2. Select **Reports**, and click **Generate New**.

NOTE: You must have the GigaVUE-FM Prime License installed for the Report functionality to work.

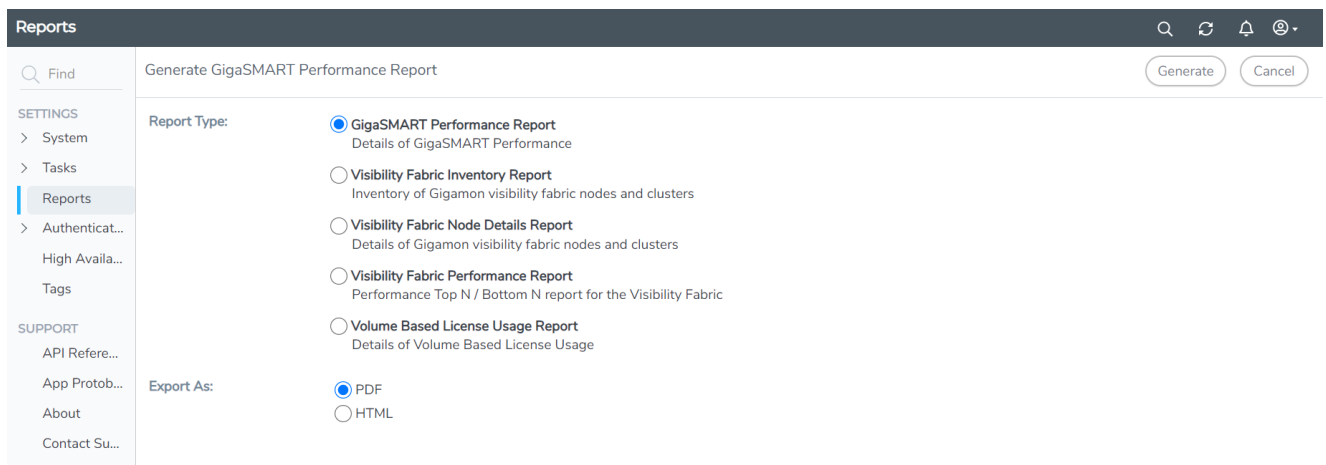


Figure 25 Reports Page View

You can download the reports in PDF or HTML format to your local drive.

- Only one report can be selected for each generate and download option.

- The report layout and format is not customizable.
- Reports can be stored or deleted in GigaVUE-FM.
- Reports are polled live and therefore can change each time they are generated.
- Each report appears with the timestamp on when the report was generated.

To view the reports directly from the GigaVUE-FM settings, ensure that the pop-up blocker settings on your browser is disabled. This allows you to view the reports without downloading. The reports will be available on a separate page.

Visibility Fabric Performance Report

This multi-page report provides you with printable format for Traffic analysis including:

- Top N / Bottom N Ports
- Top N / Bottom N Traffic Maps
- Overlay Traffic Maps / Ports
- Top N / Bottom N VM rule stats
- Top N/ Bottom N Logical Network stats

[Figure 26Visibility Fabric Performance Report](#) shows an example of a report for Visibility Fabric Performance.

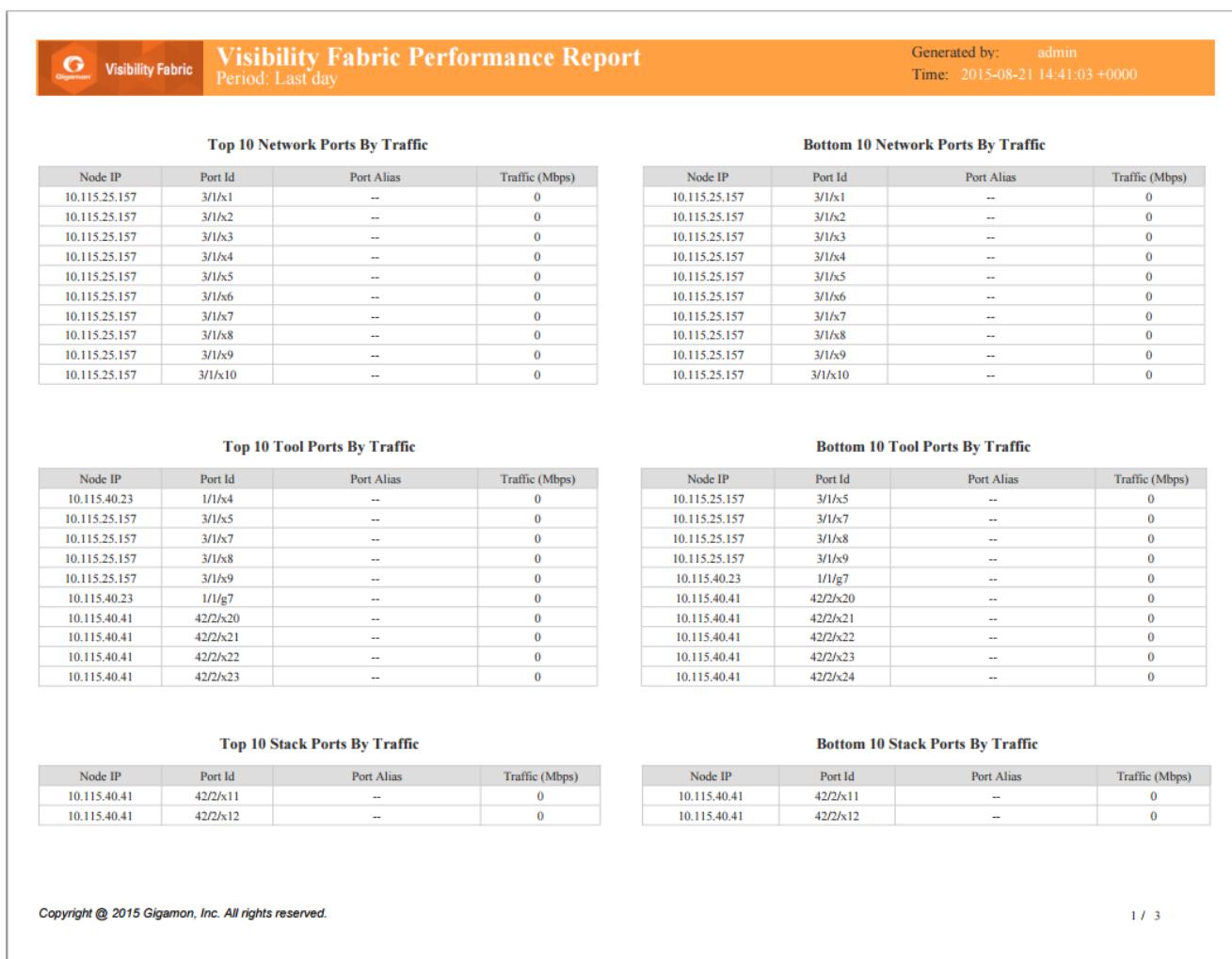


Figure 26 Visibility Fabric Performance Report

Visibility Fabric Node Details Report

This multi-page report provides you with printable format for specific details relating to the Physical Nodes (includes GigaVUE HC Series and GigaVUE TA Series) similar to what you would see under Chassis/Device pages. The report includes:

- Pie Chart of total Nodes, total (collective) ports and card types (collective)
- Table format showing each Node associated with this instance of GigaVUE-FM
- Detailed report similar to as shown on Chassis Page including clustered nodes

[Figure 27 Inventory Details Report](#) shows an example of a report for Visibility Fabric Node Details.

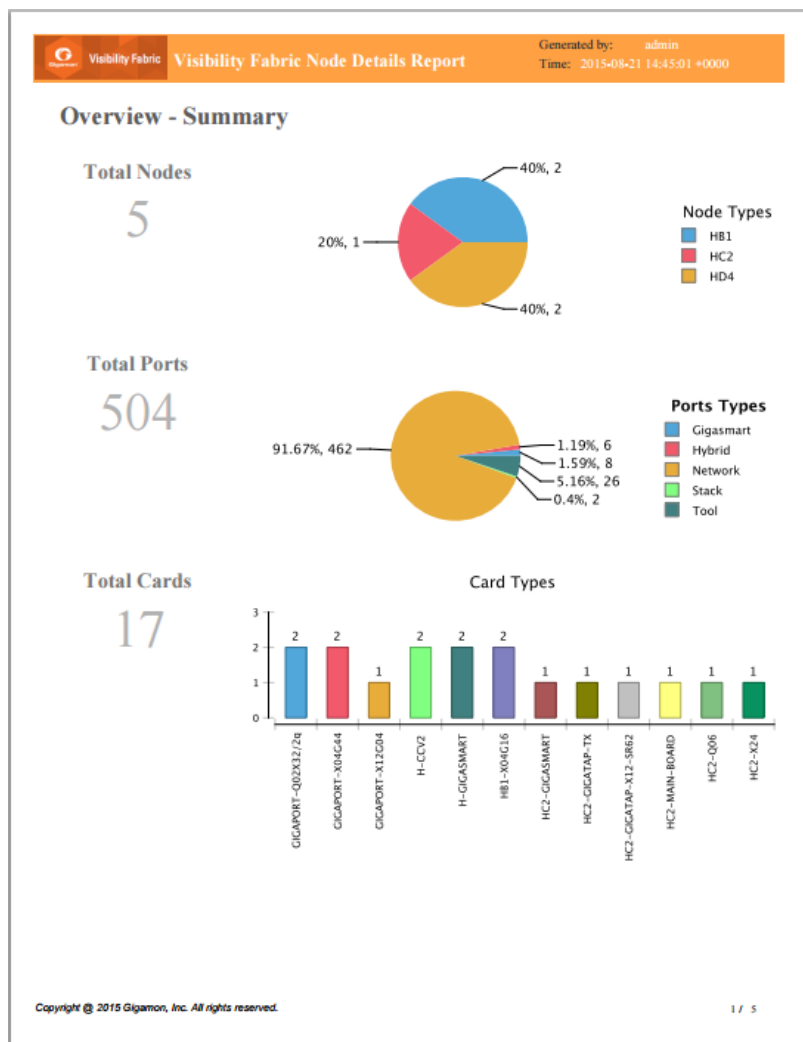


Figure 27 Inventory Details Report

Template 3: GigaVUE-VM Report

This multi-page report provides you with printable format for GigaVUE-VM traffic analysis including:

- Summary of GigaVUE-VM virtual centers
- Details on the virtual centers
- Top N / Bottom N Ports
- Top N / Bottom N Traffic Maps

Figure 28 Report Pages Available for GigaVUE-VM show an example of a report for GigaVUE-VM.

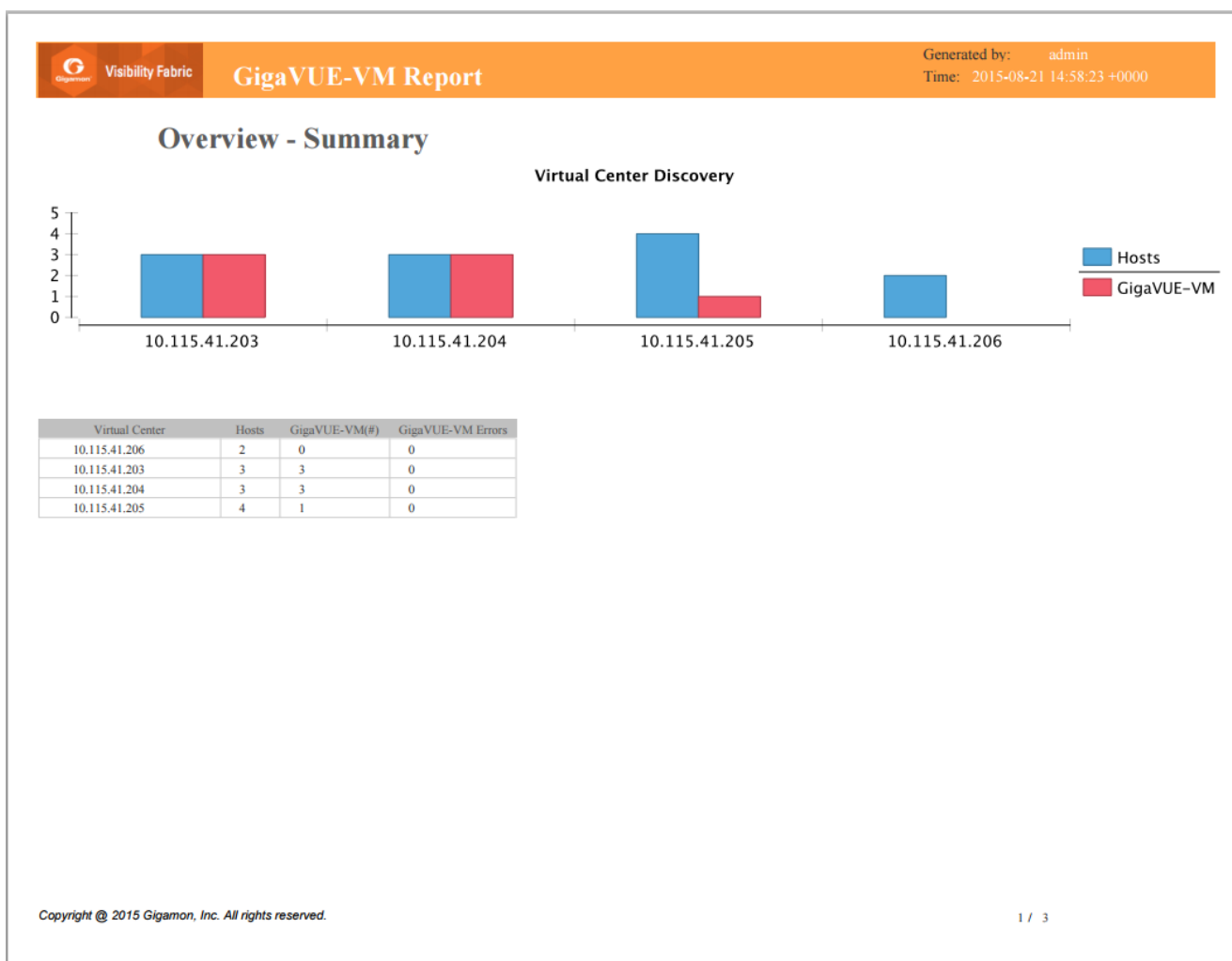


Figure 28 Report Pages Available for GigaVUE-VM

Visibility Fabric Inventory Report

This multi-page report provides you with printable format of summary on all your Physical inventory (includes GigaVUE HC Series and GigaVUE TA Series) that is visible on that GigaVUE-FM.

- Pie chart format for Status, Cluster Status, Node Types, Network and Tool Port Status and SW Versions.
- Table Format with all the Device IP with associated parameters such as Model, Status, Box ID, SW Version, Serial #, and so on.

Figure 29 [Inventory Summary Report](#) show an example of a report for Visibility Fabric Inventory.

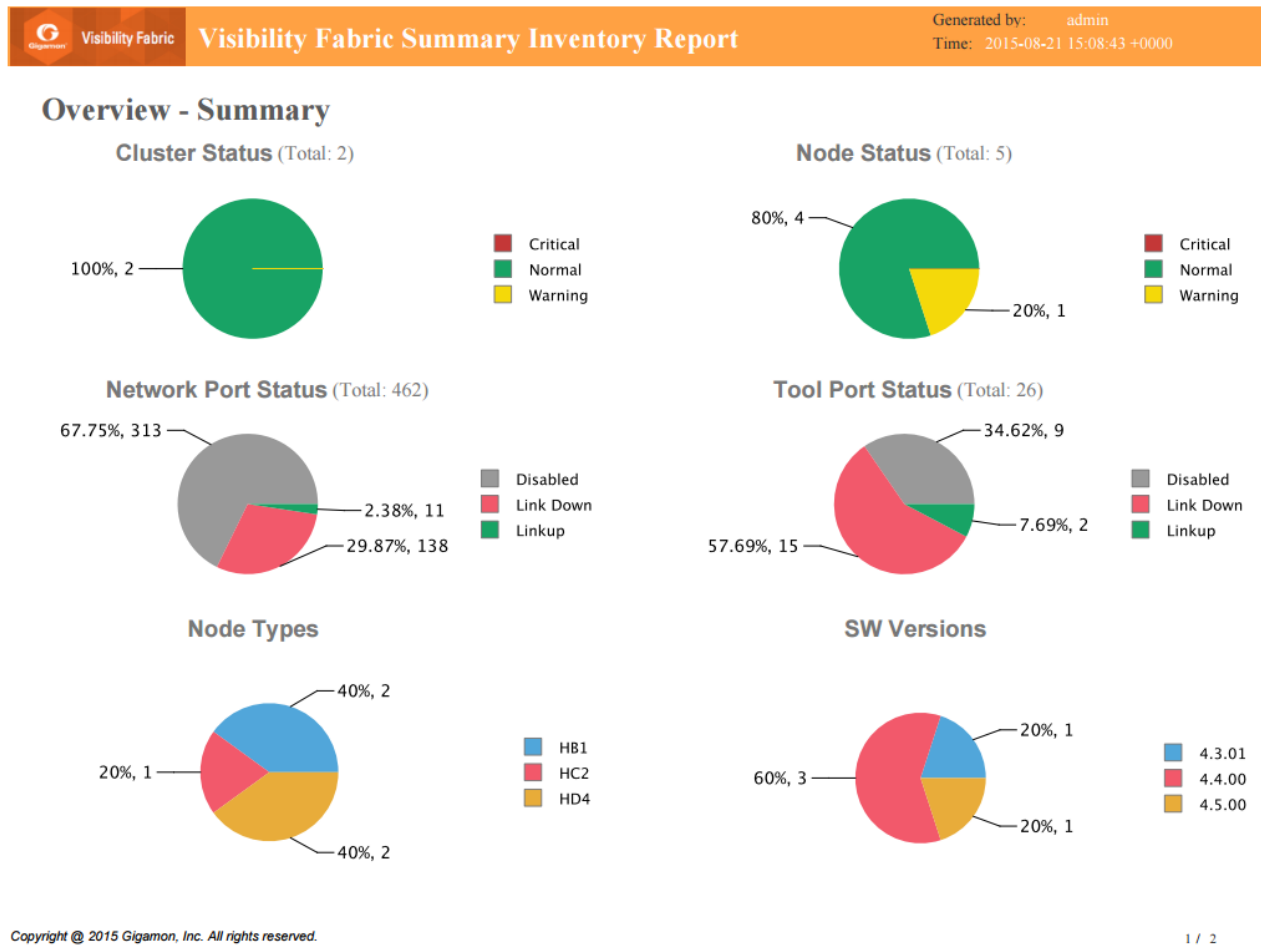


Figure 29 Inventory Summary Report

GigaSMART Performance Report

This report provides you with printable format of summary on GigaSMART performance for all GigaVUE HC Series nodes with GigaSMART functionality.

The report includes GigaSMART statistics for the following:

- Top/Bottom 10 GigaSMART (GS) Groups by Traffic: This information will indicate which GS groups are heavily utilized. To ensure to capture all the relevant information it is good to have the GS groups be description in the GS Groups alias names.
- Top/Bottom 10 GigaSMART (GS) Operations by Traffic: This information will indicate which GS operations are heavily utilized. To ensure to capture all the relevant information it is good to have the GS Operations be description in the GSOP alias names.
- Top/Bottom 10 GigaSMART (GS) Virtual Ports by Traffic: This information will indicate which virtual ports might be over-utilized and which are under-utilized.

Figure 30 Report for GigaSMART Performance Indicators show an example of a report for GigaSMART Performance.

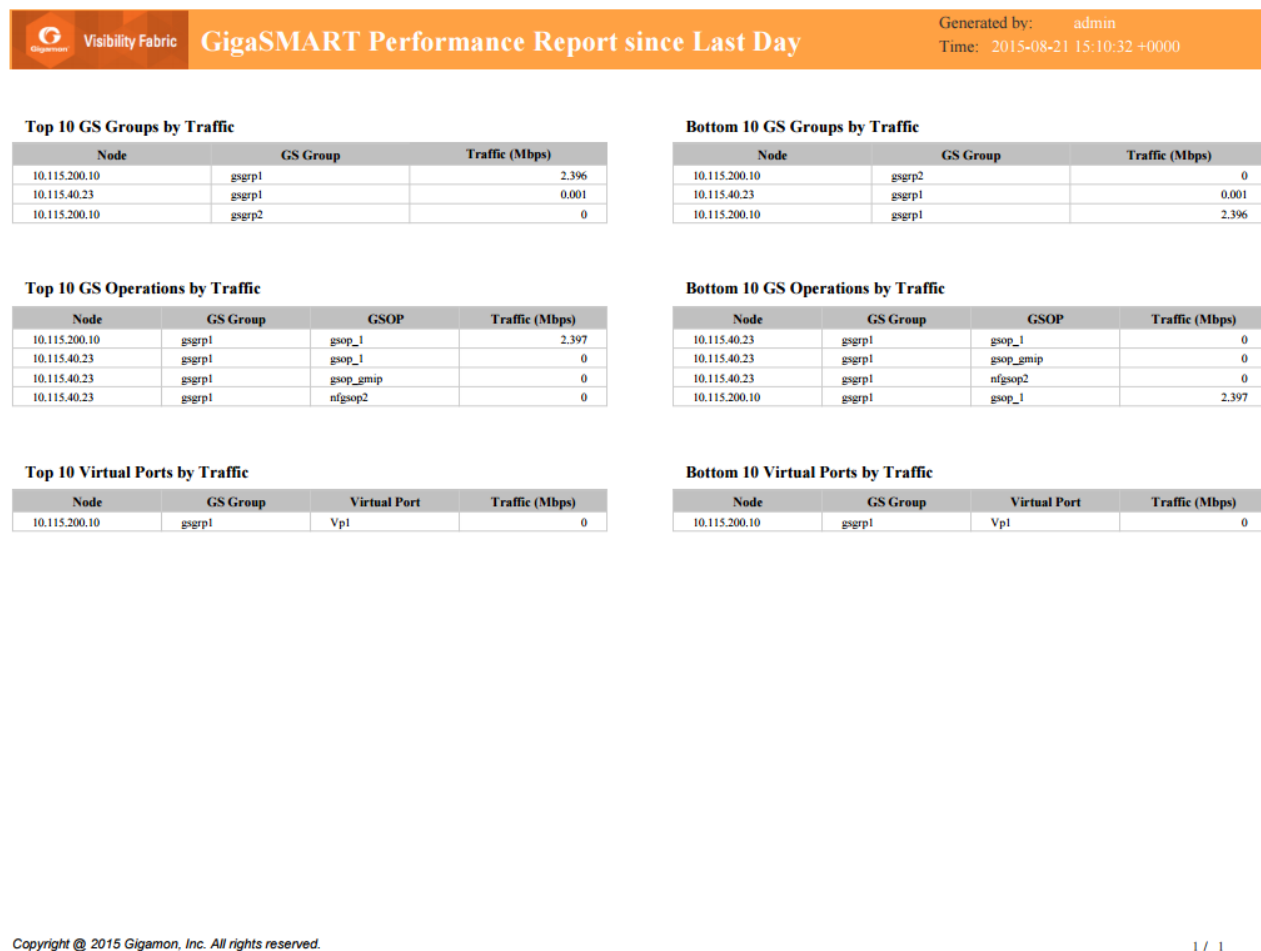


Figure 30 Report for GigaSMART Performance Indicators

Volume Based License Usage Reports

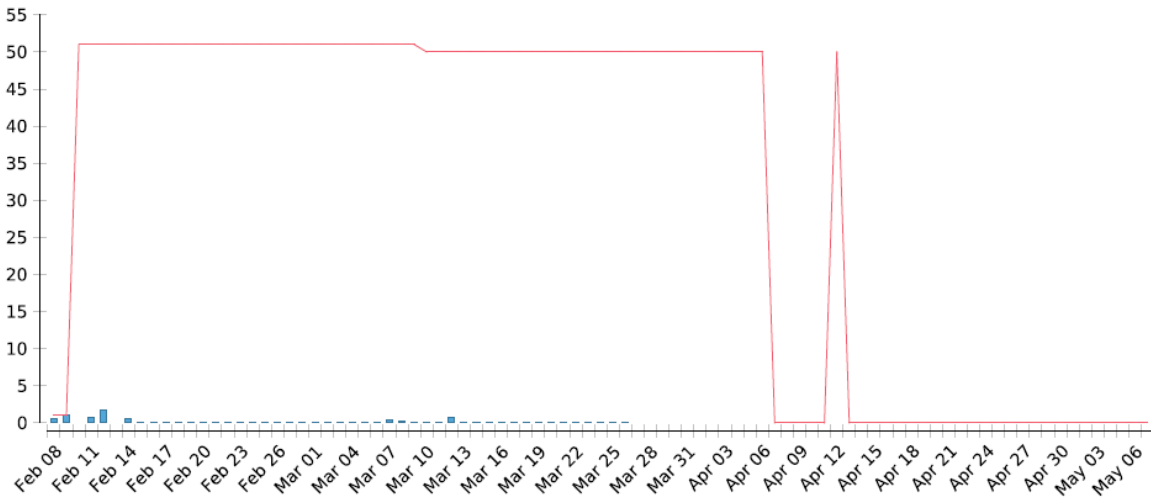
The Volume-based License Usage report is a multipage report in PDF format. The VBL Usage report contains sections for the incoming traffic (raw usage) and all license bundles that are active during the period of the report.

Section	Details
Volume Usage: Summary	• Period: Period for which the volume usage summary is displayed. • Days Completed: • Licensed Daily Volume: • Peak Daily Volume: • 95th Percentile Daily Usage: • The 95th percentile daily usage for any day is calculated as follows: the daily usage for the trailing 90 days, including and up to the current day, are sorted in ascending order and the usage at the 95th percentile (near the high end) is reported as the 95th percentile usage for the day. This aggregate statistic uses the maximum of the 95th percentile usage for the days in the Service Period. NOTE: The reason is to find the high-end usage disregarding exceptionally high values that are outliers (happening due to some extraordinary condition prevailing on the day), and hence not representative of the normal high end usage values.
Daily Usage	Graph that displays the daily usage details.
Tabular format of the volume usage details	Each section contains up to four pages. The first page contains a summary and a chart (with allowance as line chart and usage as bar chart) and the subsequent pages contain the allowance, usage and overage data for each day in the period. For example, if GigaVUE-FM has CoreVUE and NetVUE bundles imported, then report has the following sections: • First four pages: Raw ingress traffic • Next four pages: CoreVUE bundle • Last four pages: NetVUE bundle

The following figure shows an example for the Volume Based License Usage report.

Volume Usage: Summary

Period: Feb 8, 2022 - May 7, 2022
 Days Completed: 64
 Licensed Daily Volume: 51.00 TB
 Peak Daily Volume: 1.66 TB
 Days exceeding Licensed Daily Volume: 1
 95th percentile Daily Usage: 0.74 TB

Daily Usage

Copyright © 2020 Gigamon, Inc. All rights reserved.

1 / 4

 Visibility Fabric V-Series Volume Usage Report DO NOT TOUCH (Gimo Internal Account - To be used by Engineering license Generated by: admin on Apr 13, 2022 POSID: FM VMAC: 00:50:56:a0:0d:f5			
Date	Licensed Daily Volume	Usage	Overage
Feb 08, 2022	1.00 TB	0.58 TB	0.00 TB
Feb 09, 2022	1.00 TB	1.14 TB	0.14 TB
Feb 10, 2022	51.00 TB	0.00 TB	0.00 TB
Feb 11, 2022	51.00 TB	0.74 TB	0.00 TB
Feb 12, 2022	51.00 TB	1.66 TB	0.00 TB
Feb 13, 2022	51.00 TB	0.00 TB	0.00 TB
Feb 14, 2022	51.00 TB	0.54 TB	0.00 TB
Feb 15, 2022	51.00 TB	0.11 TB	0.00 TB
Feb 16, 2022	51.00 TB	0.15 TB	0.00 TB
Feb 17, 2022	51.00 TB	0.10 TB	0.00 TB
Feb 18, 2022	51.00 TB	0.10 TB	0.00 TB
Feb 19, 2022	51.00 TB	0.10 TB	0.00 TB
Feb 20, 2022	51.00 TB	0.09 TB	0.00 TB
Feb 21, 2022	51.00 TB	0.10 TB	0.00 TB
Feb 22, 2022	51.00 TB	0.10 TB	0.00 TB
Feb 23, 2022	51.00 TB	0.13 TB	0.00 TB
Feb 24, 2022	51.00 TB	0.12 TB	0.00 TB
Feb 25, 2022	51.00 TB	0.10 TB	0.00 TB
Feb 26, 2022	51.00 TB	0.10 TB	0.00 TB
Feb 27, 2022	51.00 TB	0.13 TB	0.00 TB
Feb 28, 2022	51.00 TB	0.09 TB	0.00 TB
Mar 01, 2022	51.00 TB	0.10 TB	0.00 TB
Mar 02, 2022	51.00 TB	0.12 TB	0.00 TB
Mar 03, 2022	51.00 TB	0.10 TB	0.00 TB
Mar 04, 2022	51.00 TB	0.07 TB	0.00 TB

NetFlow Format Support on Exporters

NetFlow Exporters support versions IPFIX, v5, and v9. Starting in software version 5.3, the Common Event Format (CEF) version 23 is also supported. CEF is a standard format used by event collection/correlation Security Information and Event Management (SIEM) vendors. SIEMs such as Arcsight, Splunk, and QRadar accept CEF format. By supporting CEF, NetFlow metadata can integrate with and use a variety of SIEMs.

CEF is a logging format that uses the syslog message as a transport mechanism, meaning that the CEF message (header and payload) is included within the syslog message. The transport protocol that is supported is UDP and the default port number is 514.

Metadata that is generated by NetFlow can be exported in the supported formats to one or more collectors. Each exporter must have the same export type (v5, v9, IPFIX, or CEF). One CEF message is sent out per record per flow.

Also, starting in software version 5.3, IP fragmentation is supported. CEF does not allow a message to be split over multiple CEF payloads. Since CEF messages are verbose, they can be larger than the MTU.

To support CEF messages that exceed the MTU, a single IP datagram containing a CEF message will be broken up into multiple packets of smaller sizes. The reassembly of the datagram will occur at the receiving end (at the SIEMs).

For details on the CEF message format, refer to [CEF Message Format](#).

CEF Message Format

An example of the CEF message format is as follows:

```
Fri Feb 23 02:25:37 2018 9/3/e1
CEF:23|Gigamon|metadata|5.3.00|4|metadatageneration|6| src=68.94.156.1
GigamonMdataDnsAdditionalType=41GigamonMdataDnsAdditionalTypeText=OPT
```

In the example CEF message, there is a syslog header, a CEF header, and an extension that contains the CEF payload. The fields are delimited with a vertical bar (|).

The syslog header contains the following:

- timestamp—Fri Feb 23 02:25:37 2018
- host name identifier—9/3/e1

NOTE: The host name identifier has the format <box ID>/<slot ID>/<engine ID>. For example, 9/3/e1 means 9 is the box ID, 3 is the slot ID, and e1 is the engine ID.

The CEF header contains the following:

- version—CEF:23

- device vendor—Gigamon
- device product—metadata
- device version—5.3.00
- signature identifier—4
- name—metadata generation
- severity—6

The CEF extension contains key-value pairs delimited with a space. In the example CEF message, the following is the CEF payload, in plaintext:

- src=68.94.156.1
- GigamonMdataDnsAdditionalType=41
- GigamonMdataDnsAdditionalTypeText=OPT

The CEF standard specifies key-value pairs. There are some predefined standard keys, for example, src is a predefined key for source IP address.

For keys that are not predefined in the CEF standard, such as the NetFlow metadata elements in the CEF extension, there are custom-defined keys. Custom-defined keys have the following format:

- <VendorNameProductNameExplanatoryKeyName>

For example, GigamonMdataDnsAdditionalTypeText, is a custom-defined key that contains the following:

- VendorName—Gigamon
- ProductName—Mdata
- ExplanatoryKeyName—DnsAdditionalTypeText

Another example of the CEF format is the following SSL record:

```
Thu Mar 1 08:21:28 2018 1/1/e1 CEF:23|Gigamon|metadata|5.3.00|4|metadata
generation|6|GigamonMdataSslIssuerName=DigiCert SHA2 High Assurance S
dpt=54839 GigamonMdataSslValidNotBefore=31373031303630303030305a
GigamonMdataSslSerialNo=0118ee3c2167b99e1b718c6eadb8fb4d00000000
GigamonMdataSslValidNotAfter=3230303131353132303030305a
GigamonMdataSslCertSigAlgo=2a864886f70d01010b
GigamonMdataSslCertSubAlgo=2a864886f70d010101
GigamonMdataSslCertSubKeySize=270 GigamonMdataSslServerVersion=771
GigamonMdataSslCertSubAltName=*.stickyadstv.com
GigamonMdataSslServerCompressionMethod=192 GigamonMdataSslServerCipher=49199
GigamonMdataSslServerVersionText=TLSv1.2 GigamonMdataSslServerSessionId=63
GigamonMdataSslIssuer=2f433d55532f4f3d446967694365727420496e632f4f553d7777772
e6469676963
6572742e636f6d2f434e3d446967694365727420534841322048696768204173737572616e636
52053657276 6572204341 GigamonMdataSslCertSubCommonName=*.stickyadstv.com
GigamonMdataSslSub=2f433d55532f53543d4e657720596f726b2f4c3d4e657720596f726b2f
4f3d4672656
```

5776865656c204d6564696120496e632f4f553d46726565776865656c2f434e3d2a2e737469636b796164737 4762e636f6d dst=10.50.22.59 src=38.106.34.118

Configure Security Options

This chapter describes how to set options relating to security – who can log into the node, how they are authenticated, and what rights they have once logged in.

