GigaVUE Administration Guide

GigaVUE

Product Version: 6.3

Document Version: 1.0

Last Updated: Friday, June 2, 2023

(See Change Notes for document updates.)

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.

Document Version	Date Updated	Change Notes
1.0	06/02/2023	The original release of this document with 6.3 GA.

Contents

GigaVUE Administration Guide 1

Change Notes 3

Contents 4

GigaVUE Administration 10

Administer GigaVUE-FM 11

Authentication 11

Overview of Authentication 11

GigaVUE-FM User Management 14

Device Authentication Services 47

Single Sign-On 49

ADFS 50

OKTA 57

Microsoft Azure 59

Configure External IdP in GigaVUE-FM 64

Single Sign-on for GigaVUE-FM High Availability 65

Roles and Users 68

About Role-Based Access 69

Configure Role-Based Access and Set Permissions 69

Tags 74

Introduction to Tags 75

Tag Hierarchy 79

Work with Tags 80

Create User-defined Tag 81

Edit Tags 85

Filter Tags 85

Delete Tags 86

Bulk Upload Tags 86

Import Tags 87

Export Tag Resources 89

Alarms 91

Overview of Alarms 92

Suppressed Alarms 92

Suppressing from Alarms page 93

Suppressing from Physical Nodes page 94

View Alarms 96

- View Alarms based on User's RBAC Persmissions 98
- Manage Alarms 99
- Manage Multiple Alarms 100
- Filter Alarms 100
- Alarm Correlation 101
- Alarms for Fabric Maps and Policies 102
- Events 103
- Drill down to Alarm Source 103

Events 106
- Overview of Events 107
- View Events based on User's RBAC Permissions 108
- Filter Events 110
- Archive or Purge Event Records 112

All Audit Logs 113
- Overview of Audit Logs 113
- Filter Audit Logs 114
- Audit Logs Failure 115
- Archive or Purge Audit Log Records 118

System 120
- Preferences 120
- FIPS 140-2 Compliance in GigaVUE-FM 124
- SNMP Traps 127
- Port Packet Errors and Drops 134
- GigaStream Imbalance Notification 137
- Traffic Drop Identification 144
- Port Discovery 151
- Node Details 154
- IP Resolver 156
- Backup/Restore 158
- Images 170
- Certificates 173
- Event Notifications 196
- Export Data to External Data Server 208
- Licenses 212
- System Logs 213
- Storage Management 216

Tasks 218
- Admin Tasks 219
- Scheduled Tasks 220

Reports 221
- Generate Reports 222
- Overview of Reports 223
- Generate Reports 223

NetFlow Format Support on Exporters 232
Configure Security Options 234
FIPS 140-2 Compliance in GigaVUE-FM 235
View Information About GigaVUE-FM 237
GigaVUE-FM High Availability 238
Prerequisites 257
Steps 257
Configure GigaVUE-FM High Availability in Gigamon Containerized Broker 267
Configure GigaVUE-FM High Availability in OpenStack Environment 267
Disassemble GigaVUE-FM Instances in OpenStack Environment 268
Configure GigaVUE-FM High Availability in VMware NSX-T Manager 268
Disassemble GigaVUE-FM Instances in VMware NSX-T Manager 269
Administer GigaVUE Nodes 271
Introducing the GigaVUE Nodes 271
About the GigaVUE HC Series and TA Series 271
GigaVUE HC Series Features and Benefits 274
Access Nodes From GigaVUE-FM 278
Get Started with GigaVUE Nodes 278
Configure the Host Name 279
Configure Time Options 280
Configure Logging 283
Configure Automatic Email Notifications 285
Use a Custom Banner 287
View Information About the Node 287
Cluster Safe and Limited Modes 290
Configure Port Packet Drop/Error in Devices 294
Configure Security Options 296
About Security and Access 296
About Role-Based Access 298
Configure Authentication and Authorization (AAA) 300
Supported Clients 325
Default Ports 325
FIPS 140-2 Compliance 326
UC APL Compliance 327
Common Criteria 329
GigaVUE-OS Security Hardening 334
Best Practices for Security Hardening 337
License GigaVUE TA Series 340
Chassis 340
Chassis View 340
Table View 344

Manage Roles and Users—GigaVUE-OS 355
About Role-Based Access 355
Configure Role-Based Access and Setting Permissions in GigaVUE Nodes 358
Reboot and Upgrade Options 361
Reboot the Nodes 361
Upgrade the Software 363
Backup and Restore 368
Nodes and Cluster Backup 369
Node and Cluster Restore 374
What Is Saved In a Configuration File 375
Save a Configuration File 376
Share Configuration Files with Other GigaVUE H Series Nodes 376
Use SNMP 377
SNMP and Clusters 377
Configure SNMP Notifications 377
Enable the SNMP Server 383
Monitor Utilization 387
View System Health Information 387
Work with Port Utilization Measurements 394
Configure Alarm Buffer Thresholds 398
About 402
Software Licensing Reference 404
Setting the GigaVUE-FM Admin Password 404
Logging in to GigaVUE-FM Command Line Interface 405
GigaVUE-FM CLI Commands 405
fmctl 406
Mapping of SNMP Traps with GigaVUE-FM Events and Alarms 411
GigaVUE® Fabric Management Events 420
Alarms 420
GigaVUE Cloud Suite 421
Cluster 428
Device 428
Fabric Maps 429
GigaVUE-FM Events 430
G-TAP A Series 2 431
Inline Bypass Solution 431
Software Licensing 431
SNMP 432
ACME 432