The chapter includes the following sections:

Topic	Refer to...
About Role-Based Access	About Role-Based Access
Configure Authentication and Authorization	Configure Authentication Type
Default Ports	Open Ports in GigaVUE-FM in the GigaVUE-FM User's Guide
Default Mode	Default Mode
FIPS 140-3 Compliance	Are all versions of GigaVUE-FM validated for FIPS compliance?
USGv6r1 Compliance	USGv6 Compliance
Cryptography Mode	Enable Cryptography Mode
Validation of Certificate Revocation List	Enable Validation of Certificate Revocation List
Network Audit Logs	Enable Network Audit logs

Default Mode

GigaVUE-FM operates in its default mode immediately after a fresh installation. It supports the commonly-supported TLS 1.2 and TLS 1.3 ciphers. The following ciphers are supported in TLS 1.2:

Enabled TLS Cipher Suites

Supported TLS 1.2 Ciphers

Cipher Name	Key Exchange (Kx)	Authentication (Au)	Encryption (Enc)	MAC
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	ECDSA	AES256-GCM	SHA384
ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE	ECDSA	AES128-GCM	SHA256
ECDHE-ECDSA-AES256-SHA384	ECDHE	ECDSA	AES256	SHA384
ECDHE-ECDSA-AES128-SHA256	ECDHE	ECDSA	AES128	SHA256

SSH Supported Algorithms

GigaVUE-FM supports the following SSH algorithms:

Category	Supported Algorithms
KexAlgorithms	ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, kex-strict-s-v00@openssh.com
HostKeyAlgorithms	ecdsa-sha2-nistp384
Ciphers	aes256-ctr, aes128-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com
MACs	hmac-sha2-512, hmac-sha2-256

FIPS Compliance in GigaVUE-FM

GigaVUE-FM is compliant with the Federal Information Processing Standard (FIPS), a US government standard for security requirements of cryptographic modules. The FIPS module used in GigaVUE-FM is compliant with FIPS 140-3 and was validated by the National Institute of Standards and Technology (NIST). The certificate number is 4912. For more information, refer to [Cryptographic Module Validation Program – Certificate 4912](#).

Refer to the following sections for details:

Rules, Notes and Limitations

Refer to the following rules and notes for FIPS:

- After upgrading GigaVUE-FM instance from pre 5.16.00 to 5.16.00 or above, GigaVUE-FM boots in non-FIPS mode.
- FIPS is disabled by default in GigaVUE-FM. You can enable FIPS whenever needed. However, once enabled you cannot disable it.
- Only users with super admin privileges can enable FIPS.

Refer to the Frequently Asked Questions section for further details.

Configure FIPS in GigaVUE-FM

To configure FIPS in GigaVUE-FM:

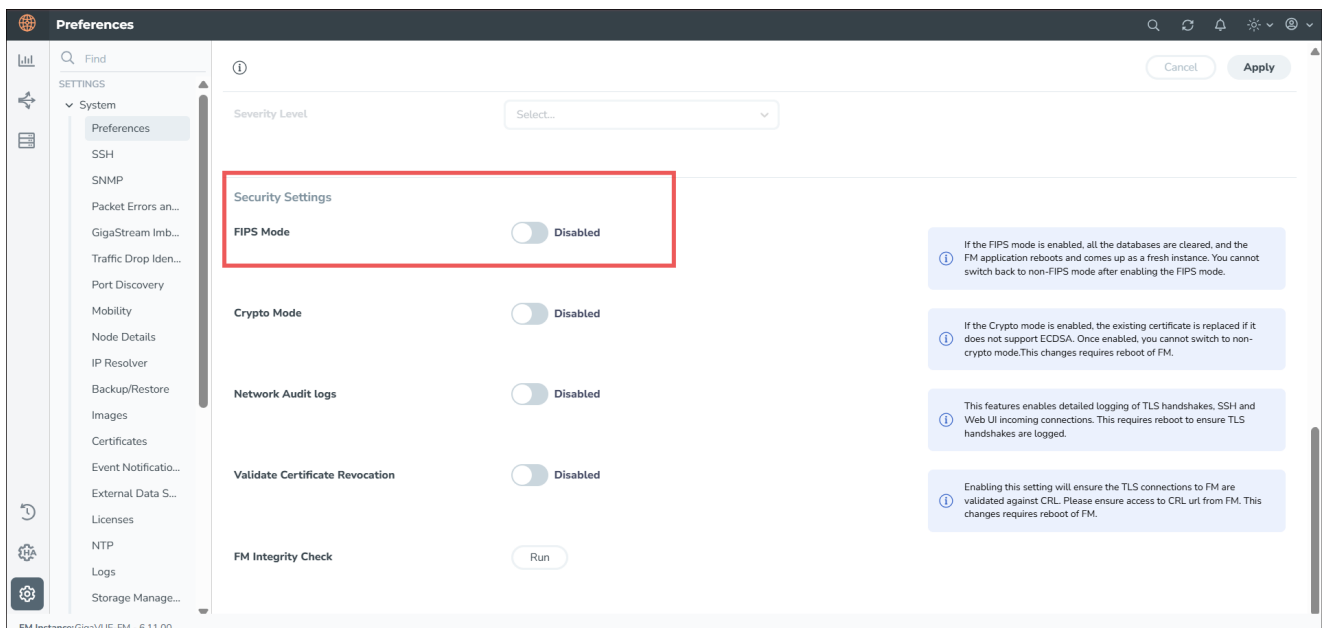
1. Go to **Settings** and go to **System > Preferences**.
2. Under **Security Settings**, enable the **FIPS Mode**.

NOTE:

- Do not enable FIPS Mode and Crypto Mode in the same request. Enable FIPS Mode first.
- After the system restarts, enable Crypto Mode in a separate request.

3. Click **Apply** to save the changes.
4. GigaVUE-FM will restart automatically after switching to FIPS Mode. Once the reboot completes, clear your browser cache and cookies to ensure the GigaVUE-FM IDP URL loads correctly.

NOTE: Once enabled, the toggle button is disabled. You cannot switch back to non-FIPS mode.



Configure FIPS in GigaVUE-FM High Availability Group

To form a FIPS enabled High Availability (HA) group:

- Enable FIPS in each of the standalone GigaVUE-FM instances.
- Assemble the HA group with FIPS enabled standalone GigaVUE-FM instances.

NOTE: You cannot add a GigaVUE-FM instance that is not FIPS enabled to a FIPS enabled High Availability group. Similarly, you cannot add a FIPS-enabled GigaVUE-FM instance to a High Availability group that is not FIPS enabled.

Enabled TLS Cipher Suites

GigaVUE-FM supports the commonly-supported TLS 1.2 and TLS 1.3 ciphers. The following ciphers are supported in TLS 1.2:

Supported TLS 1.2 Ciphers

Cipher Name	Key Exchange (Kx)	Authentication (Au)	Encryption (Enc)	MAC
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	ECDSA	AES256-GCM	SHA384
ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE	ECDSA	AES128-GCM	SHA256
ECDHE-ECDSA-AES256-SHA384	ECDHE	ECDSA	AES256	SHA384
ECDHE-ECDSA-AES128-SHA256	ECDHE	ECDSA	AES128	SHA256

Frequently Asked Questions

This page lists some of the most common issues and question related to FIPS.

Are all versions of GigaVUE-FM validated for FIPS compliance?

GigaVUE-FM versions 5.12.00.01 and 5.16.00 through 6.11 are compliant with FIPS 140-2. GigaVUE-FM version 6.11.01 and later are compliant with FIPS 140-3.

Can you enable FIPS using the fmctl command?

No. There is no support for enabling FIPS using the `fmctl` command. You can enable FIPS only using the GigaVUE-FM GUI.

Can you add a device that is not FIPS-compliant to a FIPS enabled GigaVUE-FM?

Yes. You can add a non FIPS compliant device to a FIPS enabled GigaVUE-FM.

What happens to the GigaVUE-FM database after you enable FIPS?

The GigaVUE-FM database is reset. GigaVUE-FM reboots and comes up as a new instance. You must reconfigure and setup GigaVUE-FM again.

How do I perform backup and restore operation on a FIPS enabled GigaVUE-FM?

A backup taken on a FIPS enabled GigaVUE-FM can only be restored on a GigaVUE-FM instance that is FIPS enabled. Similarly, backup taken on a non-FIPS GigaVUE-FM can be restored only on a non FIPS GigaVUE-FM.

Is the FIPS certification applicable for GigaVUE-FM instance irrespective of where it is deployed?

No. GigaVUE-FM Hardware appliance is only validated for FIPS certification.

STIG Compliance in GigaVUE-FM

A newly installed GigaVUE-FM contains several enhancements which significantly improve the STIG compliance of a new GigaVUE-FM instance. These enhancements are part of the default configuration. Key features include enhanced authentication, access controls, and encryption protocols.

The version of the STIG used is DISA STIG for Red Hat Enterprise Linux 8 V2R2.

These enhancements are designed to strengthen the security and reliability of GigaVUE-FM, ensuring that it meets stringent government and industry standards.

The following table lists the changes that directly impact the GigaVUE-FM CLI:

Rule ID	Changes made in GigaVUE-FM
SV-230295r1017106_rule	<code>/tmp</code> has been moved from the root filesystem into a separate filesystem. This change helps to preserve the integrity of the root filesystem.
SV-230513r958804_rule	Since <code>/tmp</code> is now a filesystem, the <code>noexec</code> mount option is set on the <code>/tmp</code> filesystem.
SV-237643r1050789_rule	Re-authentication is now required every time the <code>sudo</code> command is executed.
SRG-OS-000480-GPOS-00227	The setup procedure for authentication now uses the <code>authselect</code> tool and its <code>sssd</code> profile.
SV-230343r1017155_rule SV-230333r1017145_rule SV-230345r1017157_rule SV-230338r1017150_rule SV-230339r1017151_rule SV-230334r1017146_rule SV-230335r1017147_rule SV-230340r1017152_rule SV-230341r1017153_rule SV-230336r1017148_rule SV-230337r1017149_rule	The GigaVUE-FM CLI's behavior when an attempt at password authentication fails has been modified. Specifically, the CLI admin login will be locked for 10 minutes if there are three failed login attempts in a 15-minute window. After 10 minutes, the admin login is automatically unlocked. This 10-minute lock period was 5 minutes in previous GigaVUE-FM releases.

Rule ID	Changes made in GigaVUE-FM
SV-230359r1017171_rule SV-230377r1017188_rule SV-230363r1017175_rule SV-230358r1017170_rule SV-230360r1017172_rule SV-230361r1017173_rule SV-230362r1017174_rule SV-230369r1017181_rule SV-230375r1017187_rule SV-230356r982195_rule SV-251713r1017366_rule SV-251716r1017369_rule SV-230357r1017169_rule	Password complexity rules have been changed to provide a more secure password authentication experience. Specifically, to satisfy the following conditions: - o The cracklib dictionary is now used to screen well-known passwords so they can be rejected. - o At least eight of the characters used in a new password must not be present in the new password. - o The maximum run of repeated characters in a password must not exceed three. - o At least one character from each of the following categories must be present in a password: upper-case, lower-case, numeric and special. The minimum length of the password is 14.
SV-230378r1017189_rule	There is now a four second delay after password authentication fails. In previous GigaVUE-FM releases, the delay was three seconds.
SV-230346r1017159_rule	The maximum number of simultaneous admin users' CLI logins is now explicitly set to ten.
SV-230383r1017192_rule SV-230385r1017194_rule SV-230384r1017193_rule	The default unmask for the CLI admin user is explicitly set to 077.
SV-230485r1017269_rule	The chrony service is configured to operate strictly in a client-only mode.

Recommended STIG Compliance

The following table lists the additional changes that can be made further to increase the STIG compliance of an GigaVUE-FM instance:

Rule ID	Recommended Changes
xccdf_org.ssgproject.content_rule_banner_etc_issue	A generic <code>/etc/issue</code> is the default message is the default. Simple editing <code>/etc/issue</code> and replacing its contents with <code>/etc/issue.stig</code> will provide the required text and increase the STIG score.
xccdf_org.ssgproject.content_rule_accounts_password_pam_minlen	STIG requires a minimum password length of 15 characters. This is a disruptive change for Gigamon deployments since they have all enforced a 14-character minimum length for several years. Edit the file <code>/etc/security/pwquality.conf</code> and change the value 14 to 15 on the minlen line.

Rule ID	Recommended Changes
xccdf_org.ssgproject.content_rule_accounts_password_minlen_login_defs	The STIG requires a minimum password length of 15 characters. This is a disruptive change for Gigamon deployments since they have all enforced a 14 character minimum length for several years. Edit the file <code>/etc/login.defs</code> and change the value 14 to 15 on the <code>PASS_MIN_LEN</code> line.
xccdf_org.ssgproject.content_rule_set_password_hashing_min_rounds_logindefs	Increased hashing rounds make password cracking attacks more difficult, but the impact of the STIG required values on system performance may be excessive. To increase the STIG results, edit <code>/etc/login.defs</code> and replace the line that says <code>SHA_CRYPT_MAX_ROUNDS</code> with the following two lines: - o <code>SHA_CRYPT_MIN_ROUNDS 100000</code> - o <code>SHA_CRYPT_MAX_ROUNDS 100000</code> - o <code>xccdf_org.ssgproject.content_rule_rsyslog_remote_loghost</code> Configure rsyslog to send syslog messages to your environment specific log server. <code>xccdf_org.ssgproject.content_rule_service_usbguard_enabled</code> Enable the usbguard.service system service to prevent anyone from attaching a USB device to your system. Run this command: sudo systemctl enable usbguard.service

Enable Cryptography Mode

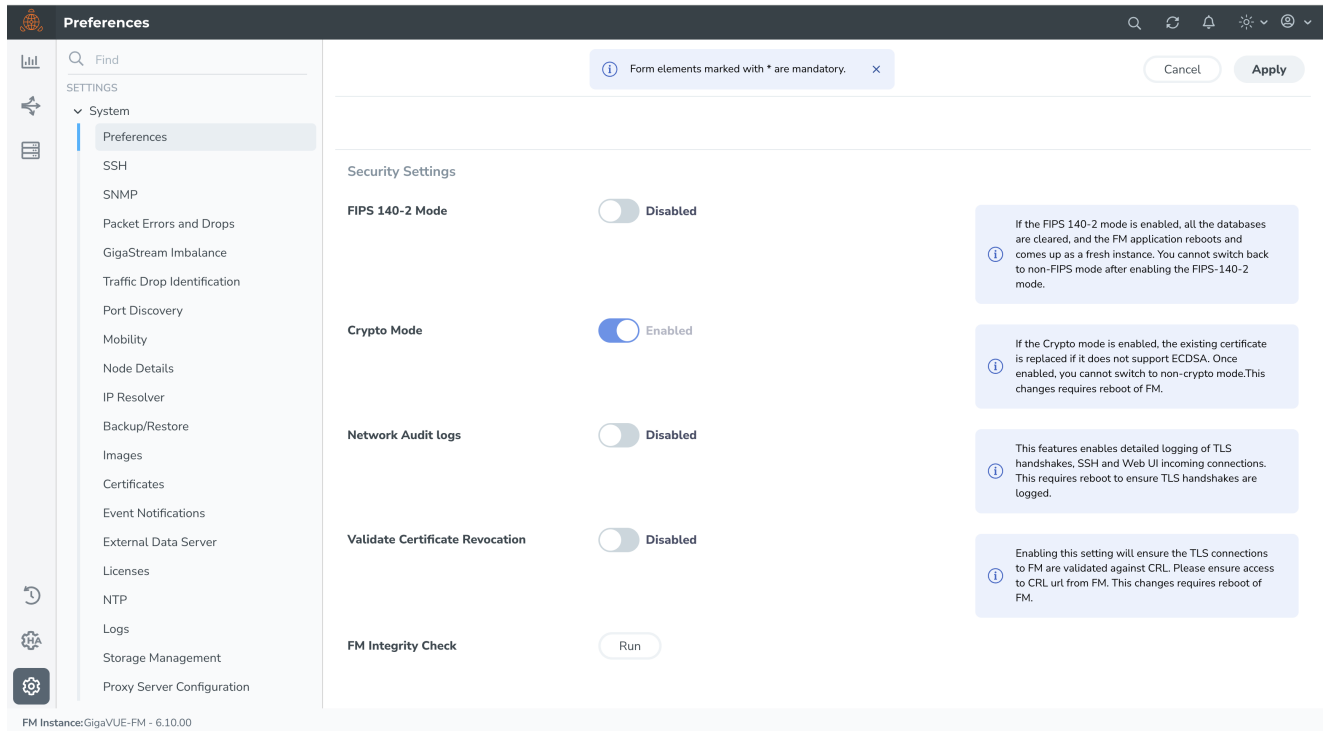
GigaVUE-FM can be configured to cryptography mode to improve the security of the management interface. In cryptography mode, weak encryption or decryption and hashing algorithms used for accessing data and generating keys are disabled. The cryptography mode limits the cryptographic algorithms that are available for use on a GigaVUE-FM.

To enable cryptography mode in the GigaVUE-FM:

1. Go to  > **Settings** > **System** > **Preferences**.
2. In the **Security Settings**, turn on the **Crypto Mode** toggle to enable the cryptography mode.

NOTE:

- Do not enable FIPS Mode and Crypto Mode in the same request.
- Enable FIPS Mode first. After the system restarts, enable Crypto Mode in a separate request.



TLS or SSL Ciphers to Use with Cryptography Mode

When enhanced cryptography mode is enabled, GigaVUE-FM supports TLS 1.2, and TLS 1.3. The following ciphers are supported in TLS 1.2:

Supported TLS 1.2 Ciphers

Cipher Name	Key Exchange (Kx)	Authentication (Au)	Encryption (Enc)	MAC
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	ECDSA	AES256-GCM	SHA384
ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE	ECDSA	AES128-GCM	SHA256
ECDHE-ECDSA-AES256-SHA384	ECDHE	ECDSA	AES256	SHA384
ECDHE-ECDSA-AES128-SHA256	ECDHE	ECDSA	AES128	SHA256

NOTE: Ensure that you configure the above ciphers on the servers or devices that communicate with GigaVUE-FM. You should also ensure that when the cryptographic mode is enabled, the certificate supports ECDSA based ciphers.

SSH Cryptographic Algorithms

GigaVUE-FM supports the following SSH algorithms:

SSH Host Key Algorithm	SSH Key Exchange	Encryption Algorithms	Hash-based Message Authentication Code
ECDSA	ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 kex-strict-s-v00@openssh.com	aes256-ctr aes128-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com	hmac-sha2-512, hmac-sha2-256

Ciphers

The Ciphers page in GigaVUE-FM provides capability to configure Cipher, which allows configuration of the SSH and TLS ciphers used when GigaVUE-FM acts as a client or server. This aligns encryption settings with your organization's security policies and supported certificates.

NOTE: Cipher configuration is optional. Deployments can operate with default ciphers. The feature is included with the base GigaVUE-FM license; no additional license is required.

Configure SSH Parameters

To configure SSH parameters in the GigaVUE-FM:

1. Go to  > **Settings** > **System** > **Cipher**.
2. On the **SSH** tab, locate the following sections:
 - **SSH server** (when GigaVUE-FM acts as an SSH server, for example from an administrator workstation to GigaVUE-FM).
 - **SSH client** (when GigaVUE-FM initiates SSH connections to other systems).

3. For **SSH server / SSH client**, review each configuration group (key exchange algorithms, host key algorithms, ciphers, and MACs):
 - In each list, select only the ciphers approved by the organization's SSH policy.
 - Ensure that at least one supported option remains selected in every list.
4. Select **Apply** on the **SSH** tab.

Confirm that SSH access to GigaVUE-FM remains available by opening a new SSH session.

NOTE: Ensure maximum cipher compatibility with all systems that interact with GigaVUE-FM. Connections fail if cipher settings are not compliant across systems.

Configure TLS Parameters

To configure TLS Parameters in the GigaVUE-FM:

1. On the Ciphers page, select the **TLS** tab.
2. In the **TLS 1.2** section, review the list of available **TLS 1.2** cipher suites presented in the UI.
3. In the Groups or Allowed Groups section:
 - Review the list of supported groups applicable to TLS 1.2 and TLS 1.3.
 - Select only the groups permitted by the organization's security policy.
 - Ensure that at least one group remains selected for each enabled TLS version that uses groups.
4. Select only the cipher suites that are both:
 - Approved by the organization's TLS policy.
 - Compatible with the certificate type configured on GigaVUE-FM (for example, RSA-based or ECDSA-based certificates).

NOTE: Ensure maximum cipher compatibility with all systems that interact with GigaVUE-FM. Connections fail if cipher settings are not compliant across systems.

5. In the **TLS 1.3** section:

- Review the Ciphers list for **TLS 1.3** and select the allowed cipher suites.
- Ensure that at least one cipher suite (and group, where applicable) remains selected when **TLS 1.3** is enabled.

6. If options are available to synchronize server and client TLS settings (for example, “**apply to both server and client**”), use those options when identical policies are required on both sides.

- TLS 1.2 or TLS 1.3 can be disabled independently; for each enabled TLS version, at least one cipher must remain selected.
- Maintain maximum compatibility by selecting a broad, approved set of ciphers.

NOTE: Multiple TLS cipher suites can be selected. Selecting only one or both of the following ciphers prevents GigaVUE-FM from issuing certificates for cloud deployments, causing the deployment to fail:

- TLS_ECDHE_ECDSA_WITH_AES_256_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_SHA256

7. Select **Apply** on the TLS tab.

NOTE: This operation logs out all active users. The UI will take at least 2 minutes to reload and become available again.

8. Open a new browser session to the GigaVUE-FM UI and confirm that HTTPS access is successful using the updated cipher configuration.

9. If GigaVUE-FM connects to external TLS endpoints (such as devices, LDAP, or third-party authentication services), validate those connections to ensure that negotiation succeeds with the selected ciphers.

NOTE:

- In an FMHA deployment, the cipher change operation cannot be performed if any GigaVUE-FM node in the group is unreachable.
- Before changing the cipher, either restore connectivity to all GigaVUE-FM nodes in the FMHA group or remove the unreachable node from the group.

Cipher Selection Behavior for Rsyslog

When you configure ciphers on the GigaVUE-FM Cipher page, Rsyslog may display or use additional ciphers beyond those you explicitly selected. This behavior is due to a limitation in Rsyslog, which applies cipher settings at the cipher group level rather than per individual cipher.

Behavior

- Rsyslog configures the entire cipher group when you enable a cipher.
- If a CBC cipher is enabled, it is enabled for both RSA and ECDSA key types, unless RSA is disabled.
- As a result, you might see CBC-based ciphers active for both RSA and ECDSA, even if you intended to use them for only one key type.

NOTE: To prevent CBC ciphers from being applied where they are not required, clear either all RSA CBC ciphers or all CBC ciphers on the GigaVUE-FM Cipher page, depending on your security policy and deployment requirements.

Recover from incorrect cipher configuration

If access to the GigaVUE-FM UI or SSH becomes unavailable after changing cipher settings, cipher configuration can be reset to defaults by using the CLI.

1. Access the GigaVUE-FM console or an available SSH session with administrative privileges.
2. At the command prompt, run:

```
reset cipher-settings
```

3. Wait until the command completes and a message indicates that GigaVUE-FM Cipher settings have been reset to default mode. This operation can take several minutes.

For more details on commands refer to :[GigaVUE-FM CLI Commands](#)

4. Reconnect to the GigaVUE-FM UI in a browser and verify that access is restored.

NOTE: In an FMHA deployment, perform this procedure independently on each node in the FMHA group.

5. Reconfigure **SSH** and **TLS** ciphers from the Ciphers page, ensuring alignment with the deployed certificates and organizational policies.

When cipher settings are reset and validated, the Cipher is restored to a safe default state and is ready for controlled re-configuration.

NOTE:

- Only users with Super Admin access or an FM Security role can modify this configuration.
- If you restore an FM backup taken on a release earlier than 6.12.02, or a backup that does not include cipher configurations, the FM cipher settings will be reset to their default values.

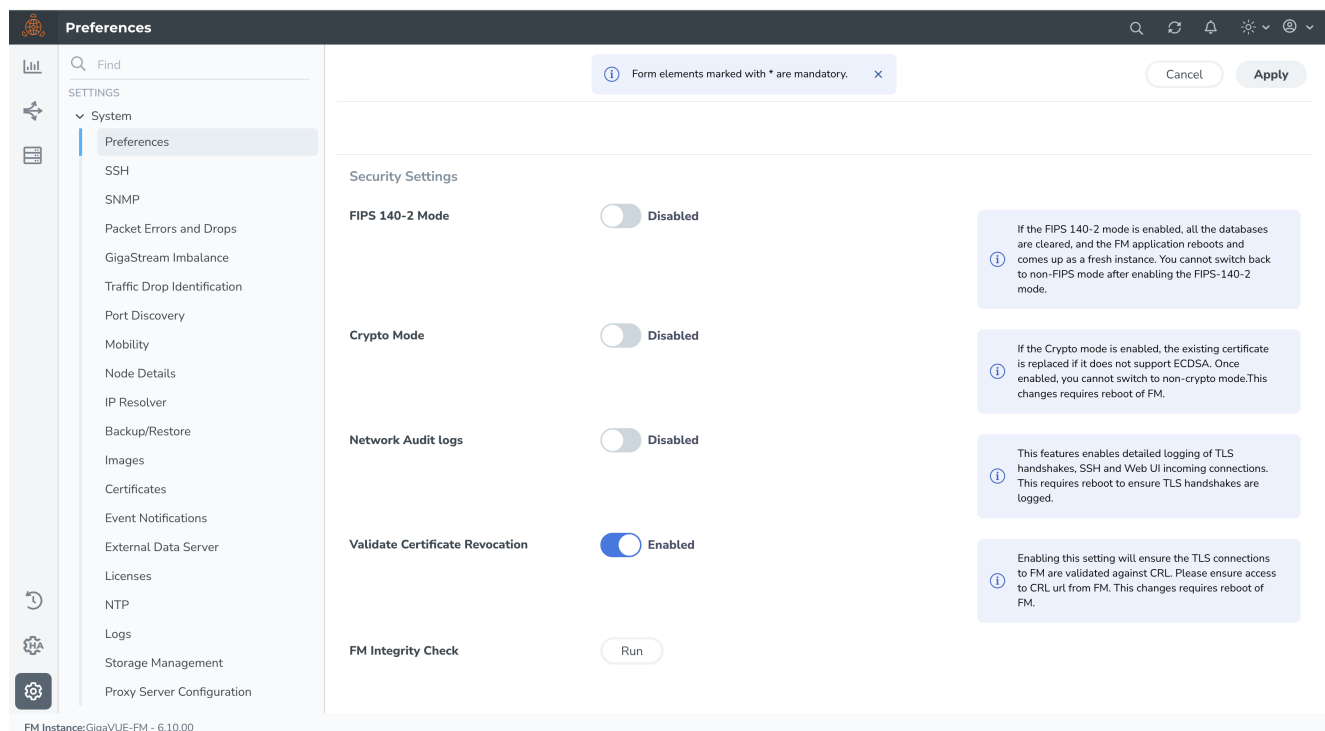
- If you take a new backup on 6.12.02, the cipher configuration details are included in the backup and will be restored as-is when that backup is restored.
- The ***fmctl reset cipher-settings*** command resets the GigaVUE-FM cipher configuration and also resets all cipher configuration of the devices (version 6.14 and above) managed by GigaVUE-FM.

Enable Validation of Certificate Revocation List

The Certificate Revocation List (CRL) Validation feature in GigaVUE-FM retrieves the CRL URL from a certificate in use and verifies if it has been revoked by the Certificate Authority (CA). If enabled, GigaVUE-FM blocks communication with nodes or devices that do not have a valid certificate.

To enable validation of certificate revocation list in the GigaVUE-FM:

1. Go to  > **Settings > System > Preferences**.
2. In the **Security Settings**, turn on the **Validate Certificate Revocation** toggle.



Enabling this setting ensures that the TLS connections established to GigaVUE-FM are validated against the CRL. GigaVUE-FM must be able to access the URL hosting the Certification Revocation List in order for this to work.

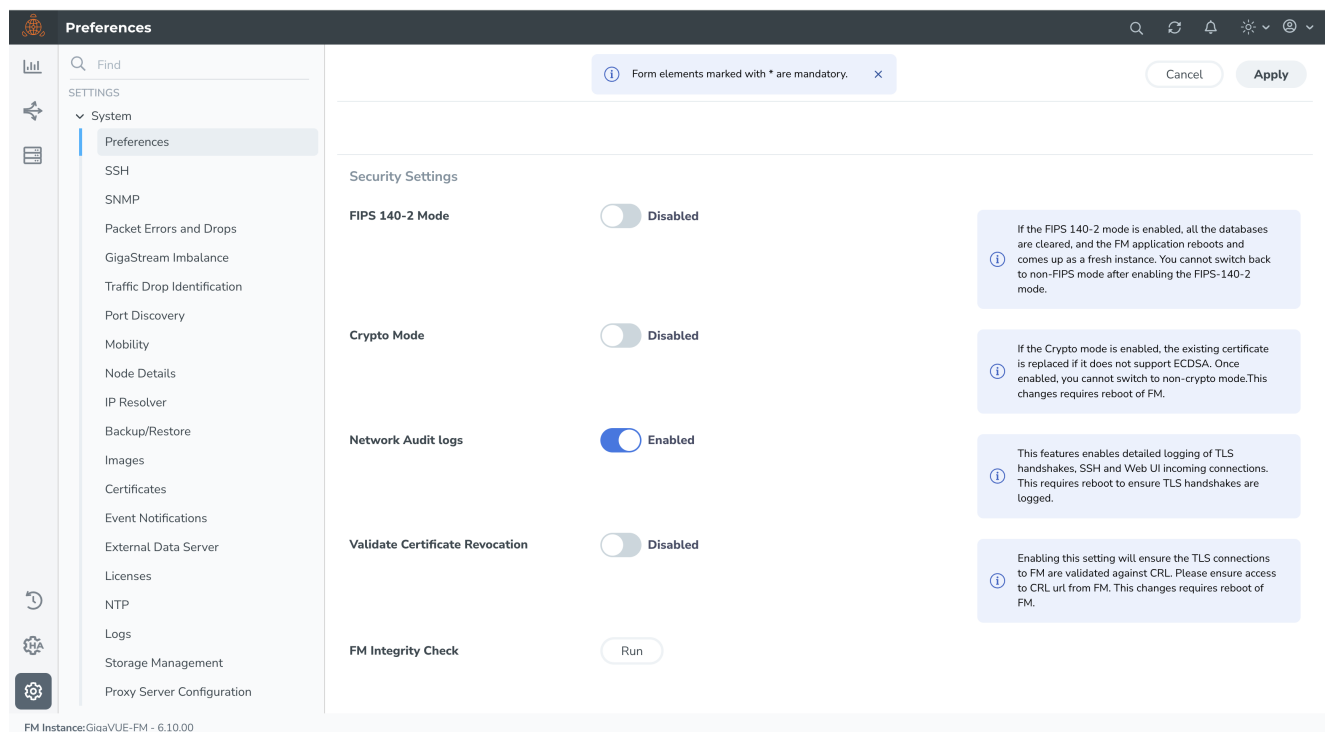
NOTE: You must enable the Secure Access feature and the Certificate Revocation List Validation for proper validation.

Enable Network Audit logs

The Network Audit Log feature in GigaVUE-FM records both the incoming and outgoing traffic between network devices. It also provides logs of the interactions with the management system through the web browser such as user requests or configuration changes. This requires rebooting to ensure TLS handshakes are logged. You can use this feature to track and identify incoming and outgoing requests.

To enable Network Audit Logs in GigaVUE-FM:

1. Go to  > **Settings** > **System** > **Preferences**.
2. In the **Security Settings**, turn on the **Network Audit Logs** toggle.



NOTE: We recommend that you disable the Network Audit Logs when log collection is not needed, as it can lead to storage and performance constraints.

Perform Integrity Check in GigaVUE-FM

This feature enables the GigaVUE-FM to perform the integrity check from the GUI and CLI. The integrity check is performed automatically on fresh installation and the reboot of GigaVUE-FM.

Integrity check validates and ensures that GigaVUE-FM is not compromised.

You can periodically validate the integrity that exceeds the Common Criteria Standard.

How to run Integrity Check

To run the integrity check, do the following:

1. Go to  > **Settings > System > Preferences**.
2. In the **Security Settings > FM Integrity Check**, click the **Run** button.

When the integrity check is complete, you can view a message notifying you that the run is complete.

If the check gets failed, the GigaVUE-FM stops working. In such cases, contact customer support to proceed further.

NOTE: For FMHA, the Integrity check is validated only in active node.

USGv6 Compliance

The following components conformance to USGv6r1 can be found at:

<https://www.iol.unh.edu/registry/usgv6?name=gigamon>.

- GigaVUE-FM (starting from software version 6.5.00)
- GigaVUE HC Series devices
- GigaVUE TA Series devices

NTP Server for Clock Synchronization

Network Time Protocol (NTP) is an internet protocol used to synchronize clocks of different servers in a network.

An NTP server provides accurate time to its clients. It can function as a primary server (directly synchronized to an authoritative time source, such as an atomic clock or GPS) or a secondary server synchronized with a primary NTP server.

Time Synchronization is essential for ensuring accurate time stamping of logs and events, which is instrumental in debugging issues.

GigaVUE-FM allows you to configure multiple NTP servers and ensures NTP settings are retained after upgrades. You can configure NTP using the server's DNS Name or IPv6 or IPv4 address.

In GigaVUE-FM, you can add, delete, and view the status of each NTP server configured. You can authenticate NTP servers to verify that time updates come from a trusted server, ensuring the integrity and security of synchronization.

GigaVUE-FM allows you to authenticate NTP servers only with valid Chrony keys. If the keys are invalid, the server will be connected in anonymous mode and will not allow a retry of the authentication process and will not fall back on the authentication process.

Rules and Notes

Keep in mind the following rules and notes when adding NTP servers in GigaVUE-FM:

- In GigaVUE-FM, Rocky Linux 8 and 9 use Chrony services for time synchronization by default.
- During the Back Up and Restore operation, GigaVUE-FM will not perform the backup and restore of GigaVUE-FM NTP Servers.
- GigaVUE-FM supports the following algorithms for authenticating the NTP servers:
 - MD5
 - SHA1
 - SHA256
 - SHA384
 - SHA512

Add NTP Server for Clock Synchronization

You should add the NTP server to GigaVUE-FM for time synchronization. You can also authenticate the server by providing the key details such as key ID, key value, key type when adding the server.

Before you begin

You must enable the NTP service in GigaVUE-FM before adding the NTP servers for clock synchronization. To enable the NTP service, go to **NTP** page (Go to  > **Settings** > **System** > **NTP**) and click **Enable NTP**.

To add the server:

1. Go to  > **Settings** > **System** > **NTP**.
2. Click **Add Server**. The Add NTP Server page appears.
3. In the **Server IP/Host Name** field, specify the server's address or the hostname.
4. In the **Version** field, select the NTP version.

If you want to authenticate the NTP server, you should enable the authentication, which is optional. When you enable the authentication, you must specify the following:

- In the **Key ID**, specify a key ID from 1 to 65535.
- From the **Key Type** drop-down list, select one of the following key types: The key type is a name of a cryptographic hash function which is used to generate and verify the MAC.
 - MD5
 - SHA1
 - SHA256
 - SHA384

- SHA512
- In the **Key Value** field, specify a value. You can specify the key value as a string of ASCII characters without white space with an optional ASCII: prefix, or as a hexadecimal number with the HEX: prefix. The maximum length of the line is 2047 characters.

NOTE: To generate keys and to use them using chronyd, you must ensure that the chronyd is installed and it is in active state in NTP server. To generate keys refer to [Generate Keys](#).

5. Click **Add** to add the NTP server.

You can view the server details added to the NTP page.

You can also update the NTP server details in GigaVUE-FM. To update the NTP server details:

1. From the NTP page, select the server that you want to update.
2. From the **Actions** drop-down list, select **Edit** to update the details.
You can edit details such as version, key type, and key value except Server IP or Host Name.
3. Click **Apply** to view the updated server details in the NTP page.

NOTE: In GigaVUE-FM High Availability, for the clock synchronization of the GigaVUE-FM present in a High Availability cluster, you must configure the NTP server for each GigaVUE-FM. You must configure all the nodes in a cluster with the same time.

Generate Keys

To generate the keys, you must execute the following command in NTP server:

```
chronyc keygen <key-id> <key-type>
```

key-id and **key type** are optional, the server will pick the default ones.

For example

```
chronyc keygen 4 SHA1
```

In the string 4 SHA1 HEX:2B5FBA344EE7C8B3B7D97431B33CEA3AEFCA6B81

key-id: 4

key-type: SHA1

key value: HEX:2B5FBA344EE7C8B3B7D97431B33CEA3AEFCA6B81

Clock Management Best Practice for devices connected to GigaVUE-FM

Before adding a device to GigaVUE-FM, you must set up the clock using NTP. Additionally, ensure that both GigaVUE-FM and the connected devices are synchronized to the same clock to prevent the following issues:

- GigaVUE-FM and connected devices falling out of sync.
- License deletion due to clock fluctuations.

View Information About GigaVUE-FM

The About page provides product and version information of GigaVUE-FM that you can use when contacting customer support.

To view the About page for GigaVUE-FM (refer to the following figure), click on the button in the upper right-hand corner of GigaVUE-FM, where your name is displayed. Select **About**.

The following information is displayed:

- Product Name—The name of the product, GigaVUE-FM.
- Version—The current version running. For example, 6.1.00.
- Host ID—Host ID of GigaVUE-FM
- Host Name—Host name
- MAC Address—MAC address of GigaVUE-FM
- IP Address—IP Address
- Netmask—Netmask
- Gateway—Gateway
- IPv6 Address—IPv6 Address
- IPv6 Mask
- IPv6 Gateway
- DNS Server
- NTP Server
- FM Start-up Time
- FM Uptime
- Build ID and Build Date—information about when the current build was created—
- Boot Image
- SHA1-Thumbprint
- SHA-256 Thumbprint

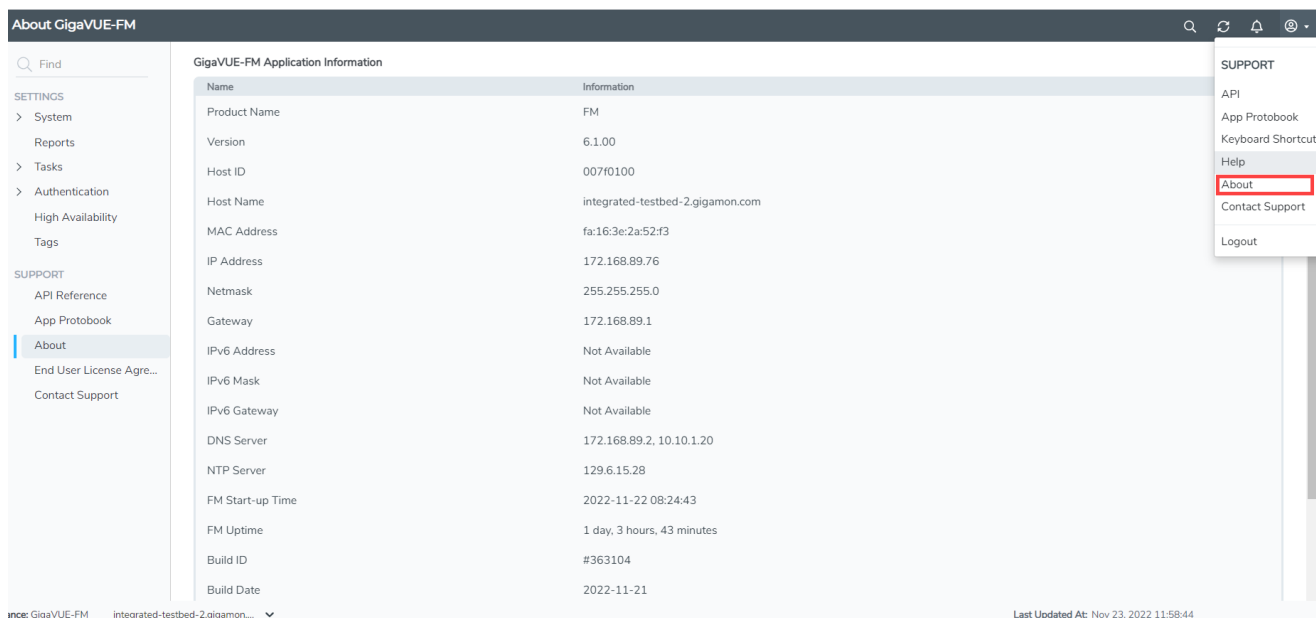


Figure 31 About Page

Generate a Report for Customer Deployed Assets

GigaVUE-FM allows you to generate a Customer Deployed Assets (CDA) report. It creates a detailed report of all deployed hardware and software by SKU, including GigaVUE-OS and GigaVUE-FM versions. GigaVUE-FM also automatically generates a CDA report every Sunday. To generate a CDA report manually:

1. Go to  > **Settings** > **Support** > **About**.
2. Click **Generate Report** in the **GigaVUE-FM Deployed Assets** section. A confirmation message stating that the **Customer Deployed Assets (CDA) audit report generated successfully** appears.

You can view the generated report in the **Report Name** column in the **GigaVUE-FM Deployed Assets** section. To download the report, click **Download**. The file gets downloaded to your local machine.

The screenshot shows the 'About GigaVUE-FM' page. The left sidebar contains navigation links for SETTINGS (System, Reports, Tasks, Authentication, Tags) and SUPPORT (API Reference, App Protobook, About, End User License Agreement, Contact Support). The main content area displays system information:

Property	Value
Gateway	
IPv6 Address	fcab:0:1:2200:8e7:14c2:6d00:8f56
IPv6 Mask	64
IPv6 Gateway	fe80::5e31:92ff:fe40:197f
DNS Server	
NTP Server	Not Available
FM Start-up Time	2026-01-20 18:01:48
FM Uptime	1 week, 1 day, 22 hours, 37 minutes
Build ID	#560751
Build Date	2026-01-10
Boot Image	Not Available
SHA-1 Thumbprint	f7:40:0b:81:10:bcd3:64:dc:0f:40:52:f1:64:aa:68:81:b2:d8:e7
SHA-256 Thumbprint	30:2d:af:52:69:91:87:36:62:29:93:50:a4:4d:f4:61:dd:be:78:a4:14:64:5a:f7:f0:24:46:6d:1d:74:86:8c

©2026 Gigamon Inc. All Rights Reserved.

GigaVUE-FM Deployed Assets

Creates a detailed report of all deployed hardware and software by SKU, including GVOS and FM versions. The report will be available in PDF.

Download Generate Report

REPORT NAME	CREATED BY	CREATED DATE	FILE SIZE
cda-audit-report-20260120-132619....	admin	2026-01-20 18:56:19	451 KB

FM Instance: FM HA Prod - 6.13.00

The report consists of information such as:

- GigaVUE-FM Deployment Details
- Physical Aggregate Inventory
- Physical Node Summary
- License Summary
- Virtual Inventory
- Physical Features Adoption Details
- Cloud Features Adoption Details
- Fabric Manager Features Adoption Details
- Physical Features Usage Metrics
- Cloud Features Usage Metrics

For more information on CDA, refer to [Customer Deployed Assets](#).

High Availability for Physical Environment

This section provides details about the GigaVUE-FM High Availability (HA) feature and describes how to configure, upgrade, and troubleshoot the feature.

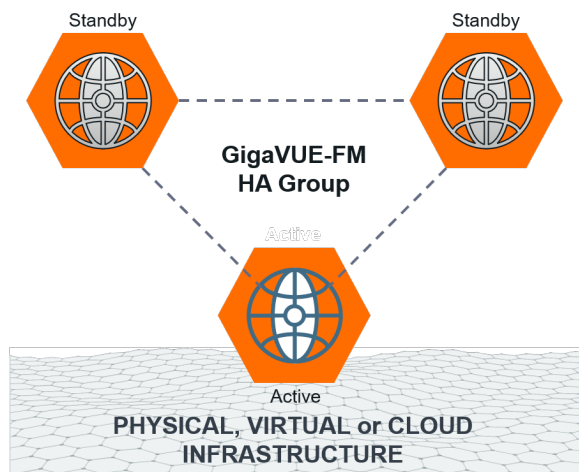
Refer to the following topics for details:

- [About GigaVUE-FM High Availability](#)
- [Get Started](#)
- [Hostname Setups](#)
- [Licensing Information](#)
- [NTP Server for Clock Synchronization](#)
- [Supported Platforms](#)
- [Rules, Notes, and Limitations](#)
- [Dynamic Addition of GigaVUE-FM Instances to HA Group](#)
- [Create and Add GigaVUE-FM Instances to HA Group](#)
- [GigaVUE-FM HA Landing Page](#)
- [GigaVUE-FM Load Balancer Functionality](#)
- [Remove Standby GigaVUE-FM Instance](#)
- [Disassemble GigaVUE-FM High Availability Group](#)
- [GigaVUE-FM High Availability States](#)
- [Failover Mechanism](#)
- [GigaVUE-FM High Availability Scenarios](#)
- [Troubleshoot GigaVUE-FM High Availability Issues](#)
- [Orchestrated Upgrade of GigaVUE-FM Instances in HA Group](#)
- [Access GigaVUE-FM Active Instance in case of Failover](#)
- [Configure GigaVUE-FM High Availability in OpenStack Environment](#)
- [Configure GigaVUE-FM High Availability in Gigamon Containerized Broker](#)
- [Configure GigaVUE-FM High Availability in VMware NSX-T Manager](#)

About GigaVUE-FM High Availability

The GigaVUE-FM High Availability (HA) feature supports a highly available fabric management environment with minimal interruption. The GigaVUE-FM HA architecture consists of a minimum of three GigaVUE-FM instances that run together as a highly available group. The highly available group provides protection from failure of any one of the members in the group. The communication between the GigaVUE-FM instances in the highly available group can be encrypted using Pre-shared Secret Key or Certificate based Authentication.

The following figure shows the high-level architecture of the GigaVUE-FM HA feature.



Starting in software version 5.14.00, you can add additional GigaVUE-FM instances to the high availability group. Refer to the [Dynamic Addition of GigaVUE-FM Instances to HA Group](#) section for details.

Get Started

To configure the GigaVUE-FM HA feature, you must have access to at least three authenticated GigaVUE-FM instances that reside on a trusted network. All GigaVUE-FM instances must run the same software version. The interfaces in the GigaVUE-FM instances must be up and must be assigned IPv4/IPv6 addresses. You can also choose to use DNS host names.

NOTE: You can configure the GigaVUE-FM HA feature only if you have administrative privileges. You must have Prime license installed for forming the GigaVUE-FM HA group.

Hostname Setups

The GigaVUE-FM instances are not required to be in the same subnet, but still must be able to communicate with each other.

In addition, ensure that the instances have unique host names. You must be able to ping a GigaVUE-FM instance from the other instances using the hostname or the IP address.

To add a GigaVUE-FM instance to a GigaVUE-FM HA group:

- The GigaVUE-FM instances in the HA group must be reachable to each other.
- If host names are used to configure the HA group, the host names of the GigaVUE-FM instances must be resolvable through a DNS server.

Licensing Information

You must install a Prime license on the active GigaVUE-FM instance to configure a High Availability group.

If the Prime license expires or if you accidentally delete the license, the existing configurations will still be present in the GigaVUE-FMs that are part of the HA group, but you will not be able to perform any new configurations. Moreover, if you disassemble the HA group, you cannot reconfigure the HA group without installing a valid Prime license. You can re-use the same Prime license to form the HA group again.

NTP Server for Clock Synchronization

It is essential to maintain synchronized time across all nodes. To do this, configure NTP on all GigaVUE-FM nodes in GigaVUE-FM HA. To configure NTP refer to [NTP Server for Clock Synchronization](#).

Supported Platforms

The GigaVUE-FM HA feature is supported on the following platforms:

- VMware vSphere
- GigaVUE-FM Hardware Appliance
- OpenStack
- VMware NSX-T Manager
- [[[Undefined variable cloudVar.CloudNavPath]]]
- Azure
- GCP
- Nutanix

Rules, Notes, and Limitations

Keep in mind the following rules and notes when you configure the GigaVUE-FM HA feature:

- The GigaVUE-FM instances in the HA group must be identical in terms of system configuration such as hard disk, memory, and network interfaces, which include domain server, NTP server, and name server. Domain server, NTP server, and name server should be configured in all GigaVUE-FM instances.

- When creating a GigaVUE-FM HA group, it is highly recommended to create the High Availability group using DNS name. GigaVUE-FM HA cannot manage the individual GigaVUE-FM instances if the IP address changes (if GigaVUE-FM IP(s) are dynamic).
- It is recommended to configure reverse DNS configuration while configuring FMHA with FQDN.
- The GigaVUE-FMs in the high availability group can be accessed using the IPv4/IPv6 address (DNS name) that is used to form the High Availability group.



Do not access all the GigaVUE-FM instances at the same time, as this will impact the performance of the HA group.

- You can deploy the GigaVUE-FM HA virtual machines on a WAN link with a maximum latency of 200 ms.
- You cannot add a GigaVUE-FM Hardware Appliance and a GigaVUE-FM virtual machine in the same HA group.
- VIP support is deprecated from software version 5.13.00. If VIP is configured in earlier GigaVUE-FM versions, it will be continued after upgrading to software version 5.13.00. However, you will be only able to delete the existing VIP, adding or updating the VIP is restricted.
- Use the orchestrated upgrade procedure to upgrade the GigaVUE-FM instances if the software version of GigaVUE-FM is 5.10.00 and above.
- The **Reload All** Or **Reload any FM** commands will work only if there is an active GigaVUE-FM instance in the HA group.
- Third Party Orchestration is supported with GigaVUE-FM High Availability only in OpenStack environment.
- You must ensure that NTP is configured across all FMHA nodes.
- The GigaVUE-FM HA Cluster functions like standalone GigaVUE-FM's when a fail-over occurs during long-running operations, such as Fabric Launch, Monitoring Session Deployment, or Fabric Upgrade. In such cases, manual intervention is required to re initiate these operations from the standalone or GigaVUE-FM HA nodes.

Dynamic Addition of GigaVUE-FM Instances to HA Group

Until software version 5.13.00, GigaVUE-FM HA architecture is based on 2N+1 redundancy model (N = 1) with one active and two standby instances providing resiliency and fault tolerance. With horizontal scaling, the services and application requests are distributed to standby GigaVUE-FMs. As the HA group was limited to only three GigaVUE-FM instances, there was a need for higher computing and memory intensive resources in the HA group because of the following use cases:

- Longer data retention period (up to 13 months).
- Better search performance with more horizontal distribution of OpenSearch for features such as Fabric Health Analytics (FHA) and Topology Visualization.
- Better indexing performance with the number of instances collecting various statistics on the configured components.

Therefore, the number of GigaVUE-FM instances in the HA group had to be increased for scalable performance of the various features in GigaVUE-FM.¹ Starting in software version 5.14.00, GigaVUE-FM allows you to add more than three GigaVUE-FM instances to the HA group. The hardware requirements and resource allocation process for the additional instances are the same as that of the active and standby instances. The additional instances can be configured either as supporting instances or as active-eligible instances:

Supporting instances are GigaVUE-FMs that run minimal services, thereby providing more resources to OpenSearch services. Supporting instances:

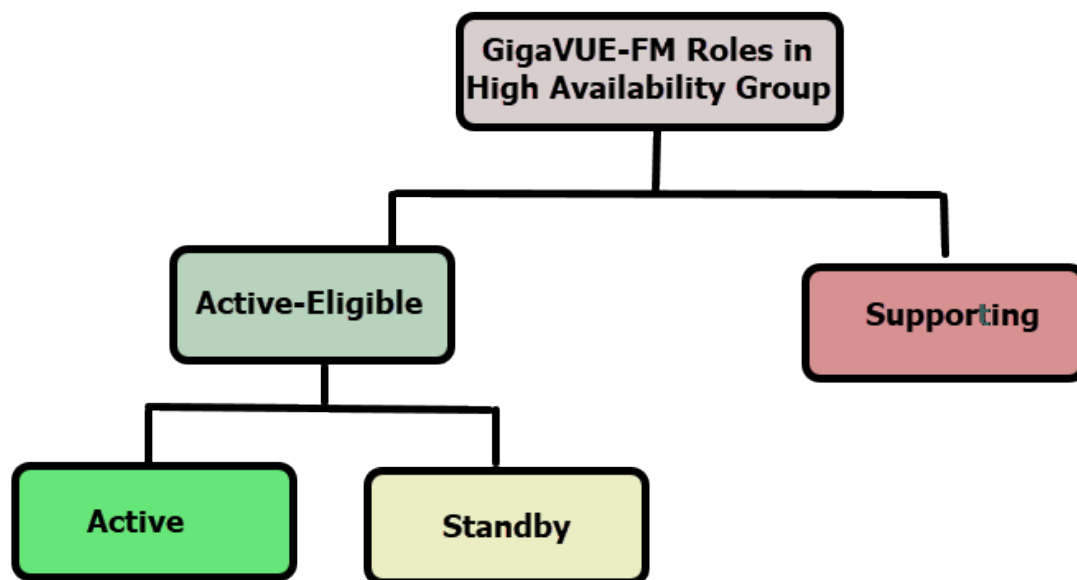
- do not distribute application requests (all application services are turned off by default) nor run any distributed services.
- offer more scalability.
- cannot become candidates for active instance election

Active-Eligible instances are GigaVUE-FMs that distribute application requests and run distributed services. Active-eligible instances:

- Add more value to fault-tolerant and high available system.
- Can be part of active instance election.

Refer to the following diagram for the roles in the HA group.

¹GigaVUE-FM software version 5.13.00 is scaled to manage 3000 nodes. However, with use cases such as Topology Visualization, Fabric Health Analytics that rely on Elastic Search database, Elastic search has become a bottleneck for efficient performance. Therefore, it is required to increase the number of ES instances for enhanced performance and scalability of the HA group.



NOTE: When you add a GigaVUE-FM instance as either a supporting instance or a standby instance, the current configuration of that GigaVUE-FM instance will be removed once it is added to the existing GigaVUE-FM HA cluster.

The following table compares GigaVUE-FM HA in software version 5.13.00 and less with GigaVUE-FM HA software version 5.14.00:

	GigaVUE-FM less than or equal to 5.13.00	GigaVUE-FM 5.14.00
Number of GigaVUE-FM Instances that can be configured in the HA group	Only three GigaVUE-FM instances can be added.	Minimum three. Additional GigaVUE-FM instances can be configured as supporting instances or active-eligible instances.
Status and Roles Supported	- Active (One) - Standby (Two)	- Active-Eligible (Seven) - active - standby - Supporting (Any number of instances) Note: GigaVUE-FM cannot support more than seven active eligible instances in a HA group.
Number of GigaVUE-FM instances that can be configured as Active Eligible.	All three GigaVUE-FM instances are active eligible.	While creating a high availability group, there must be three active-eligible instances in the group.

	GigaVUE-FM less than or equal to 5.13.00	GigaVUE-FM 5.14.00
		Both active-eligible and supporting instances are mutually exclusive. That is, GigaVUE-FM instance cannot act as both active-eligible and supporting role at any point in time.
Remove GigaVUE-FM instances	You cannot remove the GigaVUE-FM instances if the HA state is "At Risk".	You can remove the supporting GigaVUE-FM instances "At Risk" state.

Create and Add GigaVUE-FM Instances to HA Group

To add instances and to configure the HA group:

1. Go to  High Availability.
2. Click **Create**. The High Availability wizard appears.
3. In the **Group Name** field, enter a unique name for the HA group.

NOTE: Avoid using functionality names as the group alias when creating an FMHA group. Functionality names typically refer to actions or operations within the system and can cause confusion and conflicts. Choose a unique and descriptive name instead.

4. Choose any one of the following options to encrypt the communication between nodes:
 - **Pre-shared Secret Key** – Encrypts communication between GigaVUE-FM nodes using an application-managed shared secret key. Refer to [Encryption using Pre-Shared Secret Keys](#).
 - **Certificate Based** – Encrypts communication between GigaVUE-FM nodes using manually uploaded certificates. Refer to [Encryption using Pre-Shared Secret Keys](#).

NOTE: When you install or upgrade to GigaVUE-FM version 6.11.xx or later, encrypted communication between high-availability (HA) instances is automatically enabled as part of the deployment process.

5. In the **Add GigaVUE-FM Instance** section, the details of the GigaVUE-FM instance from which the HA group is created will be fetched automatically.
6. Enter the External IP Address and Third-Party Authentication details, if required. Click the **save** icon to save the configuration.

High Availability

Note:

- There must be at least three active eligible nodes that are reachable to each other.
- Save each row individually before continuing.

Cancel Submit

Group Name * FMHA1

Encryption Method ☒ Pre-Shared Key ☐ Certificate Based

ADD GigaVUE-FM INSTANCES + Add New Node

IP Address / DNS N...	External IP Address...	Role	Username	Password	Entity ID	Third Party Authen...	Take Action
		Active Eligible	admin	*****			
		Active Eligible	admin	*****			
		Active Eligible	admin	*****			
		Supporting Node	admin	*****			
		Supporting Node	admin	*****			

7. Click **Add New Node** to add the GigaVUE-FM instances. Enter the following details:

- **IP Address/DNS Name** - IP address/DNS name of the GigaVUE-FM instance (s for communication between the GigaVUE-FMs and to configure the HA group). It is always recommended to use the DNS name while creating the GigaVUE-FM High Availability group.
- **Tunnel IP Address** - IP address used for establishing the secure communication tunnel between HA instances. This is required when the instances are reachable only through public or external IP addresses. If the tunnel IP is the same as the external IP, you can select the auto-populate option.
- **External IP Address** - External IP address of the GigaVUE-FM instance (for accessing the GigaVUE-FM HA from outside the internal network.).
- **Role** - Role of the GigaVUE-FM instance. Can be configured as either:
 - **Active Eligible**- provides resiliency and load distribution.
 - **Supporting Node**- provides scalability and performance.
- **Username** - GigaVUE-FM admin's username.
- **Password** - GigaVUE-FMadmin's password.
- **Third Party Authentication** - Third-party authentication URL.

8. Click **Save Node**  to validate the details entered for the instances.

Once three active instances are added to the HA group, the **Submit** button is enabled.

NOTE: When creating a HA group, all the existing data on the first configured GigaVUE-FM instance will be preserved, allowing the system to continue using the data after it is fully set up. However, the data on the subsequent nodes will be lost during the setup.

9. Use the **Add New Node** button to continue to add the GigaVUE-FM HA instances. When adding the instances, define the role of the instances either as:
 - Active Eligible
 - Supporting Node
10. Review the details of the GigaVUE-FM instances. Use the **Back** button to go back and change the details.
11. Click the **Edit Node** icon to edit the details of the GigaVUE-FM instances, if required.

After adding the instances to the HA group, click **Submit**. The HA group is configured and will be displayed as follows:

Status	IP Address...	Role	External IP...	Entity ID	Host Name	Application Stat...	Software Ve...
Active		Active Eligible			unconfigured-gi...	Up	6.11.00
Standby		Active Eligible			unconfigured-gi...	Up	6.11.00
Standby		Active Eligible			unconfigured-gi...	Up	6.11.00

NOTE: When switching between the Pre-shared Secret Key and Certificate-Based options for encrypting communication between nodes, it's important to refresh the GigaVUE-FM to see the updated tunnel status. By clicking the link in the **Tunnel Status**, GigaVUE-FM displays the health status of the FMHA nodes.

Click the ellipses on a GigaVUE-FM instance to perform the following tasks:

- **Edit:** Edit the instance details.
- **Reboot:** Reboot a GigaVUE-FM instance.
- **Remove from group:** Remove an instance from the HA group.

The HA page displays the following details:

Table 3:

Field	Description
Status and Reachability	Status of the GigaVUE-FM instances. Can be: • Active • Standby • Supporting Reachability: •  - indicates that the instances are reachable. •  - indicates that the instances are unreachable.
IP Address/DNS Name	IP address/DNS name of the GigaVUE-FM instances
Role	Role of the GigaVUE-FM instance. Can be configured as follows: • Active Eligible: provides resiliency and load distribution • Supporting Node: provides scalability and performance
Entity ID	Entity ID of GigaVUE-FM. It is a unique alpha-numeric ID that must be configured for SSO authentication.
Host Name	Host name of the GigaVUE-FM instance.
Application Status	Status of application services that are responsible for handling the user requests: • Up: Indicates service is ready to handle the user requests • Down: Indicates service is not ready to handle the user requests with one or more underlying services being down. • In Progress: A state that appears between up and down indicating that the services are initializing.
Software Version	Software version of the GigaVUE-FM instance.
System Uptime	Time since the instance is up and active.
Third Party Authentication URL	Third party authentication URL required for SSO configuration.
Upgrade Status	Upgrade status of GigaVUE-FM. This is displayed only when the upgrade is triggered. Otherwise, this field is empty.

You can add instances to the HA group by clicking the **Add New Node** button, as required. You can also remove the instances from the HA group and reduce the size of the HA group as required. However, while removing the instances ensure to retain the quorum¹ number of instances.

NOTE: To scale components such as Fabric Health Analytics, topology visualization and to improve the performance of GigaVUE-FM by fully utilizing the resource available, it is recommended to configure three active eligible instances and additional supporting instances.

¹Quorum number of instances is the minimum number of instances that must be active-eligible in a HA group. In a HA group with five instances, the quorum number is 3 (based on the formula $n/2+1$).

The following are the behavioral changes observed in the HA group with active, standby and supporting instances:

Task	Scenario	Behavior
Backup and Restore Operation	All active-eligible instances are up and few or all supporting instances are up.	Backup will happen in active instance. During restore, all active-eligible GigaVUE-FMs will be rebooted and will perform the restore operation. Supporting instances will not participate in the restoration.
	Few active-eligible instances are up (Quorum number of instances are up)	Backup will happen in active instances. Restore will not be initiated in this case.
Upgrade Operation	Few instances not being up (either active-eligible or supporting instances not up)	Upgrade will not be initiated.
	Few supporting instances are removed from the HA group after formation of the group	Upgrade will be initiated, and the supporting instances present in HA group will be upgraded first followed by the active-eligible instances.
	All instances are up and running	Upgrade will be initiated in an active instance. Upgrade will be done in a rolling fashion starting with supporting instances and ending with the active-eligible instances.
System Configurations	All instances are active-eligible	All GigaVUE-FM's GUI will be accessible, and user can configure the system through the same
	HA with active-eligible and few Supporting instances	For supporting instances, GUI will not be available (as application service is shut down). An option is provided in the GUI to turn on the application service and its dependent service(s) and the status can be seen in HA page. You can then configure the system related configuration from the logged in GigaVUE-FM instance once the application status of the supporting instance is up.
Background processes		

Task	Scenario	Behavior
-FM Service Distribution	All GigaVUE-FMs are active-eligible instances.	Services will be equally distributed/redistributed among the instances based on the availability of the instances.
	HA group with active-eligible instances and supporting instances.	Services will be distributed/re-distributed only to active eligible instances
-Load Balancer	All GigaVUE-FMs are active-eligible instances.	All GigaVUE-FM API requests will be distributed to all instances in the HA group.
	With supporting instances.	All GigaVUE-FM API requests will be distributed only to active-eligible instances.

Important Recommendations and Notes

Keep in mind the following recommendations and notes when working with the HA group.

GigaVUE-FM cannot support more than 7 active-eligible nodes (this is due to the underlying constraint in MongoDB).

Shrinking the size of the HA group:

- When reducing the size of a HA group that has both active-eligible and supporting instances, it is always recommended to remove the supporting instances first so that the active-eligible instances remain intact in the HA group. If active-eligible instances are removed first from the HA group, then the HA group will become unstable. This, however, depends on the number of active-eligible and supporting instances in the HA group. Consider a GigaVUE-FM HA group with 7 instances. The number of active and supporting instances in a HA group may be as follows:

HA group 1	With 3 active instances and 4 supporting instances	The recommendation is specifically applicable for HA group 1 in which there are only 3 active eligible instances in the group. Removing the active-eligible instances may cause the HA group to become unstable.
-------------------	--	--

HA group 2	With 5 active instances and 2 supporting instances.	The recommendation is not applicable for HA group 2 as removing the active-eligible instances will not impact the stability of the HA group.
-------------------	---	--

For a HA group to be stable, it must have a minimum of two active-eligible instances in the group.

- When reducing the size of HA group from 7 instance to 5 instance or 3 instance, the quorum is re-computed and adjusted accordingly. This is to ensure that the HA group remains intact with the available set of instances.
- When reducing the size of the HA cluster, during removal of an instance make sure to give time for the OpenSearch to rebalance and return to a complete (100%) healthy state before removing the next instance. If you remove the instances subsequently one after the other, the health state of the HA group will turn red as there will be no time for shard rebalancing amongst the available instances. Login to GigaVUE-FM CLI as a root user and execute the following command to check the ES cluster health:

```
curl -XGET "http://localhost:9200/_cluster/health?pretty"
```

Supporting GigaVUE-FM Instances:

- When a supporting instance is added to the HA group, its system information will not be available immediately and will be available only after a minute.
- When the HA group is upgraded, application services of the supporting instances will be turned on automatically for the upgrade and once GigaVUE-FM HA upgrade is completed it will be turned off automatically. Application services will be turned off automatically irrespective of the upgrade completion status, that is, either success or failure.



Notes:

- For supporting instances, system information will be populated into MongoDB as the Application Service is down by default (scheduler populates the system information every minute into MongoDB). Hence any changes in the system hostname or GigaVUE-FM version will be reflected in the GUI only after a minute.
- In case of suspended mode, MongoDB will go into write protected mode. Therefore, any system related updates performed in the supporting nodes will not be reflected in the GUI.
- If the supporting instance is not reachable, all system related information that is populated in the GUI reflects the previous known values and not the latest values for Application Status, Up Time, and other system related information.



- Whenever the application services are up and running, events will be logged in the Events page (with the severity level - Info)

The following table displays operational scenarios and GigaVUE-FM High Availability behaviour.

Scenario	Trigger/Event	Behavior/Notes	
Failover due to FM crash	Active FM becomes unreachable	Standby GigaVUE-FM is promoted to active. Fabric Orchestration resumes automatically.	No manual Intervention required.
UCTC registration in High Availability	New UCTC node added	GigaVUE-FM High Availability master receives registration request. Node registered with fresh inventory sync	Uses POST
Policy deployment after switchover	FMHA leader changes	New recomputes desired state. Policies re-applied, stale entries removed	TAP responds asynchronously
Public IP preference for RMQ	Fabric node behind NAT	GigaVUE-FM High Availability uses public IP for RMQ notifications	Stats reach GigaVUE-FM High Availability leader reliably. Configurable via UI checkbox.
Tunnel IP configuration	GigaVUE-FM High Availability in Cloud	Tunnel IP field used for external communication	Secure Connectivity Established.
Node heartbeat failure	Node stops sending heartbeat	For supporting instances, GigaVUE-FM High Availability marks node as unreachable. Alerts triggered, node removed if persistent	Uses PUT
Standalone → FMHA migration	Existing GigaVUE-FM upgraded	Node joins HA group	Configuration synced, node re-registered

GigaVUE-FM HA Landing Page

When you login to any of the GigaVUE-FM instances of the HA group, the dashboard page appears. Use the drop-down option in the header of GigaVUE-FM, which is available on specific pages, to view the details pertaining to that GigaVUE-FM. For example, the following pages in the GigaVUE-FM GUI have drop-down option in the header:

- FM Health
- IP Resolver
- [NTP Server for Clock Synchronization](#)

GigaVUE-FM Load Balancer Functionality

GigaVUE-FM instances participating in the HA group act as Load Balancers allowing better distribution of load within the GigaVUE-FM instances. GigaVUE-FM load balancer functionality provides the following capabilities:

- **Seamless access to the GigaVUE-FM Dashboard page:** Accessing any GigaVUE-FM GUI always takes you to the GigaVUE-FM dashboard page after successful login. This provides a cluster view of the GigaVUE-FM GUI rather than individual views for the active and standby instances.
- **Ability to access the available GigaVUE-FM GUI even during a failover:** However, there will be an impact to the write operation, until a new active instance takes over. For example, when you create, update or delete any of the resources in GigaVUE-FM such as maps, GigaSMART groups, tags, etc. during failover, then the operation will fail with the following error message: *Unable to Connect to Server*.
- **Enhanced distribution of load across the members of the HA group:** This allows faster response to the HTTP GET requests.
- **Ability to perform backup/restore/upgrade operation from any of the GigaVUE-FM instances.**

GigaVUE-FM Load Balancer Replaces Get Distribution Support

The GigaVUE-FM Load Balancer functionality replaces the GetDistribution support provided in software version 5.12.00.

NOTE: You cannot disable the Load Balancer functionality.

The following behavioral changes are observed:

- After creating, updating, or deleting resources in GigaVUE-FM, the GigaVUE-FM GUI will be updated immediately. However, if there is latency between the GigaVUE-FM instances, the GUI will not be updated immediately. The subsequent refresh will display the updated data.

- GetDistribution will be impacted if DNS resolution of GigaVUE-FM instances fail:
 - If active GigaVUE-FM instance DNS is unresolvable, then the load will be distributed between the two standby instances, with an impact to the write operation.
 - If standby GigaVUE-FM DNS is unresolvable, then the load on the active instance increases, thereby increasing the CPU and Memory Usage.
- If any GigaVUE-FM instance is down in the HA group, and if a API request is forwarded to that instance due to load balancing, then for a few seconds GigaVUE-FM GUI will not load any data. The subsequent refresh or reload will display the updated data.

NOTE: Consider three GigaVUE-FM instances FM-A, FM-B, and FM- C and that you are logged in to the HA group with the IP address or DNS name of FM-A. When working with the GigaVUE-FM GUI, if FM-B goes down, then the GUI will not load any response. This is because the load balancer (FM-A in this case) has not learned about the unreachability of FM-B instance, which will happen only during the next periodic health checkup.

- The rate at which the active GigaVUE-FM instance handles the HTTP Get request and its processing will be high in case of HA upgrade when the standby GigaVUE-FM instances are upgrading and that forces active GigaVUE-FM to handle all the HTTP Get requests. In this case, CPU, Memory Usage will be slightly higher than the normal.

Important Recommendations

- For seamless access to the HA group, configure a DNS name that resolves to all the GigaVUE-FM instances participating in the cluster.
- For better user experience, the backup/restore operation must be carried out from an active GigaVUE-FM instance.
 - If you perform a restore operation from active instance, you will be notified about the restore operational status before the GigaVUE-FM goes down.
 - If you perform the same restore operation from a standby GigaVUE-FM instance, GigaVUE-FM GUI will go down without any notification about the restore operation to the users.
- If GigaVUE-FM HA upgrade fails and if the upgrade is completed manually, you must login to the GigaVUE-FM CLI as root user and run the following command. To login as root user, login into shell with admin credentials and type "sudo su -"

```
curl -XPOST "localhost:4466/fmcs/updateLoadBalancer?pretty"
```

Response :

```
{"operation":"success"}
```

NOTE: Contact Gigamon Technical Support if you do not see this response.

Remove Standby GigaVUE-FM Instance

To remove or replace a standby GigaVUE-FM instance from the GigaVUE-FM HA group follow the below listed steps:

12. Go to  High Availability.
13. Select the standby GigaVUE-FM instance that you want to remove from the HA group.
14. Click the ellipsis on the GigaVUE-FM instance widget in the High Availability page as shown in [Figure 32 Disabling GigaVUE-FM Instance](#).

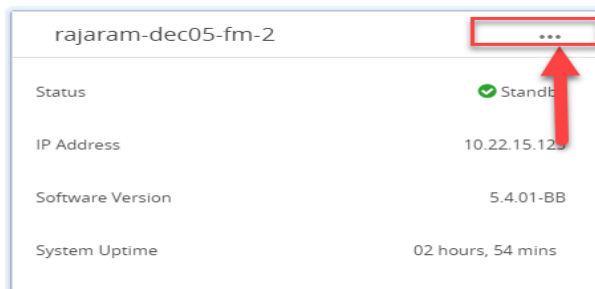


Figure 32 *Disabling GigaVUE-FM Instance*

15. Select the **Remove from group** option. The selected standby GigaVUE-FM instance is removed from the GigaVUE-FM HA group.

NOTE: The status of the GigaVUE-FM HA group changes from **Healthy** to **At Risk**. You will not be allowed to remove the other standby GigaVUE-FM instance after the HA status changes to **At Risk**. To remove the standby node, if there is any network latency in GigaVUE-FM and the node is not removed correctly, use the command **fmcs remove force** in the GigaVUE-FM CLI of the standby node.

Disassemble GigaVUE-FM High Availability Group

To completely disassemble the GigaVUE-FM HA group:

1. Go to  High Availability.

NOTE: You cannot remove an active GigaVUE-FM instance or disassemble the GigaVUE-FM HA group by logging in from a standby GigaVUE-FM instance.

2. Click the ellipsis on the GigaVUE-FM instance widget in the High Availability page.

3. Select the **Delete HA group** option. The GigaVUE-FM HA group is disassembled and each of the GigaVUE-FM instances become standalone GigaVUE-FM instances.

NOTE: Executing the above steps disassembles the GigaVUE-FM HA group completely. The database of the individual GigaVUE-FM HA group members (active, standby, and supporting instances) will be erased and reinitiated with the default database. If you had performed orchestrated configuration flows (such as the Flexible Inline Arrangement or Intent Based Orchestration) you must manually remove and recreate these if they do not backup the GigaVUE-FM database before choosing Delete HA Group.

If you cannot access the active GigaVUE-FM instance's GUI, use the following CLI command in all the GigaVUE-FM instances to disassemble the HA group:

/opt/fmcs/bin/fmcs leave force

Before disassembling the instances, take a backup of the configuration. After the GigaVUE-FM instances are disassembled from the HA group, the configurations present in the instances will be completely removed.

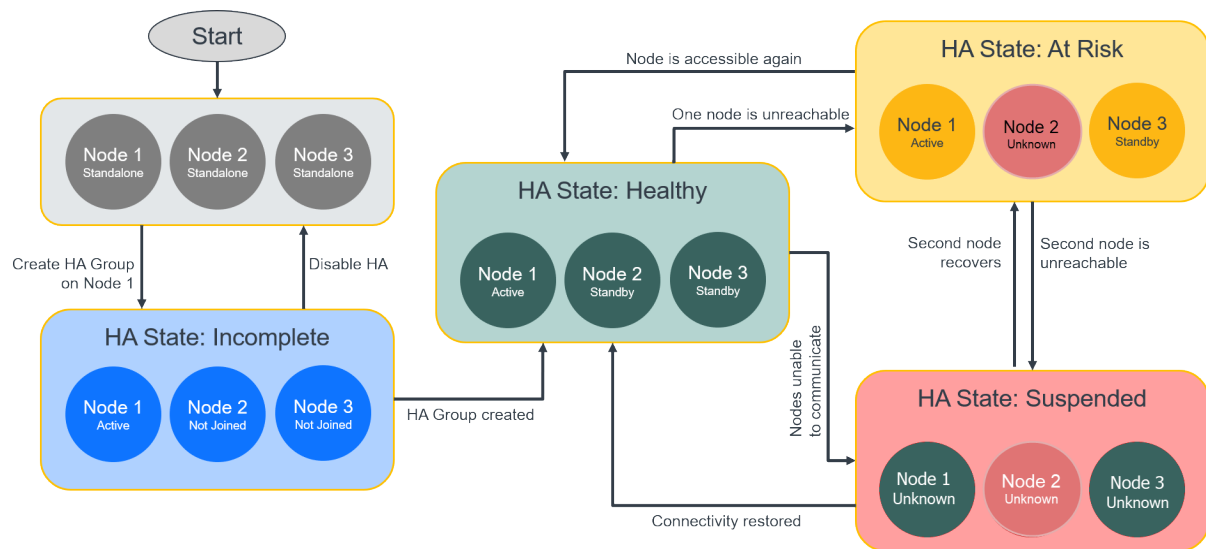
GigaVUE-FM High Availability States

The GigaVUE-FM HA state depends on the status of the three GigaVUE-FM instances. The following table lists the various states of the GigaVUE-FM HA group. You can view the HA group state from **Administration > High Availability** in the GigaVUE-FM GUI.

Table 4: High Availability States

State	Number of GigaVUE-FM Instances	Description
Healthy	Three GigaVUE-FM instances are up and running	One GigaVUE-FM instance is in active state. Other two instances are in standby state.
At Risk	Two GigaVUE-FM instances are up and running	One GigaVUE-FM instance is in active state. Another GigaVUE-FM instance is in standby state. The third GigaVUE-FM instance has either not joined the HA group or has left the HA group. NOTE: You must recover the standby GigaVUE-FM instance within 3 days (72

State	Number of GigaVUE-FM Instances	Description
		hours). Failure to do so will cause the instance to move out of the High Availability group.
Incomplete	One GigaVUE-FM instance is up and running	Only one GigaVUE-FM instance is in active state. The other two GigaVUE-FM instances have either not joined the HA group or have left the HA group.
Standalone	One GigaVUE-FM instance is up and running	HA is not configured on the GigaVUE-FM instance.
Suspended	Two or more GigaVUE-FM instances are up and running	HA is configured, but an active GigaVUE-FM instance is yet to be elected. Note: The GigaVUE-FM high availability group can move to a Suspended state from the At Risk state when the HA group has only one active-eligible and reachable GigaVUE-FM instance. Events will not be captured for the status of the GigaVUE-FM instance that went down (which causes the HA group to move into a suspended state) as there is no active/leader instance in the High Availability group.



In case of FMHA going to suspended mode from At-Risk mode, the reachability status of node which went down (due to which HA went into suspended mode) won't be audited as writes are not accepted if there is no active/leader instance in the DB cluster

Figure 33 High Availability States

Failover Mechanism

The active GigaVUE-FM instance in the high availability group may fail at times resulting in one of the standby instances to take over and become the active instance. This process is called failover.

The following table provides the reasons for failover:

NOTE: Tasks such as fabric deployment, monitoring sessions, upgrades, and orchestration workflows automatically resume after failover.

Reason for Failover	Description
Reloading the active GigaVUE-FM instance	An active GigaVUE-FM instance is reloaded (using the Reboot option) to bring back the HA group to healthy state again.
Planned downtime of the active GigaVUE-FM instance	An active GigaVUE-FM instance is brought down due to various reasons, for example to upgrade to a newer software version.

GigaVUE-FM High Availability Scenarios

The High Availability page (Go to High Availability) displays the current state of the GigaVUE-FM HA group. When a failover occurs, the HA group state changes in the GUI.

The following table lists the GUI changes for the various scenarios:

Scenario	Changes in GUI
What happens to the High Availability page immediately after a failover?	The High Availability page may not update immediately or may not show all the GigaVUE-FM instances. Note: Refresh the page after a minute to view the new active GigaVUE-FM instance. However, the page will get updated automatically after 5 minutes.

Scenario	Changes in GUI
What happens to an active GigaVUE-FM instance when it fails (either by itself or if failover is triggered manually)?	- One of the standby GigaVUE-FM instances changes to the active state. The GigaVUE-FM instance that was initially in the active state changes to the standby state. It takes a few seconds for this transition. - The GigaVUE-FM GUI of the new active instance will have all the menus and dashboards.
What happens to the GigaVUE-FM instances that were previously in standby state?	- One of the standby GigaVUE-FM instances changes to the active state - The other standby GigaVUE-FM instance remains in the standby state.
What happens to the embedded devices when a new Active instance takes over?	There are no changes to the devices except that they are being managed by the new active GigaVUE-FM instance.
How do you trigger a failover?	Click on the 'Reboot' option on the current active GigaVUE-FM instance to trigger a failover.

Troubleshoot GigaVUE-FM High Availability Issues

Use the following table to troubleshoot issues that you might encounter while working with the HA feature.

Problem	Solution
Unable to add a license to GigaVUE-FM HA group after a failover Reason: Using the MAC Address in the About page to generate the license	Always use the Challenge MAC Address in the Licenses page of the active GigaVUE-FM instance to generate licenses. Add the licenses to the HA group.

Problem	Solution
Unable to join the GigaVUE-FM HA group after changing the password Reason: Not logging out of GigaVUE-FM after changing the password and before joining the HA group	Always logout of GigaVUE-FM after changing the password and login again with the new password before joining the HA group.

Orchestrated Upgrade of GigaVUE-FM Instances in HA Group

Orchestrated upgrade of GigaVUE-FM instances in a High Availability group is similar to upgrading a standalone GigaVUE-FM instance. You can upgrade using an image that is located on an external image server, or you can use GigaVUE-FM as the image server. Refer to the [Upgrade GigaVUE-FM from the GigaVUE-FM CLI](#) section in the *GigaVUE-FM Installation and Upgrade Guide* for more details.

Prerequisites

Before upgrading the GigaVUE-FM instances in a High Availability group, ensure the following:

- The High Availability group must be in a healthy state.
- The latency between the GigaVUE-FM instances must be less than 100ms.
- The config disk space allocated to GigaVUE-FM must have a maximum sustained transfer rate of above 100MB/s. A low disk rate impacts both file sync and installation.

Upgrading GigaVUE-FM Instances in HA Group

To upgrade the GigaVUE-FM instances in a High Availability group from the GUI, click the **Upgrade** option from the User icon. Always trigger the upgrade from the active GigaVUE-FM instance.

NOTE: Do not run any scripts (example: scripts for fetching polling statistics of maps) or queries (example: database or stats queries) prior to or during the upgrade operation as this will drain GigaVUE-FM's memory and CPU resources and impact the upgrade operation.

The screenshot shows the 'Software Upgrade' interface. At the top, a progress bar indicates 'Upgrade in progress' with three stages: 'Downloading (1/3)' (active), 'Installation', and 'Reboot'. Below this, a table titled 'Software Upgrade in detail' provides information for three nodes.

HOST NAME	APPLICATION STATUS	NODE STATUS	IP ADDRESS/DNS NAME	ROLE	UPGRADE STATUS
GigaVUE-FM-6800	Up	Active	10.114.84.63	Active Eligible	Downloading
GigaVUE-FM-6800	Up	Standby	10.114.84.69	Active Eligible	Not Started
GigaVUE-FM-6800	Up	Standby	10.114.84.70	Active Eligible	Not Started

The following is the sequence of events that occur in the background:

1. **Active GigaVUE-FM Instance:** Software image download process is triggered and the image is downloaded.
2. **Active GigaVUE-FM instance:** Syncs and copies the downloaded image with one of the standby GigaVUE-FM instances - the first standby GigaVUE-FM instance.
3. **First Standby Instance:** Image is synced, and the standby instance will get upgraded first and rebooted.
4. **Second Standby Instance:** Image is then synced by the second standby instance and the second standby instance will get upgraded and rebooted.
5. **Active GigaVUE-FM Instance:** Once the standby instances are upgraded, the active GigaVUE-FM will start to upgrade and will be rebooted.
6. A new active GigaVUE-FM instance will be elected while the active GigaVUE-FM reboots.

NOTE: As orchestrated upgrade is a background process, device management tasks will be carried out seamlessly. The overall time consumed for the upgrade process is around 60 minutes and the total management loss time during orchestrated upgrade is around 1 minute. This is the time required to elect the new active GigaVUE-FM instance when the current active GigaVUE-FM instance reboots post upgrade.

Access GigaVUE-FM Active Instance in case of Failover

In a GigaVUE-FM high availability environment, you can perform the GigaVUE-FM and device configurations only from the active GigaVUE-FM instance. Standby instances provide minimal configuration options. In case of failover, it is important to be aware of the IP addresses of the three GigaVUE-FMs and also the DNS host names of the GigaVUE-FM instances so that you can access the active GigaVUE-FM instance.

To overcome this restriction and still access the GigaVUE-FM instances, you can use one of the following options:

- Use Load Balancer
- Assign a DNS Name for the GigaVUE-FM instances

Use Load Balancer

Load balancer distributes traffic across a number of servers. Integrating a load balancer with GigaVUE-FM, forwards the traffic to the active GigaVUE-FM instance. Load balancer performs healthcheck of GigaVUE-FM and forwards the traffic destined to the external GigaVUE-FM IP address and thereby to the GigaVUE-FM high availability group.

To use load balancer for forwarding the traffic, you must ensure to do the following:

- Deploy the load balancer.
- Configure the load balancer to access the active instance in the GigaVUE-FM High Availability group. This is accomplished using the following GET API endpoint exposed by GigaVUE-FM:

`https://<FM-IP>/api/v1.3/fmHa/status`

Based on the returned response codes, the load balancer can be configured in such a way that healthy servers (active instance) are those that return 200 as response code when the endpoint API is queried. The remaining servers are considered as unhealthy servers (standby instances). With these configurations, the requests are forwarded to active GigaVUE-FM always.

*Sample Response for **GET https://<FM-IP>/api/v1.3/fmHa/status***

If FM Role == active/standalone,

return 200 with Payload {"role": "active"} or {"role": "standalone"}

Else if FM Role == Standby

return 202 with Payload {"role": "Standby"}

Else if FM Role == support, suspended, unknown

return 400 with Payload for 400 {"role": "Unknown"}

Note : 5xx can be thrown if the API Gateway on FM is not available/down

- Configure the load balancer with external GigaVUE-FM IP address as the DNS IP, for example, myfm.com.

NOTE: If you add or remove the nodes in the GigaVUE-FM HA group, you must ensure to update the corresponding IP addresses of the nodes in the load balancer.

Assign DNS Name for the GigaVUE-FM IP

You can assign a DNS name to the three GigaVUE-FM IP addresses, which helps to access the GigaVUE-FM instance in case of failures. Consider a DNS name, myfm.com that has the IP addresses of the three GigaVUE-FM instances of the high availability group.

If you type the DNS name of the GigaVUE-FM, myfm.com, the DNS server returns the IP addresses of the three GigaVUE-FM instances, and:

- the Dashboard page of the active GigaVUE-FM instance appears, or
- the High Availability page of the standby GigaVUE-FM instances may appear if the active instance is not reachable, as in the case of a failover. From the High Availability page of the standby instance, you can navigate to the GigaVUE-FM active instance.

This ensures that the GigaVUE-FM High Availability group is always accessible.

Create and Add GigaVUE-FM Instances to HA Group

To add instances and to configure the HA group:

1. Go to  High Availability.
2. Click **Create**. The High Availability wizard appears.
3. In the **Group Name** field, enter a unique name for the HA group.

NOTE: Avoid using functionality names as the group alias when creating an FMHA group. Functionality names typically refer to actions or operations within the system and can cause confusion and conflicts. Choose a unique and descriptive name instead.

4. Choose any one of the following options to encrypt the communication between nodes:
 - **Pre-shared Secret Key** – Encrypts communication between GigaVUE-FM nodes using an application-managed shared secret key. Refer to [Encryption using Pre-Shared Secret Keys](#).
 - **Certificate Based** – Encrypts communication between GigaVUE-FM nodes using manually uploaded certificates. Refer to [Encryption using Pre-Shared Secret Keys](#).

NOTE: When you install or upgrade to GigaVUE-FM version 6.11.xx or later, encrypted communication between high-availability (HA) instances is automatically enabled as part of the deployment process.

- In the **Add GigaVUE-FM Instance** section, the details of the GigaVUE-FM instance from which the HA group is created will be fetched automatically.
- Enter the External IP Address and Third-Party Authentication details, if required. Click the **save** icon to save the configuration.

High Availability

Note:

- There must be atleast three active eligible nodes that are reachable to each other.
- Save each row individually before continuing.

Cancel Submit

Group Name * FMHA1

Encryption Method ☒ Pre-Shared Key ^① ☐ Certificate Based ^①

ADD GigaVUE-FM INSTANCES + Add New Node

IP Address / DNS N... ^①	External IP Address... ^①	Role ^①	Username	Password	Entity ID	Third Party Authen... ^①	Take Action
	Enter External IP Adc	Active Eligible ^①	admin	*****	Enter Entity ID	Enter URL	
	Enter External IP Adc	Active Eligible ^①	admin	*****	Enter Entity ID	Enter URL	
	Enter External IP Adc	Active Eligible ^①	admin	*****	Enter Entity ID	Enter URL	
	Enter External IP Adc	Supporting Node ^①	admin	*****	Enter Entity ID	Enter URL	
	Enter External IP Adc	Supporting Node ^①	admin	*****	Enter Entity ID	Enter URL	

- Click **Add New Node** to add the GigaVUE-FM instances. Enter the following details:
 - IP Address/DNS Name** - IP address/DNS name of the GigaVUE-FM instance (s for communication between the GigaVUE-FMs and to configure the HA group). It is always recommended to use the DNS name while creating the GigaVUE-FM High Availability group.
 - Tunnel IP Address** - IP address used for establishing the secure communication tunnel between HA instances. This is required when the instances are reachable only through public or external IP addresses. If the tunnel IP is the same as the external IP, you can select the auto-populate option.
 - External IP Address** - External IP address of the GigaVUE-FM instance (for accessing the GigaVUE-FM HA from outside the internal network.).
 - Role** - Role of the GigaVUE-FM instance. Can be configured as either:
 - Active Eligible**- provides resiliency and load distribution.
 - Supporting Node**- provides scalability and performance.
 - Username** - GigaVUE-FM admin's username.
 - Password** - GigaVUE-FMadmin's password.
 - Third Party Authentication** - Third-party authentication URL.

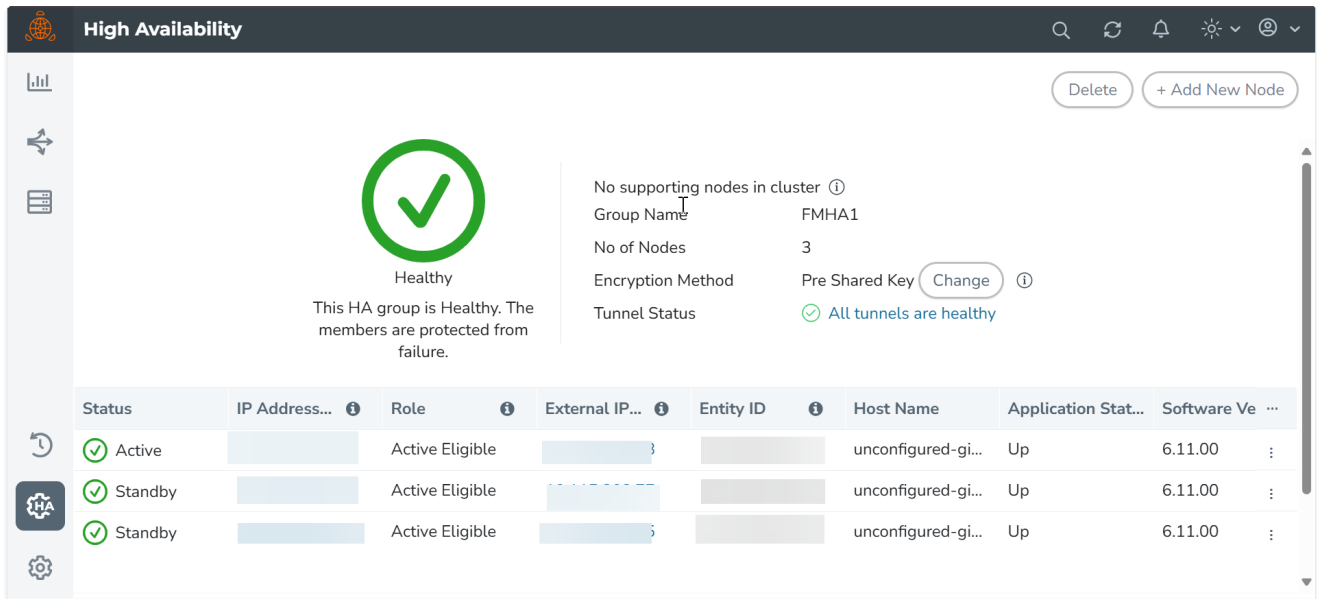
8. Click **Save Node**  to validate the details entered for the instances.

Once three active instances are added to the HA group, the **Submit** button is enabled.

NOTE: When creating a HA group, all the existing data on the first configured GigaVUE-FM instance will be preserved, allowing the system to continue using the data after it is fully set up. However, the data on the subsequent nodes will be lost during the setup.

9. Use the **Add New Node** button to continue to add the GigaVUE-FM HA instances. When adding the instances, define the role of the instances either as:
- Active Eligible
 - Supporting Node
10. Review the details of the GigaVUE-FM instances. Use the **Back** button to go back and change the details.
11. Click the **Edit Node** icon to edit the details of the GigaVUE-FM instances, if required.

After adding the instances to the HA group, click **Submit**. The HA group is configured and will be displayed as follows:



Status	IP Address...	Role	External IP...	Entity ID	Host Name	Application Stat...	Software Ve ...
Active		Active Eligible			unconfigured-gi...	Up	6.11.00
Standby		Active Eligible			unconfigured-gi...	Up	6.11.00
Standby		Active Eligible			unconfigured-gi...	Up	6.11.00

NOTE: When switching between the Pre-shared Secret Key and Certificate-Based options for encrypting communication between nodes, it's important to refresh the GigaVUE-FM to see the updated tunnel status. By clicking the link in the **Tunnel Status**, GigaVUE-FM displays the health status of the FMHA nodes.

Click the ellipses on a GigaVUE-FM instance to perform the following tasks:

- **Edit:** Edit the instance details.
- **Reboot:** Reboot a GigaVUE-FM instance.
- **Remove from group:** Remove an instance from the HA group.

The HA page displays the following details:

Table 5:

Field	Description
Status and Reachability	Status of the GigaVUE-FM instances. Can be: • Active • Standby • Supporting Reachability: •  - indicates that the instances are reachable. •  - indicates that the instances are unreachable.
IP Address/DNS Name	IP address/DNS name of the GigaVUE-FM instances
Role	Role of the GigaVUE-FM instance. Can be configured as follows: • Active Eligible: provides resiliency and load distribution • Supporting Node: provides scalability and performance
Entity ID	Entity ID of GigaVUE-FM. It is a unique alpha-numeric ID that must be configured for SSO authentication.
Host Name	Host name of the GigaVUE-FM instance.
Application Status	Status of application services that are responsible for handling the user requests: • Up: Indicates service is ready to handle the user requests • Down: Indicates service is not ready to handle the user requests with one or more underlying services being down. • In Progress: A state that appears between up and down indicating that the services are initializing.
Software Version	Software version of the GigaVUE-FM instance.
System Uptime	Time since the instance is up and active.
Third Party Authentication URL	Third party authentication URL required for SSO configuration.
Upgrade Status	Upgrade status of GigaVUE-FM. This is displayed only when the upgrade is triggered. Otherwise, this field is empty.

You can add instances to the HA group by clicking the **Add New Node** button, as required. You can also remove the instances from the HA group and reduce the size of the HA group as required. However, while removing the instances ensure to retain the quorum¹ number of instances.

¹Quorum number of instances is the minimum number of instances that must be active-eligible in a HA group. In a HA group with five instances, the quorum number is 3 (based on the formula $n/2+1$).

NOTE: To scale components such as Fabric Health Analytics, topology visualization and to improve the performance of GigaVUE-FM by fully utilizing the resource available, it is recommended to configure three active eligible instances and additional supporting instances.

The following are the behavioral changes observed in the HA group with active, standby and supporting instances:

Task	Scenario	Behavior
Backup and Restore Operation	All active-eligible instances are up and few or all supporting instances are up.	Backup will happen in active instance. During restore, all active-eligible GigaVUE-FMs will be rebooted and will perform the restore operation. Supporting instances will not participate in the restoration.
	Few active-eligible instances are up (Quorum number of instances are up)	Backup will happen in active instances. Restore will not be initiated in this case.
Upgrade Operation	Few instances not being up (either active-eligible or supporting instances not up)	Upgrade will not be initiated.
	Few supporting instances are removed from the HA group after formation of the group	Upgrade will be initiated, and the supporting instances present in HA group will be upgraded first followed by the active-eligible instances.
	All instances are up and running	Upgrade will be initiated in an active instance. Upgrade will be done in a rolling fashion starting with supporting instances and ending with the active-eligible instances.
System Configurations	All instances are active-eligible	All GigaVUE-FM's GUI will be accessible, and user can configure the system through the same
	HA with active-eligible	For supporting instances, GUI will not be available (as application service is shut down). An option is provided in the GUI to turn on the

Task	Scenario	Behavior
	and few Supporting instances	application service and its dependent service(s) and the status can be seen in HA page. You can then configure the system related configuration from the logged in GigaVUE-FM instance once the application status of the supporting instance is up.
Background processes		
-FM Service Distribution	All GigaVUE-FMs are active-eligible instances.	Services will be equally distributed/redistributed among the instances based on the availability of the instances.
	HA group with active-eligible instances and supporting instances.	Services will be distributed/re-distributed only to active eligible instances
-Load Balancer	All GigaVUE-FMs are active-eligible instances.	All GigaVUE-FM API requests will be distributed to all instances in the HA group.
	With supporting instances.	All GigaVUE-FM API requests will be distributed only to active-eligible instances.

Important Recommendations and Notes

Keep in mind the following recommendations and notes when working with the HA group.

GigaVUE-FM cannot support more than 7 active-eligible nodes (this is due to the underlying constraint in MongoDB).

Shrinking the size of the HA group:

- When reducing the size of a HA group that has both active-eligible and supporting instances, it is always recommended to remove the supporting instances first so that the active-eligible instances remain intact in the HA group. If active-eligible instances are removed first from the HA group, then the HA group will become unstable. This, however, depends on the number of active-eligible and supporting instances in the HA group. Consider a GigaVUE-FM HA group with 7 instances. The number of active and supporting instances in a HA group may be as follows:

HA group 1	With 3 active instances and 4 supporting instances	The recommendation is specifically applicable for HA group 1 in which there are only 3 active eligible instances in the group. Removing the active-eligible instances may cause the HA group to become unstable.
HA group 2	With 5 active instances and 2 supporting instances.	The recommendation is not applicable for HA group 2 as removing the active-eligible instances will not impact the stability of the HA group.

For a HA group to be stable, it must have a minimum of two active-eligible instances in the group.

- When reducing the size of HA group from 7 instance to 5 instance or 3 instance, the quorum is re-computed and adjusted accordingly. This is to ensure that the HA group remains intact with the available set of instances.
- When reducing the size of the HA cluster, during removal of an instance make sure to give time for the OpenSearch to rebalance and return to a complete (100%) healthy state before removing the next instance. If you remove the instances subsequently one after the other, the health state of the HA group will turn red as there will be no time for shard rebalancing amongst the available instances. Login to GigaVUE-FM CLI as a root user and execute the following command to check the ES cluster health:

```
curl -XGET "http://localhost:9200/_cluster/health?pretty"
```

Supporting GigaVUE-FM Instances:

- When a supporting instance is added to the HA group, its system information will not be available immediately and will be available only after a minute.
- When the HA group is upgraded, application services of the supporting instances will be turned on automatically for the upgrade and once GigaVUE-FM HA upgrade is completed it will be turned off automatically. Application services will be turned off automatically irrespective of the upgrade completion status, that is, either success or failure.



Notes:

- For supporting instances, system information will be populated into MongoDB as the Application Service is down by default (scheduler populates the system information every minute into MongoDB). Hence any changes in the system hostname or GigaVUE-FM version will be reflected in the GUI only after a minute.
- In case of suspended mode, MongoDB will go into write protected mode. Therefore, any system related updates performed in the supporting nodes will not be reflected in the GUI.



- If the supporting instance is not reachable, all system related information that is populated in the GUI reflects the previous known values and not the latest values for Application Status, Up Time, and other system related information.
- Whenever the application services are up and running, events will be logged in the Events page (with the severity level - Info)

The following table displays operational scenarios and GigaVUE-FM High Availability behaviour.

Scenario	Trigger/Event	Behavior/Notes	
Failover due to FM crash	Active FM becomes unreachable	Standby GigaVUE-FM is promoted to active. Fabric Orchestration resumes automatically.	No manual Intervention required.
UCTC registration in High Availability	New UCTC node added	GigaVUE-FM High Availability master receives registration request. Node registered with fresh inventory sync	Uses POST
Policy deployment after switchover	FMHA leader changes	New recomputes desired state.Policies re-applied, stale entries removed	TAP responds asynchronously
Public IP preference for RMQ	Fabric node behind NAT	GigaVUE-FM High Availability uses public IP for RMQ notifications	Stats reach GigaVUE-FMHigh Availability leader reliably. Configurable via UI checkbox.
Tunnel IP configuration	GigaVUE-FMHigh Availability in Cloud	Tunnel IP field used for external communication	Secure Connectivity Established.
Node heartbeat failure	Node stops sending heartbeat	For supporting instances, GigaVUE-FM High Availability marks node as unreachable. Alerts triggered, node removed if persistent	Uses PUT
Standalone → FMHA migration	Existing GigaVUE-FMupgraded	Node joins HA group	Configuration synced, node re-registered

Encryption of Communication between FMHA Nodes

This feature implements secure data transmission between Fabric Manager High Availability (FMHA) nodes using encryption. This feature aids in securing communications between FMHA nodes with IPSec, using either Pre-shared Secret Keys (PSK) or Certificate-Based Authentication.

Encryption using Pre-Shared Secret Keys

GigaVUE-FM uses a secret key (Pre-Shared Key) to verify and allow access to a secure network. GigaVUE-FM auto generates an AlphaNumeric Random Secret Key without the user intervention and shares automatically with other nodes when they are added to the FMHA group.

By default, GigaVUE-FM employs PSK for authentication, facilitating the establishment of secure tunnels between Fabric Managers within a High Availability (FMHA) cluster.

Encryption using Certificates

Once the FMHA cluster is established, GigaVUE-FM provides you with an option to switch to Certificate-Based authentication through the Graphical User Interface (GUI). This method requires each node within the cluster to have a certificate signed by the same Root Certificate Authority (RootCA), ensuring a higher level of security and trust.

Using expired certificates in GigaVUE-FM and switching the encryption mode to Certificate-Based will result in FMHA nodes communicating without encryption.

NOTE: GigaVUE-FM does not manage the certificates in this feature. You should obtain and maintain the necessary certificates. For instructions on configuring the certificates, refer to [Configure Certificates in FMHA Nodes](#).

Rules and Notes

- FMHA Secure Tunnel Authentication mode uses certificates, and you should manage the certificates manually. When you choose manual management, you should replace any revoked or expired certificates.
- When the FMHA is at risk or all nodes are disconnected, you need to check if the certificates have expired. If they have expired, replace them with the appropriate certificates. Once the right certificates are replaced, [Share Certificates to Peer FMHA Nodes](#) and then restart the IPsec service using **`systemctl restart ipsec.service`** on each FMHA node. If the certificates are not replaced, the communication will not be encrypted.
- To enable encrypted communication between GigaVUE-FM High Availability (HA) cluster members, ensure that UDP ports 4500 and 500 are open, and that Protocols 50 and 51 are allowed. Refer to [Open Ports in GigaVUE-FM](#) to know other open ports for FMHA.

Setting up Certificate (PKI) based Encryption in FMHA

Each GigaVUE-FM has its own private certificate, public certificate, and a chain of Certificate Authority (CA) and Root certificates. It is important to create certificates with different Common Name (CN) or Subject Alternative Name (SAN) for each node. This

prevents issues with certificate replacement in the Network Security Services Database (NSS DB).

Configure Certificates in FMHA Nodes

Prerequisite

You must ensure that the following key usages are added to your certificate before configuring certificates in FMHA nodes (only in PKI mode):

- serverAuth (TLS Web Server Authentication)
- clientAuth (TLS Web Client Authentication)
- ipsecEndSystem
- ipsecTunnel
- ipsecUser

To configure a three-node FMHA using certificate based IPsec tunnel for authentication, follow these steps:

1. [Import Self Certificates for Each FMHA Node to NSS DB](#)
2. [Share Certificates to Peer FMHA Nodes](#)
3. [Import Peer Certificates](#)
4. [Verify Imported Self Node Certificates and Peer Node Certificates on NSS DB](#)
5. [Create fmha.yaml](#)
6. [Switch to Certificate Based From GigaVUE-FM GUI](#)

You must start a shell to execute the procedure outlined below. To do this, after you login you must use the shell command at the fmctl prompt. For more information, refer to [GigaVUE-FM CLI Commands](#).

NOTE: When you configure, the commands must be performed in the Linux shell, which you can access by using the **shell** command.

Import Self Certificates for Each FMHA Node to NSS DB

The certificate chain, which includes the public and private certificates, is packaged in P12 format and can be found at the following location:

```
/etc/gigamon/cms.p12
```

To import the GigaVUE-FM certificate into the NSS (Network Security Services) database, use the following command on each node in the HA cluster:

```
ipsec import /etc/gigamon/cms.p12
```

This command imports the certificate from the **cms.p12** file for the respective node.

A message successfully imported certificate from **cms.p12** will show up with alias : **CMS** on the NSS DB.

To generate **cms.p12** with custom certificates, refer to [Post Installation Configurations](#).

Share Certificates to Peer FMHA Nodes

Use **scp** to copy the **localhost.crt** file from each node to every other node in a three-node FMHA cluster consisting of node-a, node-b, and node-c.

localhost.crt location on each node: **/etc/pki/tls/certs/localhost.crt**

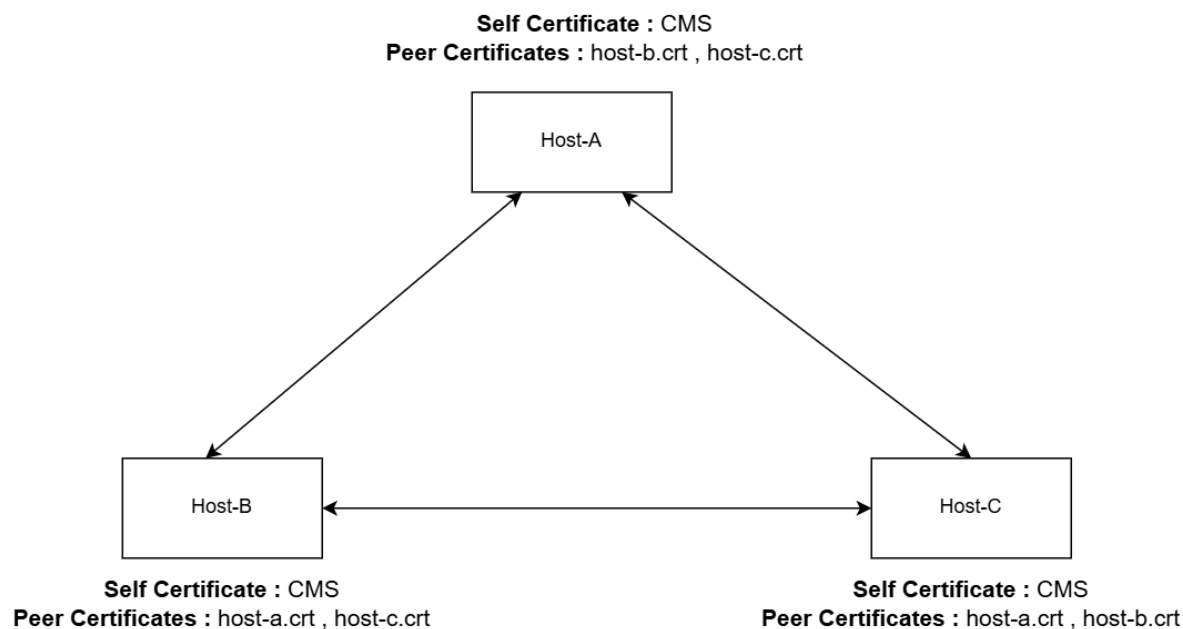
peer node certificate availability in each node

on Host-A : host-b.crt, host-c.crt are peer certificates

on Host-B : host-a.crt, host-c.crt are peer certificates

on Host-C : host-a.crt, host-b.crt are peer certificates

3N FMHA CLUSTER : PKI CONFIG



Import Peer Certificates

Add the imported certificates (Certificate Name of B and C) to the NSS db of **Host-A**:

```
certutil -A -d sql:/etc/ipsec.d -n "hostB" -t "P,P,P" -i host-b.crt
certutil -A -d sql:/etc/ipsec.d -n "hostC" -t "P,P,P" -i host-c.crt
```

Import the peer certificates in each node in HA cluster.

NOTE: Name specified with the -n flag will be used to reference this particular certificate in the fmha.yaml. The name can be GigaVUE-FM's IPv4, IPv6, or DNS address.

Verify Imported Self Node Certificates and Peer Node Certificates on NSS DB

Verify that each node in the FMHA cluster has successfully imported its self-certificate as well as the other peer node certificates to NSS DB using the following command:

```
certutil -L -d /etc/ipsec.d
```

Create fmha.yaml

After importing all the required certificates into the NSS database ([Example:](#)) on all three nodes, you must provide GigaVUE-FM with their details.

Create a new file :

fmha.yaml at **/home/admin** and update the certificate related details for each FMHA node.

fmha.yaml should be available at **/home/admin** location on each GigaVUE-FM node in FMHA cluster.

Example:

Configuring Node A

```
fmtaf@fmqaesxireg9:~/cms_log$ cat fmha.yaml
<Replace with IP address of Node A>:
  cert_name: CMS (Self Certificate Name)
  cert_san: "Replace with SAN"
  cert_type: Replace with Cert type (rsasig/ecdsa)
<Replace with IP address of Node B>:
  cert_name: Certificate name of B
  cert_san: "Replace with SAN"
  cert_type: Replace with Cert type (rsasig/ecdsa)
<Replace with IP address of Node C>:
  cert_name: Certificate name of C
  cert_san: "Replace with SAN"
  cert_type: Replace with Cert type (rsasig/ecdsa)
```

Configuring Node B

```
fmtaf@fmqaesxireg9:~/cms_log$ cat fmha.yaml
```

```
<Replace with IP address of Node B>:
    cert_name: CMS (Self Certificate Name)
    cert_san: "Replace with SAN"
    cert_type: Replace with Cert type (rsasig/ecdsa)

<Replace with IP address of Node C>:
    cert_name: Certificate name of C
    cert_san: "Replace with SAN"
    cert_type: Replace with Cert type (rsasig/ecdsa)

<Replace with IP address of Node A>:
    cert_name: Certificate name of A
    cert_san: "Replace with SAN"
    cert_type: Replace with Cert type (rsasig/ecdsa)
```

Switch to Certificate Based From GigaVUE-FM GUI

Open the FMHA landing page on GigaVUE-FM and select **Certificate Based** authentication to switch to PKI based tunnels for your existing FMHA cluster. If you are creating a new FMHA cluster, select **Certificate Based**(ensure that the certificates are imported in all the nodes) and then click **Submit** to start FMHA cluster creation with tunnel authentication mode as PKI. Refer to [Create and Add GigaVUE-FM Instances to HA Group](#)

Rules and Notes

- Currently supported certificate types : **ecdsa/rsasig**.
- Ensure that the firewall rules allow IPsec traffic UDP ports 500 and 4500, and protocol 50 and 51.
- Ensure that the certificates are correctly signed and trusted among the nodes.
- You can delete the certificate from NSS DB on any FMHA node using the following command. Replace “MYCERT” with the certificate name which you want to remove from NSS DB:

```
certutil -d sql:/etc/ipsec.d -D -n "MYCERT"
```

High Availability for Cloud Infrastructure

This section provides details about the GigaVUE-FM High Availability (HA) feature in Cloud environment and describes how to configure, upgrade, and troubleshoot the feature.

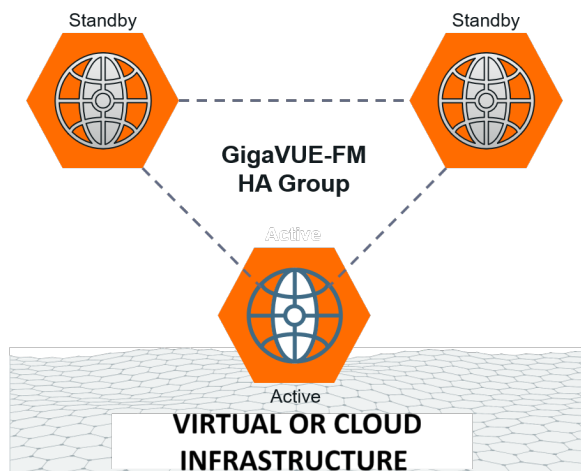
Refer to the following topics for details:

- [About GigaVUE-FM High Availability](#)
- [Supportability Information](#)
- [Recommendations, Rules, Notes, and Limitations](#)
- [Licensing Information](#)
- [Hostname Setups](#)
- [Configure GigaVUE-FM HA](#)
- [Configure Secure Communication between Fabric Components in FMHA](#)
- [GigaVUE-FM HA Landing Page](#)
- [Remove Standby GigaVUE-FM Instance](#)
- [Disassemble GigaVUE-FM High Availability Group](#)
- [GigaVUE-FM High Availability States](#)
- [Fail over Mechanism](#)
- [GigaVUE-FM High Availability Scenarios](#)
- [Troubleshoot GigaVUE-FM High Availability Issues](#)

About GigaVUE-FM High Availability

The GigaVUE-FM High Availability (HA) feature supports a highly available fabric management environment with minimal interruption. The GigaVUE-FM HA architecture consists of a minimum of three GigaVUE-FM instances that run together as a highly available group. The highly available group provides protection from failure of any one of the members in the group. The communication between the GigaVUE-FM instances in the highly available group can be encrypted using Pre-shared Secret Key or Certificate based Authentication.

The following image shows the high-level architecture of the GigaVUE-FM HA feature.



GigaVUE-FM allows you to add more than three GigaVUE-FM instances to the HA group (up to 7). The hardware requirements and resource allocation process for the additional instances are the same as that of the active and standby instances. The additional instances can be configured either as supporting instances or as active-eligible instances:

Supporting instances

Supporting instances are GigaVUE-FMs that run minimal services, thereby providing more resources to OpenSearch services. These instances:

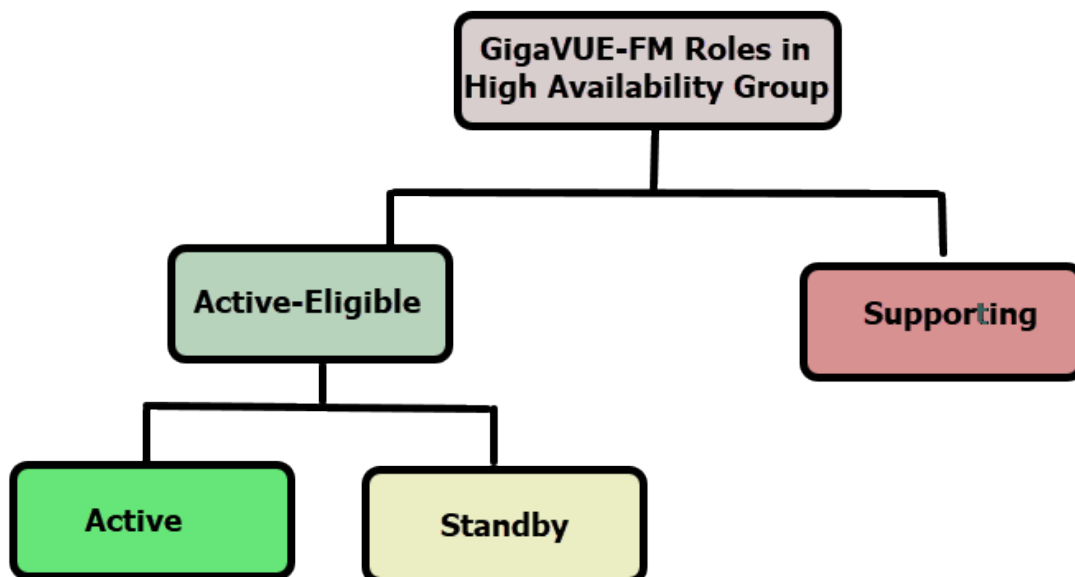
- Do not distribute application requests, as all application services are disabled by default.
- Do not participate in distributed services
- Provide enhanced scalability.
- Are excluded from active instance election

Active-Eligible instances

Active-Eligible instances are GigaVUE-FMs that distribute application requests and run distributed services. These instances:

- Enhance fault-tolerant and high available system.
- Are eligible for active instance election.

Refer to the following diagram for the roles in the HA group.



NOTE: When you add a GigaVUE-FM instance as either a supporting instance or a standby instance, the current configuration of that GigaVUE-FM instance will be removed once it is added to the existing GigaVUE-FM HA cluster.

Gigamon cloud solution deployments in GigaVUE-FM HA are supported on both public and private platforms. These deployments can operate in one of the following modes:

- GigaVUE-FM Orchestrated
- Third-party Orchestrated (Generic / Integrated)

In either scenario, you need to first launch GigaVUE-FM and run.

GigaVUE-FM Orchestration

Using GigaVUE-FM orchestration, you can deploy GigaVUE Fabric Components through the GigaVUE-FM user interface. After launching GigaVUE-FM and applying the required license, you can deploy components such as the GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controller.

Once the deployment is complete, GigaVUE-FM continuously monitors the health and status of the deployed components. If any error condition occurs, GigaVUE-FM automatically relaunches or replaces the affected component to ensure system reliability.

Third-party Orchestration

With this method, you deploy GigaVUE Fabric Components using external orchestration solutions. GigaVUE-FM does not manage the deployment process directly, but you can still use it to monitor the health of the deployed components.

To enable monitoring, you need to provide an additional configuration file during deployment. This file allows components like the GigaVUE V Series Node, GigaVUE V Series Proxy, UCT-V Controller, UCT-V, UCT-C, and GCB to register with the Monitoring Domain in GigaVUE-FM . Refer to the following sections for more details:

- [Deploy GigaVUE Cloud Suite for Third Party Orchestration](#)
- [Deploy UCT-C Solution in Kubernetes](#)
- [Deploy GCB Controller Service and Pods](#)

Supportability Information

The GigaVUE-FM HA feature is supported on the following platforms:

Orchestration Method	Platforms/components Supported
GigaVUE-FM Orchestration	[[[Undefined variable cloudVar.CloudNavPath]]] - Azure - OpenStack - VMware ESXi - VMware NSX-T - Nutanix
Third-party Orchestration	Generic Mode [[[Undefined variable cloudVar.CloudNavPath]]] - Azure - OpenStack - VMware ESXi - VMware NSX-T - Nutanix - GCP - UCT-C - GCB Integrated Mode [[[Undefined variable cloudVar.CloudNavPath]]] - Azure - OpenStack

Recommendations, Rules, Notes, and Limitations

Keep in mind the following recommendations, rules and notes when you configure the GigaVUE-FM HA feature:

Recommendations

- Do not configure GigaVUE-FM High Availability (HA) across multiple regions or multi-cloud environments. This setup is not recommended and may lead to instability.
- You can deploy HA across multiple availability zones within the same cloud region. Ensure that you deploy a GigaVUE-FM instance in each availability zone.
- Use the orchestrated upgrade procedure to upgrade the GigaVUE-FM instances.
- It is recommended to configure reverse DNS configuration while configuring FMHA with FQDN.
- When creating a GigaVUE-FM HA group, it is highly recommended to create the High Availability group using DNS name. GigaVUE-FM HA cannot manage the individual GigaVUE-FM instances if the IP address changes (if GigaVUE-FM IP(s) are dynamic).

Rules and Notes

- GigaVUE-FM cannot support more than 7 active-eligible nodes (this is due to the underlying constraint in MongoDB).

- The GigaVUE-FM instances in the HA group must be identical in terms of system configuration such as hard disk, memory, and network interfaces, which include domain server, NTP server, and name server. Domain server, NTP server, and name server should be configured in all GigaVUE-FM instances.
- The GigaVUE-FMs in the high availability group can be accessed using the IPv4/IPv6 address (DNS name) that is used to form the High Availability group.

NOTE: Do not access all the GigaVUE-FM instances at the same time, as this will impact the performance of the HA group.

- You can deploy the GigaVUE-FM HA virtual machines on a WAN link with a maximum latency of 200 ms.
- You cannot add a GigaVUE-FM Hardware Appliance and a GigaVUE-FM virtual machine in the same HA group.
- The **Reload All** or **Reload any FM** commands will work only if there is an active GigaVUE-FM instance in the HA group.
- You must ensure that NTP is configured across all FM HA nodes.
- The GigaVUE-FM HA Cluster functions like standalone GigaVUE-FM's when a fail-over occurs during long-running operations, such as Fabric Launch, Monitoring Session Deployment, or Fabric Upgrade.
- When FMHA is configured with a reverse proxy, access to GigaVUE-FM requires non-SAML authentication, such as local authentication. Use the following sample URL to access GigaVUE-FM:
`https://<proxy_ip>/admin`
- If GigaVUE-FM has multiple IPv6 addresses, ensure FMHA uses the permanent IPv6 as the source IP. GigaVUE-FM excludes temporary IPv6 addresses from the IP set, which causes connection failures and FMHA formation issues.

Shrinking the size of the HA group:

- When reducing the size of a HA group that has both active-eligible and supporting instances, it is always recommended to remove the supporting instances first so that the active-eligible instances remain intact in the HA group. If active-eligible instances are removed first from the HA group, then the HA group will become unstable. This, however, depends on the number of active-eligible and supporting instances in the HA group. Consider a GigaVUE-FM HA group with 7 instances. The number of active and supporting instances in a HA group may be as follows:

HA group 1	With 3 active instances and 4 supporting instances	The recommendation is specifically applicable for HA group 1 in which there are only 3 active eligible instances in the group. Removing the active-eligible instances may cause the HA group to become unstable.
-------------------	--	--

HA group 2	With 5 active instances and 2 supporting instances.	The recommendation is not applicable for HA group 2 as removing the active-eligible instances will not impact the stability of the HA group.
-------------------	---	--

For a HA group to be stable, it must have a minimum of two active-eligible instances in the group.

- When reducing the size of HA group from 7 instance to 5 instance or 3 instance, the quorum is re-computed and adjusted accordingly. This is to ensure that the HA group remains intact with the available set of instances.
- When reducing the size of the HA cluster, during removal of an instance make sure to give time for the OpenSearch to rebalance and return to a complete (100%) healthy state before removing the next instance. If you remove the instances subsequently one after the other, the health state of the HA group will turn red as there will be no time for shard rebalancing amongst the available instances. Login to GigaVUE-FM CLI as a root user and execute the following command to check the ES cluster health:

```
curl -XGET "http://localhost:9200/_cluster/health?pretty"
```

Supporting GigaVUE-FM Instances:

- When a supporting instance is added to the HA group, its system information will not be available immediately and will be available only after a minute.
- When the HA group is upgraded, application services of the supporting instances will be turned on automatically for the upgrade and once GigaVUE-FM HA upgrade is completed it will be turned off automatically. Application services will be turned off automatically irrespective of the upgrade completion status, that is, either success or failure.



Notes:

- For supporting instances, system information will be populated into MongoDB as the Application Service is down by default (scheduler populates the system information every minute into MongoDB). Hence any changes in the system hostname or GigaVUE-FM version will be reflected in the GUI only after a minute.
- In case of suspended mode, MongoDB will go into write protected mode. Therefore, any system related updates performed in the supporting nodes will not be reflected in the GUI.
- If the supporting instance is not reachable, all system related information that is populated in the GUI reflects the previous known values and not the latest values for Application Status, Up Time, and other system related information.



- Whenever the application services are up and running, events will be logged in the Events page (with the severity level - Info)

Licensing Information

You must install a Prime license on the active GigaVUE-FM instance to configure a High Availability group.

If the Prime license expires or if you accidentally delete the license, the existing configurations will still be present in the GigaVUE-FMs that are part of the HA group, but you will not be able to perform any new configurations. Moreover, if you disassemble the HA group, you cannot reconfigure the HA group without installing a valid Prime license. You can re-use the same Prime license to form the HA group again.

Hostname Setups

The GigaVUE-FM instances are not required to be in the same subnet, but still must be able to communicate with each other.

In addition, ensure that the instances have unique host names. You must be able to ping a GigaVUE-FM instance from the other instances using the hostname or the IP address.

To add a GigaVUE-FM instance to a GigaVUE-FM HA group:

- The GigaVUE-FM instances in the HA group must be reachable to each other.
- If host names are used to configure the HA group, the host names of the GigaVUE-FM instances must be resolvable through a DNS server.

Configure GigaVUE-FM HA

To configure the GigaVUE-FM HA feature, you must have access to at least three authenticated GigaVUE-FM instances that reside on a trusted network. All GigaVUE-FM instances must run the same software version. The interfaces in the GigaVUE-FM instances must be up and must be assigned IPv4/IPv6 addresses. You can also choose to use DNS host names.

NOTE: You can configure the GigaVUE-FM HA feature only if you have administrative privileges. You must have Prime license installed for forming the GigaVUE-FM HA group.

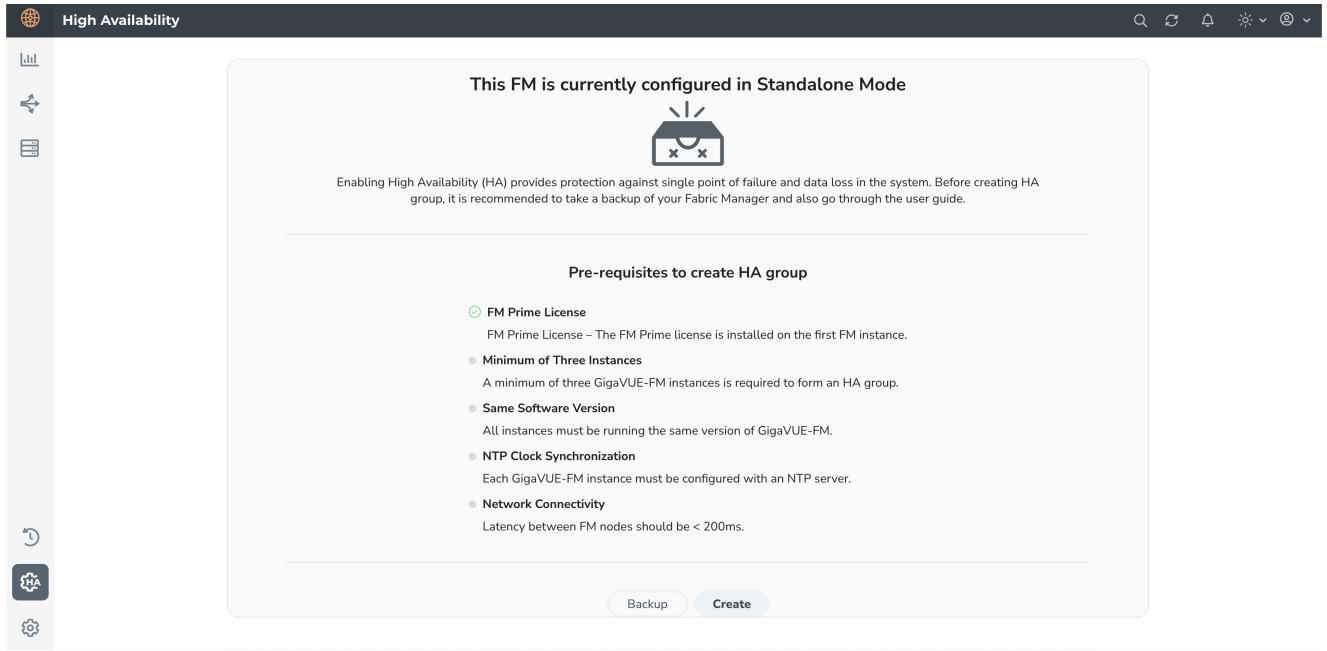
Refer to the following sections:

- [Create and Add GigaVUE-FM Instances to HA Group](#)
- [Connect GigaVUE-FM High Availability to a Monitoring Domain using GigaVUE-FM Orchestration](#)
- [Connect GigaVUE-FM High Availability to a Monitoring Domain using Third Party Orchestration](#)
- [Integrate GigaVUE-FM High Availability with UCT-C](#)
- [Integrate GigaVUE-FM High Availability with Gigamon Containerized Broker](#)

Create and Add GigaVUE-FM Instances to HA Group

To add instances and to configure the HA group:

1. Go to  High Availability. The launch page displays the required prerequisites to create a HA group.



2. Click **Create**. In the **Group Name** field, enter a unique name for the HA group.

NOTE: Avoid using functionality names as the group alias when creating an FMHA group. Functionality names typically refer to actions or operations within the system and can cause confusion and conflicts. Choose a unique and descriptive name instead.

3. Choose any one of the following options to encrypt the communication between nodes:
 - **Pre-shared Secret Key** – Encrypts communication between GigaVUE-FM nodes using an application-managed shared secret key. Refer to [Encryption using Pre-Shared Secret Keys](#).
 - **Certificate Based** – Encrypts communication between GigaVUE-FM nodes using manually uploaded certificates. Refer to [Encryption using Pre-Shared Secret Keys](#).
4. In the **Add GigaVUE-FM Instance** section, the details of the GigaVUE-FM instance from which the HA group is created will be fetched automatically.

Edit the Primary Node

1. On the first instance, click the ellipses icon and select **Edit Node**.
2. Enter the following details: (These fields are optional)

- Select the **Use Tunnel IP** check box to enable tunnel configuration. Selecting this check box reveals two additional fields:
 - **Tunnel IP Address/DNS Name:** IP address used for establishing the secure communication tunnel between HA instances. This is required when the instances are reachable only through public or external IP addresses.
 - **External IP Address / DNS Name is same as Tunnel IP Address / DNS Name:** If you check this box, GigaVUE-FM automatically copies the value from the Tunnel IP field to the External IP field and disables manual editing. If you uncheck it, the External IP field becomes editable again, retaining the previously entered value.
 - Enter the Entity ID and the IdP Metadata URL.
3. Click the **save** icon to save the configuration. Refer to [Additional Fields](#) for details about other fields displayed on the HA page.

High Availability

Create New There must be atleast three active eligible nodes that are reachable to each other. Cancel Submit

Group Name *

Secure Communication ☒ Pre-Shared Key ☐ Certificate Based

Add GigaVUE-FM Instances Add New Node

IP ADDRESS / DNS NAME	TUNNEL IP ADDRESS / D...	EXTERNAL IP ADDRESS / ...	ROLE	USERNAME	PASSWORD	ENTITY ID	IDP METADATA URL	
fcab0:1:2200:96ae:3c8...	—	—	Active Eligible	admin	*****	—	—	...

Add New Node

1. Click **Add New Node** to add the GigaVUE-FM instances. Enter the following details:
 - **IP Address/DNS Name** - IP address/DNS name of the GigaVUE-FM instances (for communication between the GigaVUE-FMs and to configure the HA group). It is always recommended to use the DNS name while creating the GigaVUE-FM High Availability group.
 - (Optional) Select the **Use Tunnel IP** check box to enable tunnel configuration. Selecting this check box reveals two additional fields:
 - **Tunnel IP Address/DNS Name:** IP address used for establishing the secure communication tunnel between HA instances. This is required when the instances are reachable only through public or external IP addresses.

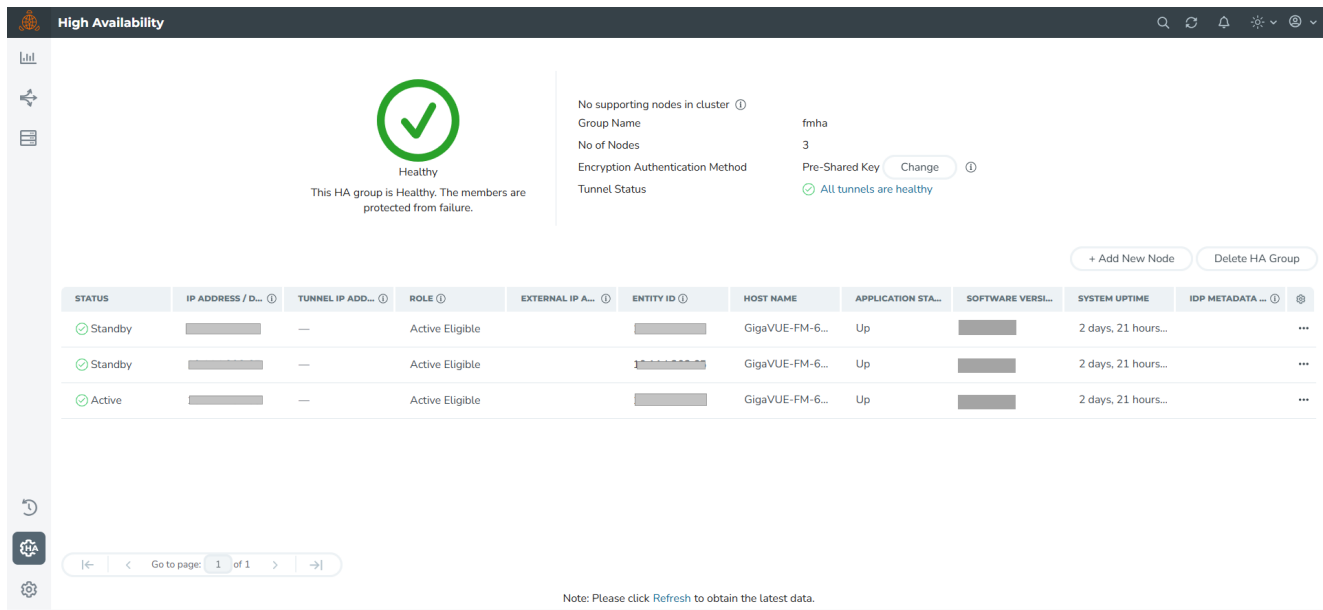
- **External IP Address / DNS Name is same as Tunnel IP Address / DNS Name:** If you check this box, GigaVUE-FM automatically copies the value from the Tunnel IP field to the External IP field and disables manual editing. If you uncheck it, the External IP field becomes editable again, retaining the previously entered value.
- When you add a new node with a Tunnel IP address to an existing HA group, the FMHA table updates to reflect the information in the newly added column.

**Notes:**

- When you add a new node with a Tunnel IP address to an existing HA group, the FMHA table updates to reflect the information in the newly added column.
- When using unique DNS for HA cluster configuration, ensure it always resolves to only one IP address—not multiple IPs.

- **Role** - Role of the GigaVUE-FM instance. Can be configured as below. Refer to [Active-Eligible instances](#) for details.
 - **Active Eligible**- provides resiliency and load distribution.
 - **Supporting Node**- provides scalability and performance.
 - **Username** - GigaVUE-FM GUI Username.
 - **Password** - GigaVUE-FM GUI password.
 - (Optional) **Entity ID** - Unique alphanumeric ID assigned to the GigaVUE-FM instance
 - (Optional) **IdP Metadata URL** - URL pointing to the IdP's XML configuration
2. Click **Save** to validate the details entered for the instances.

Use the **Add New Node** button to continue to add the GigaVUE-FM HA instances. You can click the **Edit Node** icon to change the external IP address. After adding the instances to the HA group, click **Submit**. The HA group is configured and will be displayed as follows. Refer to [Additional Fields](#) for details about other fields displayed on the HA page.



High Availability

Healthy
This HA group is Healthy. The members are protected from failure.

No supporting nodes in cluster ⓘ
Group Name: fmha
No of Nodes: 3
Encryption Authentication Method: Pre-Shared Key ⓘ
Tunnel Status: All tunnels are healthy

+ Add New Node Delete HA Group

STATUS	IP ADDRESS / D...	TUNNEL IP ADD...	ROLE	EXTERNAL IP A...	ENTITY ID	HOST NAME	APPLICATION STA...	SOFTWARE VERSI...	SYSTEM UPTIME	IDP METADATA ... ⓘ
Standby		—	Active Eligible			GigaVUE-FM-6...	Up		2 days, 21 hours...	...
Standby		—	Active Eligible			GigaVUE-FM-6...	Up		2 days, 21 hours...	...
Active		—	Active Eligible			GigaVUE-FM-6...	Up		2 days, 21 hours...	...

Go to page: 1 of 1

Note: Please click Refresh to obtain the latest data.



Notes:

- When switching between the Pre-shared Secret Key and Certificate-Based options for encrypting communication between nodes, it's important to refresh the GigaVUE-FM to see the updated tunnel status. By clicking the link in the **Tunnel Status**, GigaVUE-FM displays the health status of the FMHA nodes.
- When creating a HA group, all the existing data on the first configured GigaVUE-FM instance will be preserved, allowing the system to continue using the data after it is fully set up. However, the data on the subsequent nodes will be lost during the setup.

The HA page also displays the following details:

Table 6: Additional Fields

Field	Description
Status and Reachability	Status of the GigaVUE-FM instances. Can be: - Active - Standby - Supporting Refer to Active-Eligible instances for details. Reachability: 🟢 - indicates that the instances are reachable. ⚠️ - indicates that the instances are unreachable.
Host Name	Host name of the GigaVUE-FM instance.
Application Status	Status of application services that are responsible for handling the user requests: Up: Indicates service is ready to handle the user requests

Field	Description
	• Down: Indicates service is not ready to handle the user requests with one or more underlying services being down. • In Progress: A state that appears between up and down indicating that the services are initializing.
Software Version	Software version of the GigaVUE-FM instance.
System Uptime	Time since the instance is up and active.
Third Party Authentication URL	Third party authentication URL required for SSO configuration.
Upgrade Status	Upgrade status of GigaVUE-FM. This is displayed only when the upgrade is triggered. Otherwise, this field is empty.

You can also remove the instances from the HA group and reduce the size of the HA group as required. However, while removing the instances ensure to retain the quorum¹ number of instances.

NOTE: To scale components such as Fabric Health Analytics, topology visualization and to improve the performance of GigaVUE-FM by fully utilizing the resource available, it is recommended to configure three active eligible instances and additional supporting instances.

The following are the behavioral changes observed in the HA group with active, standby and supporting instances:

Task	Scenario	Behavior
Upgrade Operation	Few instances not being up (either active-eligible or supporting instances not up)	Upgrade will not be initiated.
	Few supporting instances are removed from the HA group after formation of the group	Upgrade will be initiated, and the supporting instances present in HA group will be upgraded first followed by the active-eligible instances.
	All instances are up and running	Upgrade will be initiated in an active instance. Upgrade will be done in a rolling fashion starting with supporting instances and ending with the active-eligible instances.
System Configurations	All instances are active-eligible	All GigaVUE-FM's GUI will be accessible, and user

¹Quorum number of instances is the minimum number of instances that must be active-eligible in a HA group. In a HA group with five instances, the quorum number is 3 (based on the formula $n/2+1$)).

Task	Scenario	Behavior
		can configure the system through the same
	HA with active-eligible and few Supporting instances	For supporting instances, GUI will not be available (as application service is shut down). An option is provided in the GUI to turn on the application service and its dependent service(s) and the status can be seen in HA page. You can then configure the system related configuration from the logged in GigaVUE-FM instance once the application status of the supporting instance is up.
Background processes		
-FM Service Distribution	All GigaVUE-FMs are active-eligible instances.	Services will be equally distributed/redistributed among the instances based on the availability of the instances.
	HA group with active-eligible instances and supporting instances.	Services will be distributed/re-distributed only to active eligible instances
-Load Balancer	All GigaVUE-FMs are active-eligible instances.	All GigaVUE-FM API requests will be distributed to all instances in the HA group.
	With supporting instances.	All GigaVUE-FM API requests will be distributed only to active-eligible instances.

Connect GigaVUE-FM High Availability to a Monitoring Domain using GigaVUE-FM Orchestration

When fabric nodes need to communicate with GigaVUE-FM using public IP addresses, you should enable the **Use Public IP** option during Monitoring Domain creation. When **Use Public IP** option is enabled, GigaVUE-FM pushes its public IP address to Fabric Nodes. Fabric Nodes use this IP to communicate back to FM. FM does not initiate communication using its private IP. This setting is essential in cloud or hybrid environments where private IPs are not reachable, such as across cloud platforms. It

ensures that GigaVUE-FM can send notifications and accept registrations using an externally accessible IP. Refer to [Supportability Information](#) for the list supported platforms.

Connect GigaVUE-FM High Availability to a Monitoring Domain using Third Party Orchestration

Fabric Nodes can be configured with either the IP address (remoteIP) or the Fully Qualified Domain Name (FQDN) (remoteAddress) of GigaVUE-FM to establish communication. The node sends registration requests to GigaVUE-FM until it successfully registers. In High Availability mode, if a node fails to register with one GigaVUE-FM instance, it automatically attempts registration with the next available GigaVUE-FM in its list until successful. Refer to [Supportability Information](#) for the list supported platforms.

Use the following data to manually configure **/etc/gigamon-cloud.conf** with registration configurations to register the fabric components with GigaVUE-FM.

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name/Alias>
  token: <Token>
  remoteAddress: <remoteIPs/FQDN of the GigaVUE-FM>
  remotePort: 443
  sourceIP: <IP address of the fabric node>
  nameServer: <DNS server's IP address>
  usePublicIP: <true/false>
  preferV6: <true/false><If set to true IPv6 will be preferred over IPv4, used only for DNS resolution>
```



Notes:

- Configure either remoteIP or remoteAddress—not both. Using both prevents the node from registering with GigaVUE-FM.
- Remote IP will continue to work as expected. However, if you plan to use FQDN, update the configuration to use the Remote Address field instead.
- When configuring a remote address, you can specify multiple IP addresses. However, if you use a FQDN, ensure that you configure only one address
- FQDN configuration requires a valid nameserver.
- Ensure that the FQDN configured for Third Party Orchestration resolves to all IP addresses in the High Availability cluster.

Integrate GigaVUE-FM High Availability with UCT-C

UCT-C supports integration with GigaVUE-FM in high availability mode. You can configure the controller with either a Fully Qualified Domain Name (FQDN) or a comma-separated list of GigaVUE-FM IP addresses in the Helm configuration. The controller iterates through the provided FQDN or IP list and attempts to register with the master

GigaVUE-FM node. If the GigaVUE-FM IP changes, you must update the configuration again. This enhancement enables UCT-C to maintain connectivity and recover from GigaVUE-FM failover events in HA deployments.

Below are the communication parameters:

- **fm_fqdn** – Specifies the GigaVUE-FM HA FQDN value used by the UCT-C Controller for communication with the GigaVUE-FM HA group. When this parameter is set, the controller uses the IP addresses resolved from the FQDN.
- **fmha_ip_list** – Specifies a comma-separated list of GigaVUE-FM HA IP addresses used by the UCT-C Controller for communication with the GigaVUE-FM HA group. If fm_fqdn is not set, the controller uses the IP addresses provided in fmha_ip_list by default.

Integrate GigaVUE-FM High Availability with Gigamon Containerized Broker

GigaVUE-FM High Availability group can be configured in an Gigamon Containerized Broker through a DNS Server in which the GigaVUE-FM instances are launched and deployed in the Gigamon Containerized Broker environment.

For GCB to make use of high availability feature of GigaVUE-FM, you must configure the FQDN (Fully Qualified Domain Name) of the GigaVUE-FM.

In a standalone GigaVUE-FM, the GCB uses the FQDN name of the GigaVUE-FM (if configured). It uses the legacy method of using the configured IP address when:

- The FQDN is not configured or
- The GCB fails to resolve to an IP address.

For example:

GCB Controller YAML file:

```
env:
  - name: GCB_CNTLRL_EXT_IP_DNS
    value: "10.xxx.xx.xx" (IP address of the DNS server - external to the
    Kubernetes cluster)
  - name: FM_FQDN
    value: "fm.myorg.com" (FMs FQDN that is used for DNS lookups)
```

NOTE: The FQDN identifies either a standalone GigaVUE-FM or an FMHA cluster that includes multiple GigaVUE-FM instances. It returns the IP addresses (IPv4, IPv6, or both) for all GigaVUE-FMs associated with that FQDN.

For more details on the GigaVUE-FM High Availability configuration, refer to the *GigaVUE Administration Guide* guide.

Configure Secure Communication between Fabric Components in FMHA

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

Follow these steps:

1. Access the active GigaVUE-FM via CLI.
2. Archive the stepCA directory using the following commands:

```
sudo su
cd /var/lib
tar -cvf /home/admin/stepca.tar stepca
```
3. Set the permissions of the tar file using the following commands:

```
chmod 666 /home/admin/stepca.tar
```
4. Copy the tar file to all standby instances in the **/home/admin/ directory** using scp:

```
scp /home/admin/stepca.tar <standby-node>:/home/admin/
```
5. Download the **runstepca_fmha** script from the Community Portal.
6. Log in to the standby instance using CLI.
7. Copy the script in the standby instance in the **/home/admin directory** and execute it using the following command:

```
sh /home/admin/runstepca_fmha
```

GigaVUE-FM HA Landing Page

When you login to any of the GigaVUE-FM instances of the HA group, the dashboard page appears. Use the drop-down option in the header of GigaVUE-FM, which is available on specific pages, to view the details pertaining to that GigaVUE-FM. For example, the following pages in the GigaVUE-FM GUI have drop-down option in the header:

- FM Health
- IP Resolver
- [NTP Server for Clock Synchronization](#)

Remove Standby GigaVUE-FM Instance

To remove or replace a standby GigaVUE-FM instance from the GigaVUE-FM HA group follow the below listed steps:

1. Go to  High Availability.
2. Click the ellipsis on the standby GigaVUE-FM instance widget in the High Availability page as shown in [Figure 34Remove Standby GigaVUE-FM Instance](#).

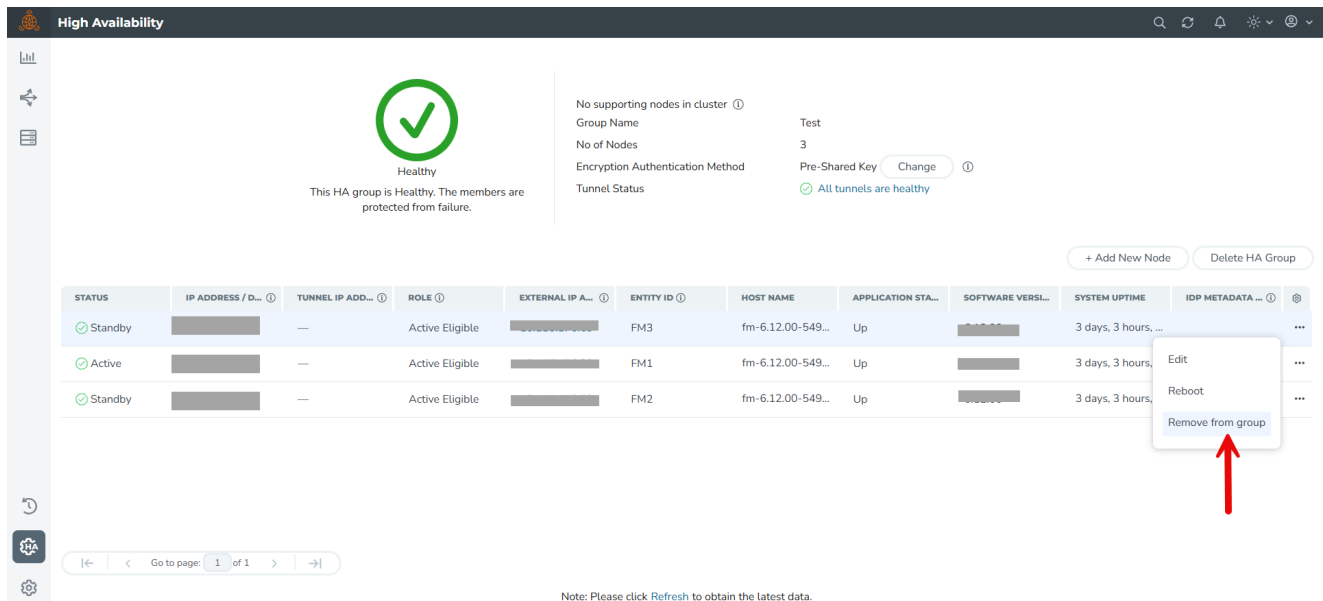


Figure 34 Remove Standby GigaVUE-FM Instance

3. Select the **Remove from group** option and confirm your changes. The selected standby GigaVUE-FM instance is removed from the GigaVUE-FM HA group.

NOTE: The status of the GigaVUE-FM HA group changes from **Healthy** to **At Risk**. You will not be allowed to remove the other standby GigaVUE-FM instance after the HA status changes to **At Risk**. To remove the standby node, if there is any network latency in GigaVUE-FM and the node is not removed correctly, use the command **fmcs remove force** in the GigaVUE-FM CLI of the standby node.

Disassemble GigaVUE-FM High Availability Group

To completely disassemble the GigaVUE-FM HA group:

1. Go to  High Availability.

NOTE: You cannot remove an active GigaVUE-FM instance or disassemble the GigaVUE-FM HA group by logging in from a standby GigaVUE-FM instance.

2. Click the **Delete HA group** option on the High Availability page and confirm your changes. The GigaVUE-FM HA group will be disassembled and each of the GigaVUE-FM instances become standalone GigaVUE-FM instances.

NOTE: Executing the above steps disassembles the GigaVUE-FM HA group completely. The database of the individual GigaVUE-FM HA group members (active, standby, and supporting instances) will be erased and reinitiated with the default database. If you had performed orchestrated configuration flows (such as

the Flexible Inline Arrangement or Intent Based Orchestration) you must manually remove and recreate these if they do not backup the GigaVUE-FM database before choosing Delete HA Group.

If you cannot access the active GigaVUE-FM instance's GUI, use the following CLI command in all the GigaVUE-FM instances to disassemble the HA group:

/opt/fmcs/bin/fmcs leave force

Before disassembling the instances, take a backup of the configuration. After the GigaVUE-FM instances are disassembled from the HA group, the configurations present in the instances will be completely removed.

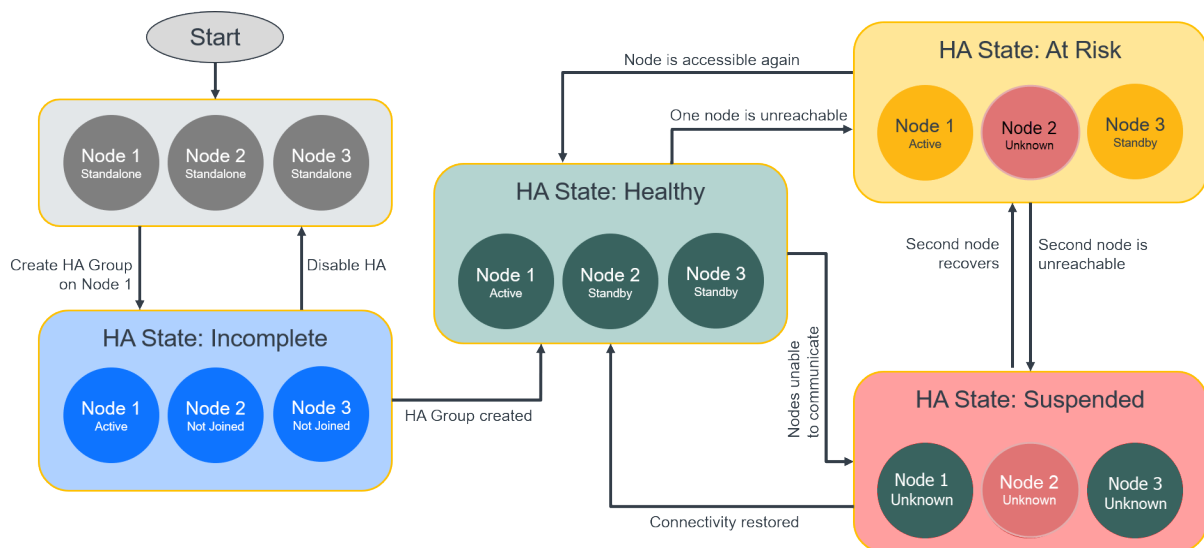
GigaVUE-FM High Availability States

The GigaVUE-FM HA state depends on the status of the three GigaVUE-FM instances. The following table lists the various states of the GigaVUE-FM HA group. You can view the HA group state from **Administration > High Availability** in the GigaVUE-FM GUI.

Table 7: High Availability States

State	Number of GigaVUE-FM Instances	Description
Healthy	Three GigaVUE-FM instances are up and running	One GigaVUE-FM instance is in active state. Other two instances are in standby state.
At Risk	Two GigaVUE-FM instances are up and running	One GigaVUE-FM instance is in active state. Another GigaVUE-FM instance is in standby state. The third GigaVUE-FM instance has either not joined the HA group or has left the HA group. NOTE: You must recover the standby GigaVUE-FM instance within 3 days (72 hours). Failure to do so will cause the instance to move out of the High Availability group.

State	Number of GigaVUE-FM Instances	Description
Incomplete	One GigaVUE-FM instance is up and running	Only one GigaVUE-FM instance is in active state. The other two GigaVUE-FM instances have either not joined the HA group or have left the HA group.
Standalone	One GigaVUE-FM instance is up and running	HA is not configured on the GigaVUE-FM instance.
Suspended	Two or more GigaVUE-FM instances are up and running	HA is configured, but an active GigaVUE-FM instance is yet to be elected. NOTE: The GigaVUE-FM high availability group can move to a Suspended state from the At Risk state when the HA group has only one active-eligible and reachable GigaVUE-FM instance. Events will not be captured for the status of the GigaVUE-FM instance that went down (which causes the HA group to move into a suspended state) as there is no active/leader instance in the High Availability group.



In case of FMHA going to suspended mode from At-Risk mode, the reachability status of node which went down (due to which HA went into suspended mode) won't be audited as writes are not accepted if there is no active/leader instance in the DB cluster

Figure 35 High Availability States

Fail over Mechanism

The active GigaVUE-FM instance in the high availability group may fail at times resulting in one of the standby instances to take over and become the active instance. This process is called failover.

The following table provides the reasons for failover:

Reason for Failover	Description
Reloading the active GigaVUE-FM instance	An active GigaVUE-FM instance is reloaded (using the Reboot option) to bring back the HA group to healthy state again.
Planned downtime of the active GigaVUE-FM instance	An active GigaVUE-FM instance is brought down due to various reasons, for example to upgrade to a newer software version.
Monitoring session deployment during HA leader switchover	The new leader automatically redeploys Monitoring Sessions that failed during the switchover.
Node registration during HA leader switchover	Registration requests may temporarily fail or be delayed. Fabric nodes automatically retry registration. The new leader's IP address is configured as the RMQ notification target on all fabric nodes.
Certificate handling or fabric deployment/upgrade during HA leader switchover	The newly elected leader resumes certificate handling and continues any in-progress fabric deployment or upgrade from the last known state. No manual intervention is required.

GigaVUE-FM High Availability Scenarios

The High Availability page displays the current state of the GigaVUE-FM HA group. When a failover occurs, the HA group state changes in the GUI.

The following table lists the GUI changes for the various scenarios:

Scenario	Changes in GUI
What happens to the High Availability page immediately after a failover?	The High Availability page may not update immediately or may not show all the GigaVUE-FM instances. NOTE: Refresh the page after a minute to view the new active GigaVUE-FM instance. However, the page will get updated automatically after 5 minutes.
What happens to an active GigaVUE-FM instance when it	One of the standby GigaVUE-FM instances changes to the active state. The GigaVUE-FM instance that was initially in the active state

Scenario	Changes in GUI
fails (either by itself or if failover is triggered manually)?	changes to the standby state. It takes a few seconds for this transition. The GigaVUE-FM GUI of the new active instance will have all the menus and dashboards.
What happens to the GigaVUE-FM instances that were previously in standby state?	- One of the standby GigaVUE-FM instances changes to the active state - The other standby GigaVUE-FM instance remains in the standby state.
What happens to the embedded devices when a new Active instance takes over?	There are no changes to the devices except that they are being managed by the new active GigaVUE-FM instance.
How do you trigger a failover?	Click on the 'Reboot' option on the current active GigaVUE-FM instance to trigger a failover.

Troubleshoot GigaVUE-FM High Availability Issues

Use the following table to troubleshoot issues that you might encounter while working with the HA feature.

Problem	Solution
Unable to add a license to GigaVUE-FM HA group after a failover Reason: Using the MAC Address in the About page to generate the license	Always use the Challenge MAC Address in the Licenses page of the active GigaVUE-FM instance to generate licenses. Add the licenses to the HA group.
Unable to join the GigaVUE-FM HA group after changing the password Reason: Not logging out of GigaVUE-FM after changing the password and before joining the HA group	Always logout of GigaVUE-FM after changing the password and login again with the new password before joining the HA group.

What Next?

You must add nodes and cluster to GigaVUE-FM after completing your administrative task in GigaVUE-FM. To learn about adding managing nodes and clusters for a device, refer to Manage GigaVUE Nodes and Clusters section of the corresponding [Physical Appliances Guide](#).

Software Licensing Reference

Refer to the GigaVUE Licensing Guide for details.

Setting the GigaVUE-FM Admin Password

You can set the admin password for GigaVUE-FM from the GigaVUE-FM Command-line Interface (CLI) or from the GigaVUE-FM GUI. This topic describes the requirements for the password.

The characters in the admin password must include, at least:

- At least 8 characters and up to a maximum of 64 characters in length
- One numerical character
- One upper case character
- One lower case character
- One special character from -!@#\$%^&*()+

If the password does not meet the complexity requirements:

- The system does not display any error message.
- The parameters configured above are not passed on to the GigaVUE-FM except the host name parameter.
- The static IP addresses that were configured originally will be unavailable after GigaVUE-FM is deployed.

Setting the Admin Password from the GigaVUE-FM CLI

The password can be a minimum of 14 characters and a maximum of 255 characters, and must comply with the character requirements specified above.

NOTE: The password that you set from the GigaVUE-FM CLI is applicable only to the GigaVUE-FM CLI.

Setting the Admin Password from the GigaVUE-FM GUI

You must change the default admin password when you first login to the GigaVUE-FM UI. The default username and password for a admin user in GigaVUE-FM GUI is *admin* and *admin123A!@*, respectively. If GigaVUE-FM is deployed inside AWS or OpenStack, then the default password is the **Instance ID**. You can change the default admin password from GUI. The password can be a minimum of 8 characters and a maximum of 64 characters, and must comply with the character requirements specified above.

NOTE: The password that you set from the GigaVUE-FM GUI is applicable only to the GigaVUE-FM GUI.

Logging in to GigaVUE-FM Command Line Interface

Access to the Linux shell prompt is now restricted and will be removed in a future release. When you log into the GigaVUE-FM CLI, you can view the **fmctl** command prompt instead of a bash shell. To access the bash shell, use the **shell** command. In the future, access to bash through the **shell** command needs Gigamon support.

NOTE: If you enter an incorrect password three times, your account will be locked for 10 minutes as a security measure. After this 10-minute lockout period, you can attempt to log in again using the correct password.

Refer to the following sections for more information:

- [GigaVUE-FM CLI Commands](#)
- [Post Installation Configurations](#)

GigaVUE-FM has all the required software pre-installed to perform the various functions. Unless directed by Gigamon, do not install any third-party software, and Gigamon explicitly does not recommend the installation of any such software.

Important: Installing Third-party software in GigaVUE-FM can have adverse effects on the operation of GigaVUE-FM. Uninstall all third-party software prior to contacting Gigamon Support for troubleshooting.

GigaVUE-FM CLI Commands

GigaVUE-FM CLI commands assist you in configuring GigaVUE-FM, performing administrative tasks, and conducting maintenance activities. These tasks include system backups, image management, interface configuration, network settings, logging, and security controls, which may be challenging to accomplish through the GigaVUE-FM UI. You can access the GigaVUE-FM CLI via SSH or through the console.

Access to the Linux shell prompt is restricted. When you log into the GigaVUE-FM CLI, you can view the **fmctl** command prompt instead of a bash shell. To access the bash shell, use the **shell** command.

NOTE: If you enter an incorrect password three times, your account will be locked for 10 minutes as a security measure. After this 10-minute lockout period, you can attempt to log in again using the correct password.

This section describes the commands for the GigaVUE-FM Command-Line Interface (CLI) related to installation and upgrade processes.

fmctl

Use the **fmctl** command to manage GigaVUE-FM-related configurations.

The **fmctl** command has the following syntax:

fmctl

shell

help

exit

configuration [backup|restore][<absolute pathname of backup file>]

image

fetch <download URI> [<filename>]

list [details] [<filename>]

install <filename> [next|location {1|2}]

boot [next|location {1|2}]

delete [force] <filename>

{move|rename} <old filename> <new filename>

show

logging [<fqdn>[:<port>]] [facility <facility>] [priority <priority>] [udp|tcp|tls]

logging <ipaddress> [port <port number>] [facility <facility>] [priority <priority>] [udp|tcp|tls]

no logging <fqdn>[:<port>]

no logging <ipaddress> [port <port number>]

reset factory halt

set crypto enable

get crypto

set audit network enable

set audit network disable

get audit network

set crl enable

get crl

set UI admin password <new password>

```

{get|show} interface [{mgmt|management}]
set interface {mgmt|management} <interface name>
[options{--help|--interface <interface name>}]
  set mapping <fqdn> <IP address>
  {get|show} {ip|ntp|hostname|domain|fqdn}
  set [ip|ip6] dhcp
  set [ip|ip6] [static] <address/cidr> [<gateway> [<dns1>[,<dns2>[,...]]]]
  set {ip|ip6} route {add|remove} address/cidr gateway
  set ntp disable [<server1>[,<server2>[,...]]]
  set ntp enable [version <version_number>] [<server>[:<key_id>:<key_
type>:<key_value>[,...]]]
  set ntp update [version <version_number>] [<server>[:<key_id>:<key_
type>:<key_value>]]
  set hostname <hostname>
  set domain <domain>
  set fqdn <hostname> <domain>
  set/get/show searchdomains [<domain1>[,<domain2>[,...]]]
  set/get/show nameservers [<dns1>[,<dns2>[,...]]]
  show backup [<absolute pathname of backup file>]
unlock UI <username>

```

NOTE: You must reboot the GigaVUE-FM, when there is a change in the IP address of the GigaVUE-FM.

The following table describes the arguments for the **fmctl** command:

Argument	Description
configuration [backup restore]	Backs up and restores the configurations such as management interface, hostname, domain, IP, search domains, and NTP. For example, use the following command to back up the system configurations: configuration backup <absolute path name of backup file> Use the following command to restore the system configurations from the backup: configuration restore <absolute path name of backup file>
image fetch <download URI> [<filename>]	Retrieves an image file from a remote host. Use HTTP(S), FTP, or SCP to retrieve the file. The format for the download URL is as follows: [protocol]://username [:password]@hostname:/path/filename For example, the following command retrieves the image file named myimage from the FTP server at 192.168.1.10 using the robh account with the xray password:

Argument	Description
	image fetch ftp://robh:xray@xxx.xxx.x.x/myimage You can also use the <filename> argument to give the retrieved file a new name on GigaVUE-FM. For example, the following command retrieves myimage and names it newconfig: image fetch scp://bbochy:catch1@xxx.xxx.x.x:/myconfig newconfig Note: You cannot retrieve a file with the same name as an existing configuration file.
image list	Provides the list of image file names available in GigaVUE-FM. For example: image list
image install <filename> [next location {1 2}]	Installs the image file. For example, use the following command to install the image file on the next partition: image install gigamon-gigavue-fm-5.8.00-160194-trial.img next Use the following command to install the image file on the specified partition: image install gigamon-gigavue-fm-5.8.00-160194-trial.img location 1 Note: Ensure that your current partition is not the same as the partition you specified for installation. Else, an error is displayed.
image boot [next location {1 2}]	Boots the image file on the specified partition. Ensure that the partition has the installed image file. For example, use the following command to boot the image file on the next partition: image boot next Use the following command to boot the image file on the specified partition: image boot location 1 Note: GigaVUE-FM reboots immediately.
image delete [force] <filename>	Deletes the named image file. For example: image delete myimage
image {move rename} <old filename> <new filename>	Moves or renames the specified image file. For example, the following command renames myimage as newimage: image rename myimage newimage
image show	Displays the last boot partition. For example: image show

Argument	Description
show securebootstatus	Displays whether UEFI secure boot is enabled or not. For example: show securebootstatus
logging [<fqdn>[:<port>]] [facility <facility>] [priority <priority>] [udp tcp tls]	Configures the logging server for sending events and audit logs to the remote server. For Example 1: logging 1.2.3.4:6514 facility auth priority debug tcp Example 2: logging 1.2.3.4:6514 tcp Note: Don't use '*' in the command. It is the default one for facility and priority . Until software version 6.2.00, you can only use the UDP and TCP protocols for logging the audit logs and Syslogs to a remote server. Starting from software version 6.3.00, GigaVUE-FM allows you to configure the logging of audit logs and syslogs using tls . You must perform specific configurations in the remote server to enable logging using TLS. Refer to the Configure rSyslog Server for Receiving TLS/SSL Packets section for more details.
logging <ipaddress> [port <port number>] [facility <facility>] [priority <priority>] [udp tcp tls]	Configure the Syslog server with an IPv4 and IPv6 address. You must use only this command when you configure the IPv6 address. For example: logging <IPv4 or IPv6 address> port 6514 tls Note: If IPv6 syslog server is configured in 6.9 version and then upgraded to 6.11, you must reconfigure the IPv6 syslog server using the new fmctl command.
no logging <ipaddress> [port <port number>]	Removes the logging server configuration when you use IPv4 or IPv6 address. For example: no logging <IPv4 or IPv6 address> port 6514
no logging <fqdn>[:<port>]	Removes the logging server configuration. For example: no logging 1.2.3.4:6514
reset factory halt	Resets the GigaVUE-FM instance to the default configuration and shuts down the system. For example: reset factory halt
set crypto enable	Enables the crypto mode in GigaVUE-FM.

Argument	Description
get crypto	Returns the response for API.
set audit network enable	Enables the network audit logs in GigaVUE-FM.
set audit network disable	Disables the network audit logs in GigaVUE-FM.
get audit network	Returns the response for API.
set srl enable	Enables the CRL validation in GigaVUE-FM.
set srl disable	Disables the CRL validation in GigaVUE-FM.
get srl	Returns the Response for API.
set UI admin password <new password>	Configures a new admin password for the GigaVUE-FM UI only. Use the password within single quotes, double quotes or without quotes. For example: • set UI admin password P@ssword123A! • set UI admin password 'P@ssword123A!' • set UI admin password "P@ssword123A!" For information on setting the GigaVUE-FM password, refer to Setting the GigaVUE-FM Admin Password .
{get show} interface [{mgmt management}]	Displays the management interface configured for the GigaVUE-FM instance. For example: get show interface management
set interface {mgmt management} <interface name>	Configures the management interface for the GigaVUE-FM instance, which has more than one ethernet interface. For example: set interface management eth1 Note: You cannot use the --interface syntax with the set interface management argument.
--interface <interface name>	Allows various configurations that can be set for the management interface. This is an optional argument. For example, use the following command to ensure that eth1 management interface uses DHCP: --interface eth1 set ip dhcp
[options{--help --interface <interface name>}] set mapping <fqdn> <IP address>	Maps the FQDN with the IP address of GigaVUE-FM. For example: --interface eth1 set mapping fm 10.10.10.1 Use the following command to remove the mapping: --interface eth1 set mapping fm
[options{--help --interface <interface name>}] {get show}	Use to either fetch or display the IP address, NTP configurations, host name, domain name, or FQDN . For example:

Argument	Description
{ip ntp hostname domain fqdn}	--interface eth1 get {ip ntp hostname domain fqdn} --help show {ip ntp hostname domain fqdn}
[options{--help --interface <interface name>}] set [ip ip6] dhcp	Configures the management interface to use DHCP. For example: --interface eth1 set ip dhcp
[options{--help --interface <interface name>}] set [ip ip6] [static] <address/cidr> [<gateway> [<dns1> [,<dns2>[,...]]]	Configures the static IP address and gateway on the management interface. You can also choose to configure DNS. For example: --interface eth1 set ip static 10.115.46.72/21 10.115.40.1 10.10.1.20
[options{--help --interface <interface name>}] set {ip ip6} route {add remove} address/cidr gateway	Adds or removes the IP address and gateway for the management interface.
[options{--help --interface <interface name>}] set ntp {disable <server1> [,<server2>[,...]]}	Use to disable NTP for synchronization of the system's clock or delete a NTP server. For example, the following command disables NTP: --interface eth1 set ntp disable For example, the following command deletes NTP server: --interface eth1 set ntp disable 1.2.3.4
[options{--help --interface <interface name>}] set ntp [enable] [version <version_number>] [<server>[:<key_id>:<key_type>:<key_value>[,...]]]	You choose to enable NTP and add NTP servers. For example, the following command enables NTP and adds a NTP server: --interface eth1 set ntp enable 192.168.1.10 For example, the following command enables NTP and adds a NTP server with Authentication: --interface eth1 set ntp enable 192.168.1.10:50:SHA1:HEX:0EAB2E8193262AA0DA64C96A63E9221A20395313
[options{--help --interface <interface name>}] set ntp update [version <version_number>] [<server>[:<key_id>:<key_type>:<key_value>]	Use to update the Auth-details (keys) of the NTP server or to remove the Auth-details. For example, the following command updates the Auth-details (keys) of a NTP server: --interface eth1 set ntp update 1.2.3.4:54:SHA1:HEX:0EAB2E8193262AA0DA64C96A63E9221A20395313 For example, the following command removes the Auth-details (keys) of a NTP server if configured already: --interface eth1 set ntp update 1.2.3.4

Argument	Description
[options{--help --interface <interface name>}] set hostname <hostname>	Configures the hostname. For example: --interface eth1 set hostname myfm Note: Ensure that you log out and re-login to the GigaVUE-FM to view the changes.
[options{--help --interface <interface name>}] set domain <domain>	Configures the domain for GigaVUE-FM. For example: --interface eth1 set domain gigamon.com
[options{--help --interface <interface name>}] set fqdn <hostname> <domain>	Configures the Fully Qualified Domain Name (FQDN) for the current GigaVUE-FM. --interface eth1 set fqdn myfm gigamon.com
[options{--help --interface <interface name>}] set/get/show searchdomains [<domain1> [,<domain2>[,...]]]	Displays a list of domains for the current GigaVUE-FM For example: --interface eth1 set searchdomains --help get show searchdomains
[options{--help --interface <interface name>}] set/get/show nameservers [<dns1> [,<dns2>[,...]]]	Displays a list of name servers for the current GigaVUE-FM For example: --interface eth1 set nameservers --help get show nameservers
[options{--help --interface <interface name>}] show backup	Displays the configurations that were backed up. For example: --help show backup <absolute path name of backup file>
unlock UI <username>	Unlocks the admin user whose account is locked after the maximum attempt to login is reached. --unlock UI <username>
shell	Navigates from fmctl shell to linux shell for advanced troubleshooting.
help	Displays the list of fmctl commands
exit	Exit the GigaVUE-FM CLI session.

NOTE: The command **fmctl jump-start** is deprecated.

Backing Up Configurations

Configurations that can be backed up using **fmctl** commands are as follows:

BackupVersion
fmMgmtPort
fmHostname

fmDomain
fmNtpEnabled
fmNtpServers
fmDevice
fmlp4Connection
fmDhcpEnabled
fmlp4Address
fmlp4Gateway
fmlp4DNS
fmlp4Routes
fmlp6Connection
fmDhcp6Enabled
fmlp6Address
fmlp6Gateway
fmlp6DNS
fmlp6Routes
fmNameServers
fmSearchDomains
fmExtraPortCount

NOTE: When there are multiple interfaces in GigaVUE-FM, back up files provide the configurations of all the interfaces.

Rules, Notes and Limitations

Refer to the following rules and notes:

- To include special characters in the **fmctl** command line, enclose the string containing the special characters within single quotes. For example, to include the bang (!) special character in a password string, you must enclose the password string within single quotes, as shown in the following example:
fmctl set UI admin password 'admin!!'
- When you manually restart the rsyslog service or change any fmctl logging configuration parameters, a few GigaVUE-FM audit log messages will not be captured in the syslog. This occurs as a result of limitations of the library used for pushing GigaVUE-FM's audit logs to syslog.

Mapping of SNMP Traps with GigaVUE-FM Events and Alarms

When a GigaVUE node that is managed by GigaVUE-FM generates an SNMP Trap, a corresponding Event, and sometimes, a corresponding Alarm are generated by GigaVUE-FM. The following table provides the complete list of SNMP Traps along with the corresponding Events and Alarms.

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
coldStart	.1.3.6.1.6.3.1.1.5.1	TrapMib2ColdStart	N/A	N/A
warmStart	.1.3.6.1.6.3.1.1.5.2	TrapMib2WarmStart	N/A	N/A
linkDown	.1.3.6.1.6.3.1.1.5.3	TrapMib2LinkDown	Device Port Unhealthy	Port Unhealthy
linkUp	.1.3.6.1.6.3.1.1.5.4	TrapMib2LinkUp	Device Port Unhealthy	Port Unhealthy
authenticationFailure	.1.3.6.1.6.3.1.1.5.5	TrapMib2AuthFailure	FM Alarm support currently not available	N/A
gigamonSnmpResetSystemNotification	.1.3.6.1.4.1.26866.1.1.1	TrapSysReset	N/A	N/A
gigamonSnmpAcmeReqStatusNotification	.1.3.6.1.4.1.26866.1.1.81	TrapAcmeReqStatusNotification	N/A	N/A
gigamonSnmpUserAuthFailNotification	.1.3.6.1.4.1.26866.1.1.2	TrapUserAuthFailed	N/A	N/A
gigamonSnmpFirmwareChangeNotification	.1.3.6.1.4.1.26866.1.1.3	TrapFirmwareChanged	N/A	N/A
gigamonSnmpConfigSaveNotification	.1.3.6.1.4.1.26866.1.1.4	TrapConfigSave	N/A	N/A
gigamonSnmpModuleChangeNotification	.1.3.6.1.4.1.26866.1.1.5	TrapModuleChange	N/A	N/A
gigamonSnmpPacketDropNotification	.1.3.6.1.4.1.26866.1.1.6	TrapPacketDrop	Device Port Unhealthy	Port Unhealthy
gigamonSnmpTapRelayChangeNotification	.1.3.6.1.4.1.26866.1.1.7	TrapTapRelayChange	N/A	N/A

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
gigamonSnmpPortLinkChangeNotification	.1.3.6.1.4.1.26866.1.1.8	TrapPortLinkChange	Device Port Unhealthy	Port Unhealthy
gigamonSnmpRXTxErrorNotification	.1.3.6.1.4.1.26866.1.1.9	TrapRXTxError	Device Port Unhealthy	Port Unhealthy
gigamonPowerChangeNotification	.1.3.6.1.4.1.26866.1.1.10	TrapPowerChange	Device Power Module Faulty	Faulty Power Module
gigamonFanChangeNotification	.1.3.6.1.4.1.26866.1.1.11	TrapFanChange	Device Fan Trays Operation Abnormal	Abnormal Fan Operation
gigamonSnmpProxyServerConnectionStatusChangeNotification	.1.3.6.1.4.1.26866.1.1.91	TrapGSPProxyServerConnectionStatusChange	GigaSMART Engine is Unhealthy or the event is due to Proxy Server connection status	N/A
gigamonSnmpOverThresholdChangeNotification	.1.3.6.1.4.1.26866.1.1.12	TrapOverThreshold	N/A	N/A
gigamonSnmpBatteryLevelChangeNotification	.1.3.6.1.4.1.26866.1.1.13	TrapBatteryLevelChange	FM Alarm support currently	N/A

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
			y not available	
gigamonLinkSpeedStatusChangeNotification	.1.3.6.1.4.1.26866.1.1.14	TrapLinkStateChange	N/A	N/A
gigamonSnmpUnexpectedShutdownNotification	.1.3.6.1.4.1.26866.1.1.17	TrapUnexpectedShutdown	N/A	N/A
gigamonSnmpWatchdogResetNotification	.1.3.6.1.4.1.26866.1.1.19	TrapWatchdogReset	N/A	N/A
gigamonSnmpBufferOverThresholdNotification	.1.3.6.1.4.1.26866.1.1.21	TrapBufferUsage	N/A	N/A
gigamonSnmpInlineBypassStateChangeNotification	.1.3.6.1.4.1.26866.1.1.22	TrapInlineBypassStateChange	N/A	N/A
gigamonSnmpEvalLicenseExpireNotification	.1.3.6.1.4.1.26866.1.1.23	TrapEvalLicenseExpire	N/A	N/A
gigamonSnmpGsCpuUtilizationNotification	.1.3.6.1.4.1.26866.1.1.24	TrapGsCpuUtilization	FM Alarm support currently not available	N/A
gigamonSnmpBelowThresholdChangeNotification	.1.3.6.1.4.1.26866.1.1.25	TrapPortUtilBelowThreshold	Device Port Unhealthy	Port Unhealthy
gigamonSnmpInlineToolRecoveryNotification	.1.3.6.1.4.1.26866.1.1.26	TrapInlineToolRecovery	FM Alarm support currently not available	N/A
gigamonSnmpOpticsTemperatureNotification	.1.3.6.1.4.1.26866.1.1.27	TrapOpticsTemperature	N/A	N/A
gigamonSnmpExhaustTemperatureNotification	.1.3.6.1.4.1.26866.1.1.28	TrapExhaustTemperature	N/A	N/A
gigamonSnmpSwitchCPUTemperatureNotification	.1.3.6.1.4.1.26866.1.1.29	TrapSwitchCpuTemperature	N/A	N/A

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
gigamonSnmpCPUTemperatureNotification	.1.3.6.1.4.1.26866.1.1.30	TrapCpuTemperature	DeviceCpuTemperatureUnhealthy	Device CPU Temperature Unhealthy
gigamonSnmpSecondaryFlashBootNotification	.1.3.6.1.4.1.26866.1.1.31	TrapSecondaryFlashBoot	N/A	N/A
gigamonSnmpOperationalModeNotification	.1.3.6.1.4.1.26866.1.1.32	TrapOperationalModeChangeTrapOperationalModeChanged	N/A	N/A
gigamonSnmpCaviumCPUTemperatureNotification	.1.3.6.1.4.1.26866.1.1.33	TrapGigaSMARTCpuTemperature	N/A	N/A
gigamonSnmpEPortTemperatureNotification	.1.3.6.1.4.1.26866.1.1.34		N/A	N/A
gigamonSnmpSubLicenseExpireNotification	.1.3.6.1.4.1.26866.1.1.35	TrapSubscriptionLicenseReminder	N/A	N/A
gigamonSnmpCcProcessCpuUtilizationNotification	.1.3.6.1.4.1.26866.1.1.36	TrapProcessCpuUtilHigh	N/A	N/A
gigamonSnmpCcProcessMemoryUtilizationNotification	.1.3.6.1.4.1.26866.1.1.37	TrapProcessMemoryUtilHigh	N/A	N/A
gigamonSnmpPolicyTriggerNotification	.1.3.6.1.4.1.26866.1.1.38	TrapPolicyTrigger	N/A	N/A
gigamonSnmpCcSystemCpuUtilizationNotification	.1.3.6.1.4.1.26866.1.1.39	TrapSystemCpuUtilHigh	FM Alarm support currently not available	N/A
gigamonSnmpCcSystemMemoryUtilizationNotification	.1.3.6.1.4.1.26866.1.1.40	TrapSystemMemoryUtilHigh	FM Alarm support currently not available	N/A
gigamonSnmpGdpUpdateNotification	.1.3.6.1.4.1.26866.1.1.41	TrapGigamonDiscovery	N/A	N/A
gigaSmartTunnelStatus	.1.3.6.1.4.1.268	TrapTunnelGwStatus	Tunnel	Tunnel

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
	66.1.1.42		Port Unhealthy	Port Unhealthy
gigaSmartTunnelDestStatus	.1.3.6.1.4.1.268 66.1.1.43	TrapTunnelDestIpStatus	Tunnel Port Unhealthy	Tunnel Port Unhealthy
gigamonSnmplpGwStatusNotification	.1.3.6.1.4.1.268 66.1.1.44	TrapIpGwStatusUpdate	IP Interface Unhealthy	IP Interface Unhealthy
gigamonSnmpTrapThrottleReport	.1.3.6.1.4.1.268 66.1.1.45	TrapThrottleReport	N/A	N/A
gigamonSnmpClusterRoleChange Notification	.1.3.6.1.4.1.268 66.1.1.46	TrapClusterRoleChange	N/A	N/A
gigamonSnmpClusterNodeJoinNotification	.1.3.6.1.4.1.268 66.1.1.47	TrapClusterNodeJoin	N/A	N/A
gigamonSnmpClusterNodeLeaveNotification	.1.3.6.1.4.1.268 66.1.1.48	TrapClusterNodeLeave	N/A	N/A
gigamonSnmpClusterNodeJoinFail Notification	.1.3.6.1.4.1.268 66.1.1.49	TrapClusterNodeJoinFail	N/A	N/A
gigamonSnmpVportStateChange Notification	.1.3.6.1.4.1.268 66.1.1.50	TrapVportStatusChange	Virtual Port Unhealthy	Virtual Port Unhealthy
gigamonSnmpTrapIsslResource	.1.3.6.1.4.1.268 66.1.1.51	TrapGSIsslResourceUtilization	N/A	N/A
gigamonSnmpGigaSMARTCPUTemperatureNotification	.1.3.6.1.4.1.268 66.1.1.52	TrapGigaSMARTCpuTemperature	N/A	N/A
gigamonSnmpLicenseExpireNotification	.1.3.6.1.4.1.268 66.1.1.53	TrapLicenseExpirationReminder	N/A	N/A
gigamonSnmpBatteryPresenceNotification	.1.3.6.1.4.1.268 66.1.1.54	TrapBatteryPresence	N/A	N/A
gigamonSnmpBatteryTestNotification	.1.3.6.1.4.1.268 66.1.1.55	BatteryTestStatusNotifWrapper	N/A	N/A

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
gigamonSnmpBatteryTemperatureNotification	.1.3.6.1.4.1.26866.1.1.56		FM Alarm support currently not available	N/A
gigamonSnmpFipsTestNotification	.1.3.6.1.4.1.26866.1.1.57	TrapsFipsTestNotification	N/A	N/A
gigamonSnmpGsOverThresholdChangeNotification	.1.3.6.1.4.1.26866.1.1.58	TrapGsOverThreshold	N/A	N/A
gigamonSnmpGsBelowThresholdChangeNotification	.1.3.6.1.4.1.26866.1.1.59	TrapGsBelowThreshold	FM Alarm support currently not available	N/A
gigamonSnmpSfpIncompatibleNotification	.1.3.6.1.4.1.26866.1.1.60	TrapSFPCompatibility	N/A	N/A
gigamonSnmpPowerSourceChangeNotification	.1.3.6.1.4.1.26866.1.1.61	TrapPowerSourceChangeGTAP	FM Alarm support currently not available	N/A
gigamonSnmpSfpPortPowerChangeNotification	.1.3.6.1.4.1.26866.1.1.62	TrapSFPPowerSourceChange	N/A	N/A
gigamonSnmpTopSwitchTemperatureNotification	.1.3.6.1.4.1.26866.1.1.63	TrapTopSwitchTemp	N/A	N/A
gigamonSnmpBottomSwitchTemperatureNotification	.1.3.6.1.4.1.26866.1.1.64	TrapBottomSwitchTemp	N/A	N/A
gigamonSnmpRearPanelTemperatureNotification	.1.3.6.1.4.1.26866.1.1.65	TrapRearPanelTemp	N/A	N/A
gigamonSnmpQsfpCageTemperatureNotification	.1.3.6.1.4.1.26866.1.1.66	TrapQsfpCageTemp	N/A	N/A
gigamonSnmpSfpCageTemperatureNotification	.1.3.6.1.4.1.26866.1.1.67	TrapSfpCageTemp	N/A	N/A
gigamonSnmpNearCpuTemperature	.1.3.6.1.4.1.268	TrapNearCpuTemp	N/A	N/A

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
ureNotification	66.1.1.68			
gigamonSnmpBcmSocTemperatureNotification	.1.3.6.1.4.1.26866.1.1.69	TrapBcmSocTemp	N/A	N/A
gigamonSnmpCpuSocTemperatureNotification	.1.3.6.1.4.1.26866.1.1.70	TrapCpuSocTemp	N/A	N/A
gigamonSnmpCpuHibernationStatusNotification	.1.3.6.1.4.1.26866.1.1.71	TrapCPUHibernation	N/A	N/A
gigaSmartNetFlowResourceAllocationFailed	.1.3.6.1.4.1.26866.1.1.72	TrapNetflowResourceAllocationFailed	N/A	N/A
gigamonSnmpSysdumpStatusNotification	.1.3.6.1.4.1.26866.1.1.73	TrapSysdumpGeneration	N/A	N/A
gigamonSnmpInlineToolHbStatusChangeNotification	.1.3.6.1.4.1.26866.1.1.74	TrapInlineToolHbChange	Inline Tool Unhealthy	N/A
gigamonSnmpMobTunnelExhaustionTrap	1.3.6.1.4.1.26866.1.1.92	TrapGSMobRTunnelUtilization	GigaSMART Engine Tunnel Utilization Exceeded	N/A
gigamonSnmpMobSessionExhaustionTrap	1.3.6.1.4.1.26866.1.1.93	TrapGSMobSessionUtilization	GigaSMART Engine Session Utilization Exceeded	N/A
gigamonSnmpMobPersistRestoreFailTrap	1.3.6.1.4.1.26866.1.1.94	TrapGSMobPersistenceFailure	N/A	N/A
gigamonSnmpMobPacketBufferUtilizationTrap	1.3.6.1.4.1.26866.1.1.95	TrapGSMobPacketBufferUtilization	GigaSMART	N/A

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
			Engine Packet Buffer Utilization Exceeded	
gigamonSnmpMobCpuUtilizationTrap	1.3.6.1.4.1.26866.1.1.96	TrapGSMobCpuUtilization	GigaSMART Engine CPU Utilization Exceeded	N/A
gigamonSnmpGigastreamImbalanceNotification	.1.3.6.1.4.1.26866.1.1.82	TrapGigaStreamImbalance	GigaStream Unhealthy	Corrective Actions for GigaVUE-FM Alarms
gigamonSnmpGigastreamRecoveryNotification	.1.3.6.1.4.1.26866.1.1.83	TrapGigaStreamBalanced	GigaStream Unhealthy	Corrective Actions for GigaVUE-FM Alarms

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
gigamonSnmpSwitchBoard2TemperatureNotification	.1.3.6.1.4.1.26866.1.1.84	TrapSwitchBoard2Temperature	Switch Board 2 Temperature Unhealthy	N/A
gigamonSnmpSwitchBoard3TemperatureNotification	.1.3.6.1.4.1.26866.1.1.85	TrapSwitchBoard3Temperature	Switch Board 3 Temperature Unhealthy	N/A
gigamonSnmpSwitchBoard1TemperatureNotification	.1.3.6.1.4.1.26866.1.1.86	TrapSwitchBoard1Temperature	Switch Board 1 Temperature Unhealthy	N/A

GigaVUE® Fabric Management Events

This section provides the consolidated list of Events along with their descriptions.

Alarms

The following table lists all the events related to Alarms.

GigaVUE-FM Event	Description
AlarmCreateEvent	Alarm Created Event
AlarmUpdateEvent	Alarm Updated Event
AlarmDeleteEvent	Alarm Deleted Event

GigaVUE Cloud Suite

The following table provides the list of all the events that are generated for the various GigaVUE Cloud Suite platforms.

GigaVUE-FM Event	Description
AnyCloudInventoryUpdateCompleted	AnyCloud Inventory Update Completed
AnyCloudInventoryUpdateStarted	AnyCloud Inventory Update started
AwsConnectionStateChanged	AWS Connection Status Changed
AwsConnectionTriggeredInventoryUpdateCompleted	Aws Connection Triggered Inventory Update Completed
AwsConnectionTriggeredInventoryUpdateFailed	Aws Connection Triggered Inventory Update Failed
AwsConnectionTriggeredInventoryUpdateStarted	Aws Connection Triggered Inventory Update Started
AwsFabricDeploymentInventoryUpdateFailed	AWS Fabric Deployment Inventory Update Failed
AwsInstanceInventoryUpdateFailed	AWS Instance Inventory Update Failed
AwsInventoryUpdateCompleted	AWS Inventory Update Completed
AwsInventoryUpdateStarted	AWS Inventory Update Started

GigaVUE-FM Event	Description
AwsLicenseExpire	AWS License Has Expired
AzureConnectionStateChanged	Azure Connection Status Changed
AzureConnectionTriggeredInventoryUpdateCompleted	Azure Connection Triggered Inventory Update Completed
AzureConnectionTriggeredInventoryUpdateFailed	Azure Connection Triggered Inventory Update Failed
AzureConnectionTriggeredInventoryUpdateStarted	Azure Connection Triggered Inventory Update Started
AzureConnResGrpLimitExceeded	Azure Connection Resource Group Limit Exceeded
AzureFabricDeploymentInventoryUpdateFailed	Azure Fabric Deployment Inventory Update Failed
AzureInventoryUpdateCompleted	Azure Inventory Update Completed
AzureInventoryUpdateStarted	Azure Inventory Update Started
AzureLicenseExpire	Azure License Has Expired
AzureVMInventoryUpdateFailed	Azure VM Inventory Update Failed
deviceHealthChanged	OpenStack Fabric Deployment Inventory Update Failed
FabricNodeRegistered	GigaVUE V Series Node deployed using Third party orchestration registered
FabricNodeUnRegistered	GigaVUE V Series Node deployed using Third

GigaVUE-FM Event	Description
	party orchestration unregistered
FabricNodeHeartBeat	Fabric Node Heart Beat
FabricNodeRegistered	Fabric Node Registered
FabricNodeUnRegistered	Fabric Node UnRegistered
FmIntermediateCaChangeEvent	GigaVUE-FM Intermediate CA change Event
FmIntermediateCaCsrCreateEvent	GigaVUE-FM Intermediate CA CSR Generate Event
FabricNodeCertificateEvent	Cloud Fabric Node Certificate Generate Event
FmIntermediateCaExpiryEvent -	GigaVUE-FM Intermediate CA Expiry Event
NodeAdded	GigaVUE V Series Node Added
NodeDown	GigaVUE V Series Node Down
NodeRebootFailed	GigaVUE V Series Node Reboot Failed
NodeRemoved	GigaVUE V Series Node Removed
NodeReplacementLaunched	GigaVUE V Series Node Replacement Launched
NodeRestarted	GigaVUE V Series Node Restarted
NodeUp	GigaVUE V Series Node Up

GigaVUE-FM Event	Description
VmmVSeriesNodeInstallEvent	GigaVUE V Series Node Install Event
VmmVSeriesNodeUpdateFailed	GigaVUE V Series Node Update Failed
VSeriesNodeUpdateComplete	GigaVUE V Series Node Update Completed
GcbDeregistered	GCB Deregistered
GcbRegistered	GCB Registered
InstanceRunning	VM Instance Running
InstanceStopped	VM Instance Stopped
InstanceTerminated	VM Instance Terminated
KubernetesConnectionStateChanged	Kubernetes Connection Status Changed
KubernetesConnTriggeredInvUpdateCompleted	Kubernetes Connection Triggered Inventory Update Completed
KubernetesConnTriggeredInvUpdateFailed	Kubernetes Connection Triggered Inventory Update Failed
KubernetesConnTriggeredInvUpdateStarted	Kubernetes Connection Triggered Inventory Update Started
NoCompatibleUctVController	No compatible UCT-V Controller exists for UCT-V version
NodeDeleted	GigaVUE V Series Node Deleted
NodeRebooted	GigaVUE V Series Node Rebooted
NodeReplacementLaunchFailed	GigaVUE V Series Node

GigaVUE-FM Event	Description
	Replacement Launch Failed
NodeRestartFailed	GigaVUE V Series Node Restart Failed
NodeUnreachable	GigaVUE V Series Node Unreachable
NodeUnrecoverable	GigaVUE V Series Node Unrecoverable
NsxtLicenseExpire	VMware NSX-T License Has Expired
NutanixConnectionStateChanged	Nutanix Connection Status Changed
NutanixConnTriggeredInvUpdateCompleted	Nutanix Connection Triggered Inventory Update Completed
NutanixConnTriggeredInvUpdateFailed	Nutanix Connection Triggered Inventory Update Failed
NutanixConnTriggeredInvUpdateStarted	Nutanix Connection Triggered Inventory Update Started
NutanixInventoryUpdateCompleted	Nutanix Inventory Update Completed
NutanixInventoryUpdateStarted	Nutanix Inventory Update started
OpenStackConnectionStateChanged	Openstack Connection State Changed
OpenStackConnectionTriggeredInventoryUpdateCompleted	OpenStack Connection Triggered Inventory Update Completed
OpenStackConnectionTriggeredInventoryUpdateFailed	OpenStack Connection Triggered Inventory Update Failed
OpenStackConnectionTriggeredInventoryUpdateStarted	OpenStack Connection Triggered Inventory Update Started

GigaVUE-FM Event	Description
OpenStackInstanceInventoryUpdateFailed	OpenStack Instance Inventory Update Failed
OpenStackInventoryUpdateCompleted	OpenStack Inventory Update Completed
OpenStackInventoryUpdateStarted	OpenStack Inventory Update Started
OpenStackProjectLimitExceeded	OpenStack Project Limit Exceeded
UctVInventoryUpdateCompleted	UCT-V Inventory Update Completed
VcenterConnectionStateChanged	vCenter Connection Status Changed
VmmDvsPortLinkDown	DVS Port Link Down
VmmDvsPortLinkUp	DVS Port Link Up
VmmError	Vmm error
VmmGvmNoIp	GigaVUE-VM does not have an IP
VmmGvmPinToHost	GigaVUE-VM pinned to host
VmmGvmUnPinFromHost	GigaVUE-VM unpinned from host
VmmHostAdded	Host added
VMMHostMoveInCluster	Host Moved In Cluster
VmmHostMultiGvm	Host has Multiple Gvms
VmmHostNetworkConfiged	Host Network reconfiged
VmmHostPoweredOff	Host powered off
VmmHostPoweredOn	Host powered on
VmmHostRemoved	Host removed
VmmNsxvAgentDeleted	NSX-V Agent Deleted
VmmNsxvAgentUpdated	NSX-V Agent Created/Updated

GigaVUE-FM Event	Description
VmmNsxvProfileDeleted	NSX-V Profile Deleted
VmmNsxvProfileUpdated	NSX-V Profile Created/Updated
VmmNsxvServiceInstanceCreated	NSX-V Service Instance Created
VmmNsxvServiceInstanceDeleted	NSX-V Service Instance Deleted
VmmPortAdded	vNIC added
VmmPortEdited	vNIC configuration changed
VmmPortRemoved	vNIC removed
VmmUctVControllerCameOnline	UCT-V Controller VM came online
VmmUctVControllerInstallComplete	UCT-V Controller VM install completed
VmmUctVControllerInstallStarted	UCT-V Controller VM install started
VmmUctVControllerInstallFailed	UCT-V Controller VM Install Failed
VmmUctVControllerUpgradeComplete	UCT-V Controller upgrade completed
VmmUctVControllerUpgradeFailed	UCT-V Controller upgrade failed
VmmUctVControllerUpgradeStarted	UCT-V Controller upgrade started
VmmVcenterAdded	vCenter Added
VmmVcenterConnected	vCenter Connected
VmmVcenterConnectionStateChanged	vCenter Connection State Changed
VmmVcenterDeleted	vCenter Deleted
VmmVcenterDisconnected	vCenter Disconnected
VmmVcenterInventoryCompleted	vCenter Inventory Completed

GigaVUE-FM Event	Description
VmmVmConnected	VM connected
VmmVmCreated	VM created
VmmVmDisconnected	VM disconnected
VmmVmGuestReboot	VM Guest rebooted
VmmVmGuestShutdown	VM Guest shutdown
VmmVmMigrated	vMotion completed
VmmVmPoweredOff	VM powered off
VmmVmPoweredOn	VM powered on
VmmVmRemoved	VM removed
VmmVmRenamed	VM renamed
VmmVmResetting	VM resetting
VmmVmStartMigrating	vMotion started
VmmVmSuspended	VM suspended
VmmVSeriesControllerInstallComplete	V Series Controller VM install completed
VmmVSeriesControllerInstallFailed	V Series Controller VM install failed
VmmVSeriesControllerInstallStarted	V Series Controller VM install started
VmmVSeriesControllerUpgradeComplete	V Series Controller upgrade completed
VmmVSeriesControllerUpgradeFailed	V Series Controller upgrade failed
VmmVSeriesControllerUpgradeStarted	V Series Controller upgrade started
VmmVSeriesNodeInstallComplete	V Series Node VM install completed
VmmVSeriesNodeInstallFailed	V Series Node VM install failed
VmmVSeriesNodeInstallStarted	V Series Node VM install started
VmmVSeriesNodeUpgradeComplete	V Series Node upgrade completed

GigaVUE-FM Event	Description
VmmVSeriesNodeUpgradeFailed	V Series Node upgrade failed
VmmVSeriesNodeUpgradeStarted	V Series Node upgrade started
VmwareConnectionTriggeredInventoryUpdateCompleted	VMware Connection Triggered Inventory Update Completed
VmwareConnectionTriggeredInventoryUpdateFailed	VMware Connection Triggered Inventory Update Failed
VmwareFabricDeploymentInventoryUpdateFailed	VMware Fabric Deployment Inventory Update Failed
VmwareInventoryUpdateCompleted	VMware Inventory Update Completed
VmwareNsxtNodeDeploymentCompleted	VMware NSX-T Node Deployment completed
VmwareNsxtNodeDeploymentFailed	VMware NSX-T Node Deployment failed
VmwareNsxtNodeDeploymentStarted	VMware NSX-T Node Deployment started
VmwareNsxtNodeDeploymentSuccess	VMware NSX-T Node Deployment successful
VmwareNsxtNodeUndeploymentCompleted	VMware NSX-T Node Undeployment completed
VmwareNsxtNodeUndeploymentFailed	VMware NSX-T Node Undeployment failed
VmwareNsxtNodeUndeploymentStarted	VMware NSX-T Node Undeployment started
VmwareNsxtNodeUndeploymentSuccess	VMware NSX-T Node Undeployment successful
VmwareVmInventoryUpdateFailed	VMware VM Inventory Update Failed

GigaVUE-FM Event	Description
VmwareVmPinToHost	GigaVUE-VM pinned to host
VmwareVmUnPinFromHost	GigaVUE-VM unpinned from host
VmwareVseriesNodeRediscoveryEvent	GigaVUE V Series Node Rediscovery for VMware
VmwareVseriesNodeRediscoverySummaryEvent	GigaVUE V Series Node Rediscovery Summary for VMware

Cluster

The following table provides the list of all the cluster-related events.

GigaVUE-FM Event	Description
ClusterCreationStarted	Cluster creation started
ClusterCreationCompleted	Cluster creation completed
AddClusterMembersCompleted	Add members completed
AddClusterMembersFailed	Add members failed
ClusterCreationFailed	Cluster creation failed
NodeJoinedToCluster	Node joined to cluster
NodeFailedToJoinCluster	Node failed to join cluster
NodeRemovedFromCluster	Node removed from cluster
ClusterNodeUpdated	Cluster node updated
NodeFailedToRemoveFromCluster	Node failed to remove from cluster

Device

The following table provides the list of events related to device upgrade, device discovery, and device configuration.

GigaVUE-FM Event	Description
DiscoveryStarted	Device discovery started
DiscoveryFinished	Device discovery finished
DiscoveryFailed	Device discovery failed
DeviceImageDownloadStarted	Device image download started
DeviceImageDownloadFinished	Device image download finished
DeviceImageDownloadFailed	Device image download failed
DeviceImageInstallStarted	Device image install started
DeviceImageInstallFinished	Device image install finished
DeviceImageInstallFailed	Device image install failed
DeviceConfigSaveStarted	Device configuration save started
ClusterImageInstallStarted	Cluster image install started
PostDeviceUpgradeVerificationStarted	Post Device Upgrade Verification Started
PostDeviceUpgradeVerificationFinished	Post Device Upgrade Verification Finished
PostDeviceUpgradeVerificationFailed	Post Device Upgrade Verification Failed
DeviceRebootStarted	Device reboot started
DeviceRebootFinished	Device reboot finished
DeviceRebootFailed	Device reboot failed
DeviceBuildVerificationStarted	Device build verification started
DeviceBuildVerificationFinished	Device build verification finished
DeviceBuildVerificationFailed	Device build verification failed
DeviceFirmwareUpgradeStarted	Device firmware upgrade started
DeviceFirmwareUpgradeFinished	Device firmware upgrade finished
DeviceFirmwareUpgradeFailed	Device firmware upgrade failed
DeviceConfigBackedUp	Device configuration backed up
DeviceConfigDeleted	Device configuration deleted
DeviceConfigRestored	Device configuration restored
ApplyDeviceConfig	Apply device configuration

GigaVUE-FM Event	Description
ClusterRebootStarted	Cluster reboot started
ClusterRebootFinished	Cluster reboot finished
FMMetadataTemplateConfigTypeCompleted	GigaVUE-FM Metadata Template Configuration Type Completed

Fabric Maps

The following table provides the list of Fabric Maps-related events.

GigaVUE-FM Event	Description
FabricPathUnusedSrcPorts	Un-utilized source ports in fabric path
FabricPathMultipleClusterTermination	Fabric path has multiple source or destination cluster termination
FabricMapFailover	Fabric Map tunnel end-point change as response to path status

GigaVUE-FM Events

The following table lists the events related to GigaVUE-FM backup and restore, image upgrade, health, topology, and High Availability.

GigaVUE-FM Event	Description
FMServerConfigBackup	FM Server config backup
FMServerConfigRestore	FM Server config restore
FMImageUpgradeStarted	FM Image Upgrade Started
FMImageUpgradeCompleted	FM Image Upgrade Completed
FMImageUpgradeFailed	FM Image Upgrade Failed
FMImageInstallFinished	FM image install Finished
FMImageRollback	FM Image Rollback Status
FMRebootStarted	FM reboot started

GigaVUE-FM Event	Description
FMRebootFinished	FM reboot finished
FMConfigSaveStarted	FM config save started
DeviceAdded	Node added
DeviceDeleted	Node removed
DeviceStateChanged	Node state changed
ManualNodeAdded	Manual node added
ManualNodeDeleted	Manual node removed
ManualNodeUpdated	Manual node updated
ManualLinkAdded	Manual link added
ManualLinkDeleted	Manual link removed
StatsCollectionFailed	Stats Collection Failed
LinkUp	Link Up
LinkDown	Link Down
FlowHealthStateChanged	Flow health state changed
FlowComputationErrorEvent	Error while computing flow
FMHaEvent	GigaVUE-FM High Availability configured
FMHealthQueueInfo	FM Health Queue Information
FMDeviceHealthComputationLimitExceededEvent	When GigaVUE-FM processes too many traps from managed devices, it affects health calculations. If the health computation queue gets too full, the system will skip health calculations until there is space available in the queue. In such cases, GigaVUE-FM generates an event to notify the number of devices for which the

GigaVUE-FM Event	Description
	health computation task is skipped.
FMDeviceHealthComputationLimitExceededThrottleEvent	When the health computation limit exceeding event is occurring continuously, instead of having an individual event for each, GigaVUE-FM will throttle them and send them as a single event.
FMAPIRateLimitExceededEvent	When the API rate limits configured in GigaVUE-FM are exceeded, an event is triggered.
FMAPIRateLimitExceededThrottleEvent	When the API rate limits breaches persist, the events are throttled and events are raised. The throttled events have a default absorption window of 30 minutes during which further events are suppressed.
FMBasicAuthDeniedEvent	When basic authentication is denied GigaVUE-FM raises an event.
FMBasicAuthDeniedThrottledEvent	When the basic authentication denial persist, the throttled and events are raised. The throttled events have a default absorption window of 30 minutes during which further events are suppressed.

G-TAP A Series 2

The following table lists the events related to G-TAP A Series 2.

GigaVUE-FM Event	Description
BatteryTestStartFailedEvent	Battery Test Failed to Start
BatteryTestStartedEvent	Battery Test Started
BatteryTestInProgressEvent	Battery Test is In-Progress
BatteryTestCompletedEvent	Battery Test Completed
BatteryTestNotExecutedEvent	Battery Test not executed
BatteryTestAbortedEvent	Battery Test Aborted
BatteryTestAbortedFailedEvent	Battery Test Aborted Failed

GigaSMART Events

The following table lists the events related to GigaSMART.

GigaVUE-FM Event	Description
TrapGSMobRTunnelUtilization	Mobility Tunnel Utilization
TrapGSMobSessionUtilization	Mobility Session Utilization

GigaVUE-FM Event	Description
TrapGSMobPersistenceFailure	Mobility Persistence Failure
TrapGSMobPacketBufferUtilization	Mobility Packet Buffer Utilization
TrapGSMobCpuUtilization	Mobility CPU Utilization

Software Licensing

The following table lists the events related to GigaVUE-FM Licensing.

GigaVUE-FM Event	Description
FloatingLicenseAssignFailed	Floating license assign failed when start time reached
FloatingLicenseUnassignFailed	Floating license un-assign failed when renewal succeeded
VolumeUsageAlertThresholdExceeded	Volume Usage alert threshold exceeded
VolumeUsageReportEmailSendFailed	Volume Usage report email send failed
LicensesRecentlyExpired	Licenses in the 45-day window (licenses for which the 45-day window is applicable)
LicensesExpired (applicable for floating and node-locked licenses)	Licenses expired

SNMP

The following table lists all the events related to SNMP throttle.

GigaVUE-FM Event	Description
SnmpThrottleConfigSaveFailed	SnmpThrottleConfigSaveFailed
SnmpVersionNotSupported	Snmp version is not supported
SnmpThrottleUpdated	Snmp Throttle updated

GigaVUE-FM Event	Description
FMTemplatesSnmpTrapEnforced	FM Templates SNMP TRAP Enforced
FMTemplatesSnmpTrapConfigTypeCompleted	FM Templates SNMP TRAP Config Type Completed
SnmpV3MigrationActionRequired	Snmpv3 migration action required

ACME

The following table lists all the events related to ACME.

GigaVUE-FM Event	Description
FMAcmeCertificateIssueSuccess	ACME certificate issue succeeded
FMAcmeCertificateRenewSuccess	ACME certificate renewal succeeded
FMAcmeCertificateRevokeSuccess	ACME certificate revoke succeeded
FMTemplateAcmeGlobalCompleted	ACME global configuration of devices completed
FMAcmeCertificateClearFailed	ACME certificate clear failed
FMAcmeCertificateIssueFailed	ACME certificate issue failed
FMAcmeCertificateRenewFailed	ACME certificate renewal failed
FMAcmeCertificateRevokeFailed	ACME certificate revoke failed
FMAcmeCertificateClearStarted	ACME certificate clear started
FMAcmeCertificateRenewStarted	ACME certificate renew started
FMAcmeCertificateRevokeStarted	ACME certificate revoke started
TrapAcmeReqStatusNotification	ACME Trap request status notification
FMAcmeCertificateClearSuccess	ACME Certificate Clear Success

Traffic Drop Identification

The following table lists the events related to Traffic Drop Identification.

GigaVUE-FM Event	Description
TrafficDropThresholdExceeded	This event is triggered when traffic drop is detected and the computed traffic drop value exceeds the configured threshold for a given entity.
TrafficDropAlertPolicyDeleted	This event is triggered when traffic drop

GigaVUE-FM Event	Description
	identification alert policy is deleted for a given entity.
TrafficDropAlertPolicyUpdated	This event is triggered when traffic drop identification alert policy is updated for a given entity

Cluster with Not Reachable Nodes

The following table lists the events related to Traffic Drop Identification.

GigaVUE-FM Event	Description
ClusterMemberOnline	This event is triggered when GigaVUE-FM sends a notification to the external servers when a not-reachable member in a device cluster becomes online.
ClusterMemberNotReachable	This event is triggered when GigaVUE-FM sends a notification to the external servers when one of the members in a device cluster goes not-reachable from the cluster.

GigaVUE-FM SNMP Traps

GigaVUE-FM generates and sends a list of SNMP traps and GigaVUE-FM events to the external servers. The following table list the SNMP traps and GigaVUE-FM with the respective Object Identifier and description:

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	Event Severity	Description
gigamonFMServerConfigBackupCompletionStatusNotification	.1.3.6.1.4.1.26866.6.1.1	FMServerConfigBackupCompletionStatus	Info	GigaVUE-FM sends a notification to the external servers whenever

				r the server backup configuration operation has started.
			Info	GigaVUE-FM sends a notification to the external servers whenever the server backup configuration operation is completed.
			Major	GigaVUE-FM Server configuration backup failed.
gigamonFMServerConfigRestoreCompletionStatusNotification	.1.3.6.1.4.1.26866.6.1.2	ServerConfigRestoreCompletionStatus	Info	GigaVUE-FM sends a notification to the external servers when the server restoration is complete.
			Major	GigaVUE-FM Server configuration

				restore failed.
gigamonFMImageUpgradeStartedNotification	.1.3.6.1.4.1.26866.6.1.3	ImageUpgradeStarted	Info	GigaVUE-FM sends a notification to the external servers if GigaVUE-FM image upgrade process is started.
gigamonFMImageUpgradeCompletedNotification	.1.3.6.1.4.1.26866.6.1.4	ImageUpgradeCompleted	Info	GigaVUE-FM sends a notification to the external server if GigaVUE-FM image upgrade process is complete.
gigamonFMImageUpgradeFailedNotification	.1.3.6.1.4.1.26866.6.1.5	ImageUpgradeFailed	Major	GigaVUE-FM sends a notification to the external server if GigaVUE-FM image upgrade is failed.
gigamonFMImageInstallFinishedNotification	.1.3.6.1.4.1.26866.6.1.6	ImageInstallFinished	Info	GigaVUE-FM sends a notification to the external server if the GigaVUE-

				FM image installation is complete.
gigamonFMSLicenseExpiryEmailSendFailedNotification	.1.3.6.1.4.1.26866.6.1.7	LicenseExpiryEmailSend	Major	GigaVUE-FM sends a notification to the external server if the email sent on the event of License expiry is failed.
gigamonFMLicensesExpiringIn90DaysNotification	.1.3.6.1.4.1.26866.6.1.8	LicensesExpiringIn90Days	Info	GigaVUE-FM sends a notification to the external server if the GigaVUE-FMs license is about to expire in about 90 days.
gigamonFMLicensesExpiredNotification	.1.3.6.1.4.1.26866.6.1.9	LicensesExpiringSoon	Warn	GigaVUE-FM sends a notification to the external server if the GigaVUE-FMs license is about to expire soon. This notification is

				generated when the GigaVUE-FM license is about to expire in 15 days.
gigamonFMLicensesExpiredNotification	.1.3.6.1.4.1.26866.6.1.10	LicensesExpired	Critical	GigaVUE-FM sends a notification to the external server if GigaVUE-FM license is expired.
gigamonFMDeviceAddedNotification	.1.3.6.1.4.1.26866.6.1.11	DeviceAdded	Info	GigaVUE-FM sends a notification to the external server when a new device is added to GigaVUE-FM.
gigamonFMDeviceDeletedNotification	.1.3.6.1.4.1.26866.6.1.12	DeviceDeleted	Info	GigaVUE-FM sends a notification to the external server when a device is deleted from GigaVUE-FM.
gigamonFMSnmpThrottleConfigSaveFailedNotification	.1.3.6.1.4.1.26866.6.1.13	SnmpThrottleConfigSaveFailed	Info	GigaVUE-FM sends a notification

				on to the external server when SNMP Throttle configuration push to devices is failed.
gigamonFMVolumeUsageAlertThresholdExceededNotification	.1.3.6.1.4.1.26866.6.1.14	VolumeUsageAlertThresholdExceeded	Major	GigaVUE-FM sends a notification to the external server when the traffic flow volume exceeds the license limit. This is for both Volume Based License (VBL) and other device licenses. In case of VBL if add-on package are added, then the notification is sent once the volume usage exceeds the volume allowanc

				e of the base bundle as well as the add-on packages volume allowance.
			Critical	
gigamonFMVolumeUsageReportEmailSendFailedNotification	.1.3.6.1.4.1.26866.6.1.15	VolumeUsageReportEmailSendFailed	Major	GigaVUE-FM sends a notification to the external server when the email for the traffic flow volume usage report is failed to send.
gigamonFMFlowComputationErrorEventNotification	.1.3.6.1.4.1.26866.6.1.16	FlowComputationErrorEvent	Critical	GigaVUE-FM sends a notification to the external server when any unexpected error occurs while computing the flow.
gigamonFMSFlowHealthStateChangedNotification	.1.3.6.1.4.1.26866.6.1.17	FlowHealthStateChanged	Info	GigaVUE-FM sends a notification to the external server

				whenever there is a change in the health status.
			Major	
gigamonFMSyslogOverThresholdNotification	.1.3.6.1.4.1.26866.6.1.18	SyslogOverThreshold	Major	GigaVUE-FM sends a notification to the external servers when the number of syslog per minute exceeds the threshold limit. The threshold limit for the respective memory is as follows: For 16GB-100 logs per minute For 32GB-1000 logs per minute For more than 32GB-5000 logs per minute
gigamonSnmpHsmGroupOperationalStatusChangeNotification	.1.3.6.1.4.1.26866.1.1.90	HSMGroupOperationalState	Info	GigaVUE-FM sends a

				notification when the operational state of a HSM Group changes.
gigamonFMHighAvailabilityNotification	.1.3.6.1.4.1.26866.6.1.23	HighAvailability	Info	GigaVUE-FM sends a notification to the external servers when a state change happens in GigaVUE-FM High availability.
			Major	GigaVUE-FM HA Group creation completed unsuccessfully or with partial errors.
			Critical	GigaVUE-FMHA Group initialization failed.
gigamonFMDiskReclaimEventNotification	.1.3.6.1.4.1.26866.6.1.24	DiskReclaimEvent	Clear	GigaVUE-FM sends a notification to the external servers when configura

				tion directory occupies more than 70% of the memory.
			Warn	Disk Reclaim cleared stale indices.
			Critical	Disk Usage is at Critical level.
gigamonFMTrafficDropThresholdExceededEventNotification	.1.3.6.1.4.1.26866.6.1.25	TrafficDropThresholdExceeded	Critical	GigaVUE-FM sends a notification to the external servers when an entity's traffic drop is exceeding the configured threshold in the traffic drop policy.
gigamonFMClusterMemberOnlineEventNotification	.1.3.6.1.4.1.26866.6.1.26	ClusterMemberOnline	Info	GigaVUE-FM sends a notification to the external servers when a not-reachable member in a device

				cluster becomes online.
gigamonFMClusterMemberNotReachableEventNotification	.1.3.6.1.4.1.26866.6.1.27	ClusterMemberNotReachable	Critical	GigaVUE-FM sends a notification to the external servers when one of the members in a device cluster goes not-reachable from the cluster.
gigamonFloatingLicensesExpiredEventNotification	.1.3.6.1.4.1.26866.6.1.28	LicensesExpiredPhysical	Critical	Floating Licenses Expired in devices.
gigamonFloatingLicensesGraceEventNotification	.1.3.6.1.4.1.26866.6.1.29	LicensesInGrace	Critical	Floating Licenses that are in the 45-day window after expiry.
gigamonFMStatsRollUpEventNotification	.1.3.6.1.4.1.26866.6.1.30	FMStatsRollUp	Info	GigaVUE-FM Stats RollUp happens.
			Critical	Failed to Initialize RollUp Job.
gigamonAddFeatureVolumeAllowanceDifferenceEventNotification	.1.3.6.1.4.1.26866.6.1.31	AddFeatureVolumeAllowanceDifferent	Major	Add feature volume allowance differs from base

				bundle allowance.
gigamonFMDiskSpaceEventNotification	.1.3.6.1.4.1.26866.6.1.32	FMDiskSpaceEvent	Info	GigaVUE-FMDisk Usage has reached it's threshold level.
			Warn	GigaVUE-FMDisk Usage has reached it's threshold level.
			Critical	GigaVUE-FMDisk Usage has reached it's threshold level.
gigamonMonitoringSessionConfigUnhealthyNotification	.1.3.6.1.4.1.26866.6.1.33	MonitoringSessionConfigUnhealthy	Critical	GigaVUE-FM sends a notification to the external servers when the Monitoring Session configuration is failed to sync in GigaVUE V Series Node.
gigamonMonitoringSessionTrafficUnhealthyNotification	.1.3.6.1.4.1.26866.6.1.34	MonitoringSessionTrafficUnhealthy	Critical	GigaVUE-FM sends a

				notification to the external servers when the Applications / Tunnel End Points / Raw End Points traffic breaches the threshold in the Monitoring Session.
gigamonMonitoringSessionConfigHealthyNotification	.1.3.6.1.4.1.26866.6.1.35	MonitoringSessionConfigHealthy	Info	GigaVUE-FM sends a notification to the external servers when the Monitoring Session configuration is in sync in GigaVUE V Series Node.
gigamonMonitoringSessionTrafficHealthyNotification	.1.3.6.1.4.1.26866.6.1.36	MonitoringSessionTrafficHealthy	Info	GigaVUE-FM sends a notification to the external servers when the Applications / Tunnel End Points / Raw End

				Points traffic comes below the threshold in the Monitoring Session.
gigamonFabricNodeUnreachableNotification	.1.3.6.1.4.1.26866.6.1.37	NodeUnreachable	Critical	GigaVUE-FM sends a notification to the external servers when the cloud fabric node is down or unreachable.
gigamonFabricNodeUpNotification	.1.3.6.1.4.1.26866.6.1.38	NodeUp	Info	GigaVUE-FM sends a notification to the external servers when the cloud fabric node is running OK.
gigamonFabricNodeDeletedNotification	.1.3.6.1.4.1.26866.6.1.39	NodeDeleted	Info	GigaVUE-FM sends a notification to the external servers when the cloud fabric node is deleted from the Monitoring

				ng Domain.
			Major	Failed to delete node with IP from ESXi host.
			Critical	Failed to delete node name in maintenance mode state with IP from database and host. Node should be deleted directly on host through vCenter.
gigamonFabricNodeRestartFailedNotification	.1.3.6.1.4.1.26866.6.1.40	NodeRestartFailed	Info	GigaVUE-FM sends a notification to the external servers when the cloud fabric node restart is failed.
			Critical	GigaVUE-FM sends a notification to the external servers

				when the cloud fabric node restart is failed.
gigamonFabricNodeRebootFailedNotification	.1.3.6.1.4.1.26866.6.1.41	NodeRebootFailed	Major	GigaVUE-FM sends a notification to the external servers when the cloud fabric node reboot is failed.
			Critical	GigaVUE-FM sends a notification to the external servers when the cloud fabric node reboot is failed.
gigamonFabricNodeUnrecoverableNotification	.1.3.6.1.4.1.26866.6.1.42	NodeUnrecoverable	Critical	GigaVUE-FM sends a notification to the external servers when the cloud fabric node is unrecoverable after multiple reboots.
gigamonFabricNodeRegisteredNotification	.1.3.6.1.4.1.26866.6.1.43	FabricNodeRegistered	Info	GigaVUE

				-FM sends a notification to the external servers when the cloud fabric node registration event is raised in Third Party Orchestration.
			Warn	UCT-V Controller version in request is not the actual version.
			Critical	Failed to get UCT-V interface details.
gigamonFabricNodeUnRegisteredNotification	.1.3.6.1.4.1.26866.6.1.44	FabricNodeUnRegistered	Info	GigaVUE-FM sends a notification to the external servers when the cloud fabric node deregistration event is raised in Third Party Orchestration.
			Critical	V Series Node

				with id not found.
gigamonFabricNodeHeartbeatNotification	.1.3.6.1.4.1.26866.6.1.45	FabricNodeHeartbeat	Critical	GigaVUE-FM sends a notification to the external servers when the cloud fabric node heartbeat event raised in Third Party Orchestration.

gigamonVSeriesOperationalUnhealthyNotification	.1.3.6.1.4.1.26866.6.1.46	VSeriesNodeOperationalUnhealthy	Critical	GigaVUE-FM sends a notification to the external servers when the GigaSMART Applications service is crashed or hanged in GigaVUE V Series Node.
gigamonVSeriesOperationalHealthyNotification	.1.3.6.1.4.1.26866.6.1.47	VSeriesNodeOperationalHealthy	Info	GigaVUE-FM sends a notification to the external servers when the GigaSMART Applications service is recovered in GigaVUE V Series Node.

Corrective Actions for GigaVUE-FM Alarms

This section provides corrective actions that you must perform when you see an Alarm.

Alarms Related to Traffic

Port Unhealthy

Description

This alarm is generated under the following circumstances:

- The status of the port is Admin-Enabled, however, the port link is down.
- The port traffic is unhealthy based on the configured parameters.

Corrective Action

1. Check whether the connections are enabled at the port.
2. Check the hardware status of the port.
3. Check whether the traffic crosses the upper or lower threshold value defined.
4. Check whether the GigaSMART engine ports have traffic drops.
5. Contact Customer Support.

Port Pair Unhealthy

Description

This alarm is generated when a port pair becomes unhealthy based on the associated ports.

Corrective Action

Refer to [Port Unhealthy](#).

Port Group Unhealthy

Description

This alarm is generated when a port group becomes unhealthy based on the associated ports or GigaStreams.

Corrective Action

Refer to [Port Unhealthy](#).

Tunnel Port Unhealthy

Description

This alarm is generated based on the health status of the tunnel ports. Tunnel ports are supported in devices that run on GigaVUE-OS versions 5.4.xx and below. The tunnel port is replaced with IP Interface on devices that run on GigaVUE-OS versions 5.5.xx and above.

Corrective Action

1. Check whether the IP address of the tunnel is resolved.
2. If the ARP is unresolved, check the configurations at the port level.
3. If the ports associated with the tunnel is unhealthy, refer to [Port Unhealthy](#).

IP Interface Unhealthy

Description

This alarm is generated based on the health status of the ports that are attached to the IP Interface.

Corrective Action

1. Check whether the IP address of the IP interface is resolved.
2. If the ARP is unresolved, check the configurations at the port level.
3. If the ports associated with the IP interface is unhealthy, refer to [Port Unhealthy](#).

Map Unhealthy

Description

This alarm is generated when a map becomes unhealthy based on the health of the components associated with the map. The components include ports, port groups, virtual ports, GigaStreams, IP interfaces, inline tools, inline tool groups, inline networks, inline network groups, tool mirror, and so on.

Corrective Action

Refer to the following sections:

- [Port Unhealthy](#)
- [Virtual Port Unhealthy](#)
- [IP Interface Unhealthy](#)

GigaStream Unhealthy

Description

This alarm is generated when the GigaStream is unhealthy based on the health of the components associated with the GigaStream or when the traffic distribution across the ports in a GigaStream exceeds or falls below a user-defined threshold value.

Corrective Action

- Check if the underlying ports are unhealthy, refer to [Port Unhealthy](#).
- Change the Advanced Hash settings
- Use a Weighted GigaStream to apply more hashing buckets to under utilized ports and lesser hashing buckets to over utilized ports

Inline Network Unhealthy

Description

This alarm is generated when the inline network ports associated with the inline network is unhealthy.

Corrective Action

Refer to [Port Unhealthy](#).

Inline Network Group Unhealthy

Description

This alarm is generated when the inline ports or inline networks associated with the inline network group is unhealthy.

Corrective Action

Refer to [Port Unhealthy](#).

Inline Tool Unhealthy

Description

This alarm is generated when the inline tool ports associated with the inline tool is unhealthy.

Corrective Action

1. Check if the heartbeat of the inline tool is healthy.
2. Check if the inline tool is enabled.
3. Refer to [Port Unhealthy](#).

Inline Tool Group Unhealthy

Description

This alarm is generated when the inline ports or inline tools associated with the inline tool group is unhealthy.

Corrective Action

Refer to [Port Unhealthy](#).

Tunnel Logical Group Unhealthy

Description

This alarm is generated for a tunnel logical group when the components (maps and IP Interfaces) participating in the tunnel encapsulation and tunnel decapsulation turn unhealthy.

Corrective Action

- Check the health status of the IP Interface and maps components associated with tunnel logical group encapsulation and decapsulation.
- Bring up the health status of the required component to clear the alarm.

Traffic Drop Threshold Exceeded

Description

This alarm is generated when computed traffic drop value for a given entity exceeds the configured threshold value. For software version 6.1.00, Traffic Drop Identification is supported only for Tunnel Logical Group.

Corrective Action

Check and fix the following:

- Network Connectivity used for tunnel encapsulation and decapsulation.
- Over Utilization of the link.

- Incorrect tunnel encapsulation and decapsulation configuration.

Re-evaluate threshold value that must be configured in the alert policy.

Giga Fabric Map Unhealthy

Description

This alarm is generated when the Fabric Map is unhealthy due to its associated components.

Corrective Action

1. Check the health status of the ports or GigaStream associated with the Fabric Map.
2. Bring the health status up for the required component to clear the alarm.

Alarms Related to GigaVUE Nodes and Clusters

Low Memory

Description

This alarm is generated when certain applications or processes overload the memory of the device.

Corrective Action

1. Run the **show system-health box-id <box id>** command. The memory usage statistics such as the total, used, and free amount of physical and swap memory available are displayed. The memory usage for all the processes is displayed and the process consuming the largest amount of memory is displayed at the top. Refer to [Display the System Health Statistics](#).
2. Make a note of the processes that have crossed the pre-defined threshold value for the device. Refer to [Enable the System Health Threshold Notification](#).
3. Make a note of all the configuration changes after which the alarm was generated.
4. Run the **debug generate dump** command to generate a system dump file.
5. Contact [Customer Support](#).

CPU Overloaded

Description

This alarm is generated when certain applications or processes overload the CPU of the device.

Corrective Action

1. Run the **show system-health box-id <box id>** command. The CPU utilization statistics such as the CPU load average over the last 5 secs, 1 minute, and 5 minutes are displayed. In addition, all the processes running in the cluster or a specified node in the cluster display the CPU utilization for the last 5 second, 1 minute, and 5 minute intervals. The process consuming the largest amount of CPU is displayed at the top. Refer to [Display the System Health Statistics](#).
2. Make a note of the processes that have crossed the pre-defined threshold value for the device. Refer to [Enable the System Health Threshold Notification](#).
3. Make a note of all the configuration changes after which the alarm was generated.
4. Run the **debug generate dump** command to generate a system dump file.
5. Contact [Customer Support](#).

Operational Mode [SAFE or Limited]

Description

During clustering operations, there may be system errors that put the cluster or clustered nodes into unsafe or unstable state. When the node or cluster is at this state, the upcoming configurations or operations may cause the system to crash, cluster to deform, and data traffic to be impacted.

Corrective Action

You need to reset the device. Refer to the "reset" topic in the *GigaVUE-OS CLI Reference Guide*.

Card Unhealthy

Description

This alarm is generated due to various reasons. Most common scenarios are:

- The operational status of the card is "inserted", but the card is not configured.
- The card is configured but the operational status of the card is "shutdown".

- At least 50% of the ports in the card are down.

Corrective Actions

1. Run the **show cards** command. The card information is displayed. Refer to the "Displaying Cards" topic in the *GigaVUE-OS CLI Reference Guide*.
2. If the operational status of the card is "inserted", but the card is not configured (as shown in the figure below), run the **card <box ID>/<slot ID>** command to configure the card.

```
Thiago-HC3-VM [sysdumpDemo: master] (config) # show cards
```

Box ID: 1 (master)								
Slot	Config	Oper Status	HW Type	Product Code	Serial Num	HW Rev	PowerReq	PowerPriority
cc1	yes	up	HC3-Main-Board	132-00DR	1DR0-1100	1.0-00	N/A	N/A
1	yes	up	PRT-HC3-X24	132-00DY	1DY0-1000	1.0-0	60	1
2	yes	up	PRT-HC3-C08Q08	132-00DW	1DW0-2001	1.0-0	160	2
3	yes	up (unlicensed)	SMT-HC3-C05	132-00DX	1DX0-1005	1.0-0	200	3
4	yes	up	PRT-HC3-C08Q08	132-00DW	1DW0-2002	1.0-0	160	4


```
Box ID: 2
```

Slot	Config	Oper Status	HW Type	Product Code	Serial Num	HW Rev
cc1	yes	up	HC1-Main-Board	132-00D6	1D60-0010	1.0-00
1	no	inserted	HC1-X12G4	132-00D7	1D60-0010	1.0-0
2	yes	up	TAP-HC1-G10040	132-00D8	1D80-0020	1.0-0
3	yes	up	TAP-HC1-G10040	132-00D8	1D80-0020	1.0-0

```
Thiago-HC3-VM [sysdumpDemo: master] (config) #
```

3. If the card is configured but the operational status of the card is "shutdown" (as shown in the figure below), run the **no card slot <slot ID> down** command to reactivate the card.

```
Thiago-HC3-VM [sysdumpDemo: master] (config) # show cards
```

Box ID: 1 (master)								
Slot	Config	Oper Status	HW Type	Product Code	Serial Num	HW Rev	PowerReq	PowerPriority
cc1	yes	up	HC3-Main-Board	132-00DR	1DR0-1100	1.0-00	N/A	N/A
1	yes	up	PRT-HC3-X24	132-00DY	1DY0-1000	1.0-0	60	1
2	yes	up	PRT-HC3-C08Q08	132-00DW	1DW0-2001	1.0-0	160	2
3	yes	up (unlicensed)	SMT-HC3-C05	132-00DX	1DX0-1005	1.0-0	200	3
4	yes	up	PRT-HC3-C08Q08	132-00DW	1DW0-2002	1.0-0	160	4


```
Box ID: 2
```

Slot	Config	Oper Status	HW Type	Product Code	Serial Num	HW Rev
cc1	yes	up	HC1-Main-Board	132-00D6	1D60-0010	1.0-00
1	yes	shutdown	HC1-X12G4	132-00D7	1D60-0010	1.0-0
2	yes	up	TAP-HC1-G10040	132-00D8	1D80-0020	1.0-0
3	yes	up	TAP-HC1-G10040	132-00D8	1D80-0020	1.0-0

```
Thiago-HC3-VM [sysdumpDemo: master] (config) #
```

Abnormal Fan Operation

Description

The status and speed of the fan may not be available or the fan trays may not be functional. This may increase the device temperature.

Corrective Action

Perform the following tasks to troubleshoot this issue:

1. Run the **show chassis** command and verify the fan tray status.

```
Fan Tray 2:
  HW type      : N/A
  Product Code  : N/A
  Serial Num    : N/A
  HW Rev       : N/A
  Status       : absent
```

2. If the status is displayed as absent (as depicted in the screenshot above), check and ensure that the fans are inserted properly.
3. Run the **show chassis** command again to verify the fan tray status.
4. Run the **show environment type fan** command to verify the fan speed in RPM.

```
HC3-V2-SDK (config) #
HC3-V2-SDK (config) # show environment type fan
*** Box 1 (GVS-HC300) ***
-----
Fan tray 1 (FAN-HC3-001):
  1st fan      : 11988 RPM
  2nd fan      : 10240 RPM
-----
Fan tray 2 (N/A):
  1st fan      : 0 RPM
  2nd fan      : 0 RPM
```

5. If the RPM is displayed as 0, contact [customer support](#).

NOTE: Ensure that you collect the logs of the **show chassis** and **show environment type fan** commands.

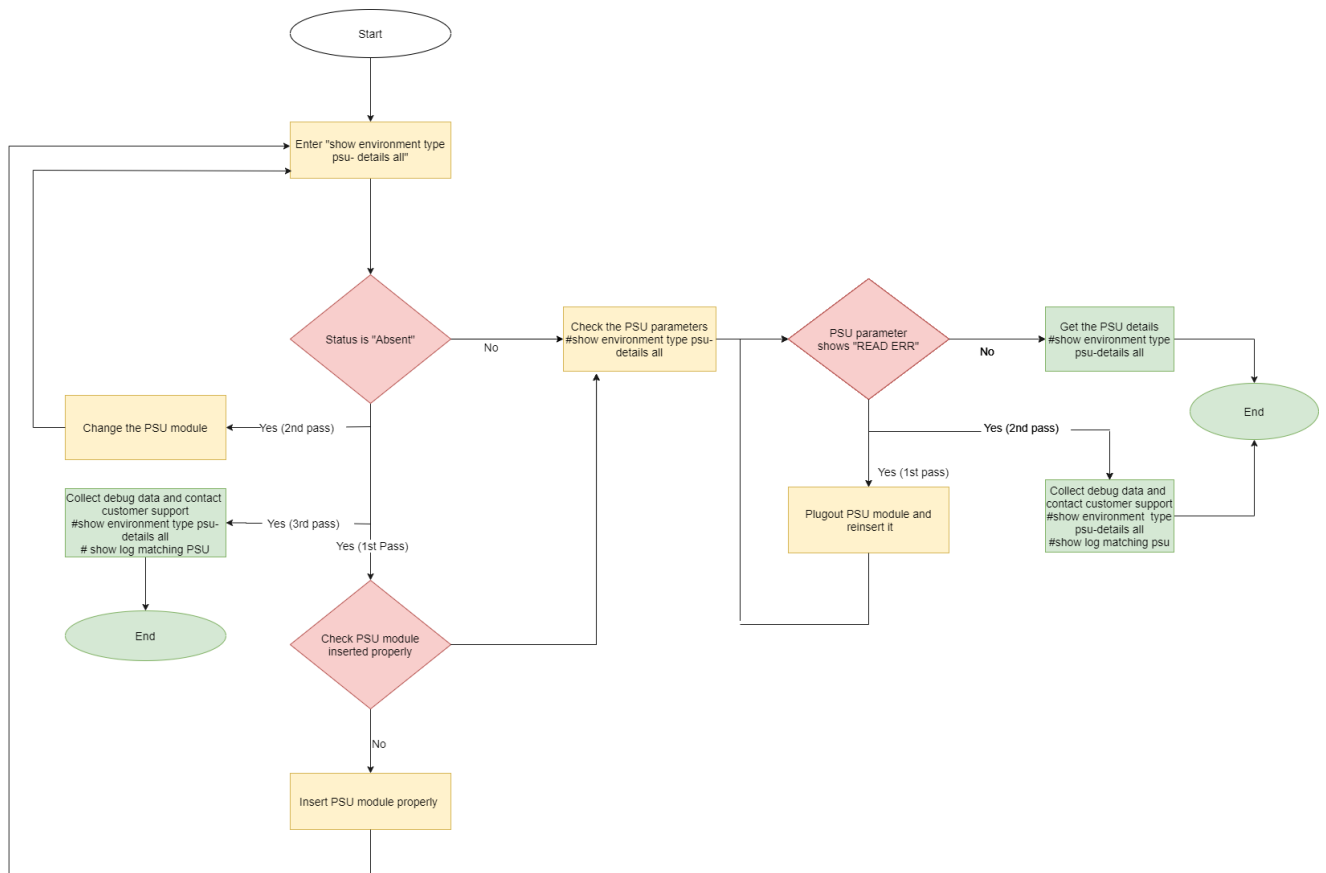
Faulty Power Module

Description

This alarm is generated when the power supply module is faulty.

Corrective Action

Here are the set of tasks depicted in the form of a flow chart. Perform these tasks to troubleshoot this issue.



G-TAP Battery Unhealthy

Description

This alarm is generated when the health status of the battery is below the defined threshold value. If the charge is below 75%, it is indicated by yellow and if it is below 50%, it is indicated by red.

Corrective Action

1. Make sure that the power supply is connected.

2. Check the reason for the power outage.
3. Configure the Battery Optimization feature to avoid traffic drops. Refer to [battery optimization](#).
4. If power is available but battery is not getting detected or charged, remove and reinsert the battery properly.

G-TAP Port Group Incompatible

Description

This alarm is generated when the underlying ports of the G-TAP port group is not compatible with the transceiver and speed.

Corrective Action

- Change the transceiver to match equal speed on all the four ports of G-TAP port group.

Device CPU Temperature Unhealthy

Description

This alarm is generated when the temperature of the device's CPU exceeds the threshold value.

Corrective Action

1. Ensure that all the fans are working properly.
2. If there is a fan failure detected, remove and re-insert the fan tray.
3. Run the **show system-health** command and get the details. Contact Customer Support.

Stack Link Unhealthy

Description

This alarm is generated when the status of the stack link or stack GigaStream is unhealthy.

Corrective Action

1. If the Stack link is unhealthy:

- a. Run the **show port params** command to check the power level of the transceiver used.
 - b. Disable and then enable the ports to bring the stack link up.
2. If Stack GigaStream is unhealthy, reconfigure the Stack GigaStream.
3. If the status is still unhealthy, verify the transceiver inserted in the port.
4. If the port flaps continuously before or during the state, flap the port and then observe the power level of the port.
5. Reload the device and then check the status.
6. If the status is still unhealthy, contact Customer Support.

Device Unreachable/Health Indeterminable

Description

These alarms are generated when a standalone device is unreachable and the health status of the physical and logical components of the unreachable device could not be determined.

Corrective Action

1. Ping the DNS name or IP Address of the device.
2. Check the Console Access of the device.

Device Not Reported/Health Indeterminable

Description

These alarms are generated when a device that is part of a cluster leaves the cluster and therefore is unreachable. Also, the health status of the physical and logical components of the unreachable device could not be determined.

The alarm gets cleared if the device comes online with the same IP address or with a different IP address and is added as a member of the same cluster.

Corrective Action

1. Check if the device is still part of the cluster.
2. Use the following show command to see if the device is part of the cluster.

Show cluster global brief

Cluster Member Not-reachable

Description

This alarm is generated when a member node becomes not-reachable to the cluster leader.

Corrective Action

1. Check and try to bring up the cluster.
2. Add the node to the same cluster.

Alarms Related to GigaSMART

Gsgroup Unhealthy

Description

This alarm is generated when the health status of the GigaSMART engine ports that are associated with the GigaSMART group become unhealthy.

Corrective Action

1. Run the show port command to check the link status.
2. If the link status is down, run the show cards command to check the operational status of the GigaSMART engine port. The status should be Up or Shutdown. If the status is Shutdown, bring up the card.
3. If the status is down, contact Customer Support.
4. Run the show port stats portlist <engine port alias> command to check whether there are any IflnPktDrops. If there are packet drops, GigaSMART engine may be oversubscribed.

Virtual Port Unhealthy

Description

This alarm is generated when the health status of the GigaSMART group to which the virtual port is associated with is unhealthy.

Corrective Action

1. Run the show vport command to determine the GigaSMART group to which the virtual port is associated with.
2. Check the health status of the GigaSMART engine port.

3. Run the show port stats portlist <engine port alias> command to check whether there are any IfInPktDrops. If there are packet drops, GigaSMART engine may be oversubscribed.

GigaSMART Operation Unhealthy

Description

This alarm is generated when the GigaSMART group that the GSOP is associated with is unhealthy.

Corrective Action

1. Run the show gsggrp command to determine the GigaSMART group to which the GSOP is associated with.
2. Refer to [Gsgroup Unhealthy](#)

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)