Traffic Drop Identification 433
Manage Cluster with Not Reachable Nodes 433
GigaVUE-FM Events 434
Corrective Actions for GigaVUE-FM Alarms 440
Alarms Related to Traffic 441
Port Unhealthy 441
Port Pair Unhealthy 441
Port Group Unhealthy 441
Tunnel Port Unhealthy 442
IP Interface Unhealthy 442
Map Unhealthy 442
GigaStream Unhealthy 443
Inline Network Unhealthy 443
Inline Network Group Unhealthy 443
Inline Tool Unhealthy 443
Inline Tool Group Unhealthy 444
Tunnel Logical Group Unhealthy 444
Traffic Drop Threshold Exceeded 444
Giga Fabric Map Unhealthy 445
Alarms Related to GigaVUE Nodes and Clusters 445
Low Memory 445
CPU Overloaded 446
Operational Mode [SAFE or Limited] 446
Card Unhealthy 446
Abnormal Fan Operation 448
Faulty Power Module 449
G-TAP Battery Unhealthy 449
G-TAP Port Group Incompatible 450
Device CPU Temperature Unhealthy 450
Stack Link Unhealthy 450
Device Unreachable/Health Indeterminable 451
Device Not Reported/Health Indeterminable 451
Cluster Member Not-reachable 452
Alarms Related to GigaSMART 452
Gsgroup Unhealthy 452
Virtual Port Unhealthy 452
GigaSMART Operation Unhealthy 453
Additional Sources of Information 454
Documentation 454
How to Download Software and Release Notes from My Gigamon 457
Documentation Feedback 457
Contact Technical Support 458

Contact Sales 459

Premium Support 459

The VÜE Community 459

Glossary 460

GigaVUE Administration

This guide describes how to get started and administer the GigaVUE® Fabric Manager (GigaVUE-FM) and GigaVUE-OS.

Featured Content:

- Administer GigaVUE-FM
- Administer GigaVUE Nodes
- Software Licensing Reference
- GigaVUE-FM CLI Commands
- Mapping of SNMP Traps with GigaVUE-FM Events and Alarms
- GigaVUE® Fabric Management Events
- Corrective Actions for GigaVUE-FM Alarms
- GigaVUE-FM CLI Commands

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.

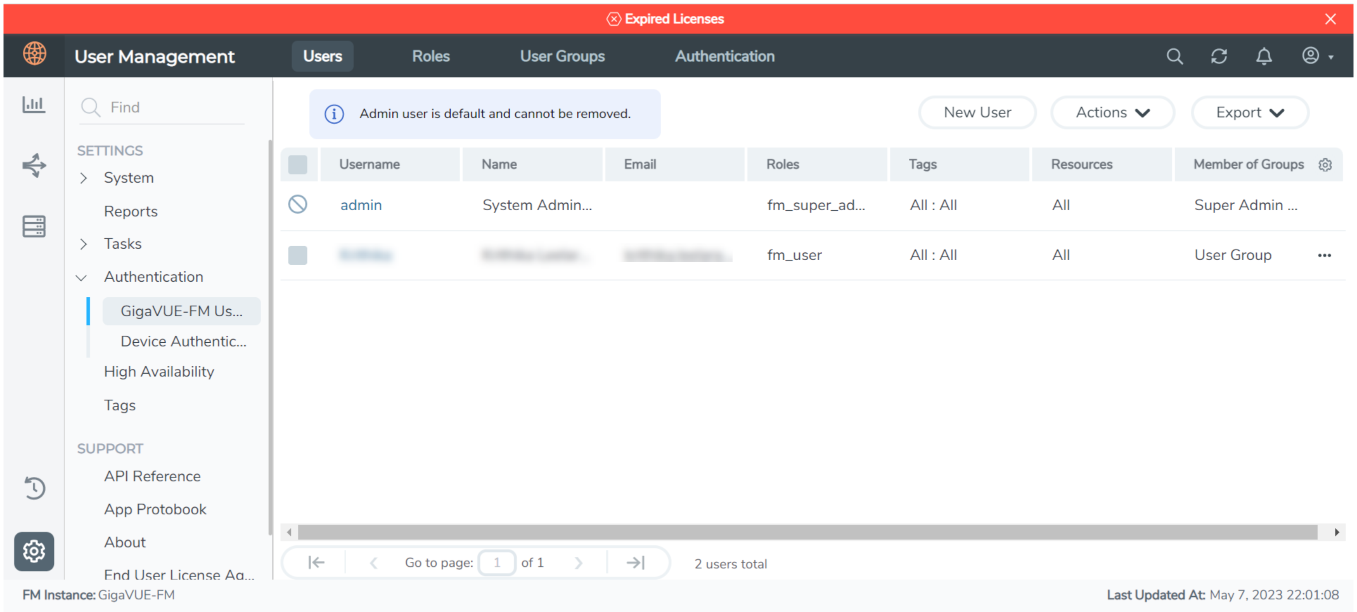
This section covers of the following main topics:

- Overview of Authentication
- GigaVUE-FM User Management
- Single Sign-on
- Authentication Type
- RADIUS
- TACACS+
- 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. On the left navigation pane, click ⚙ and select **Authentication**.



Admin user is default and cannot be removed.

Username	Name	Email	Roles	Tags	Resources	Member of Groups
admin	System Admin...		fm_super_ad...	All : All	All	Super Admin ...
[redacted]	[redacted]	[redacted]	fm_user	All : All	All	User Group

2 users total

Last Updated At: May 7, 2023 22:01:08

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

Software Version	AAA Configuration in GigaVUE-FM	AAA Configuration in CLI	Comments
			GigaVUE-FM in CLI 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
- 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 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.

Users

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.
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 FM security Management category.

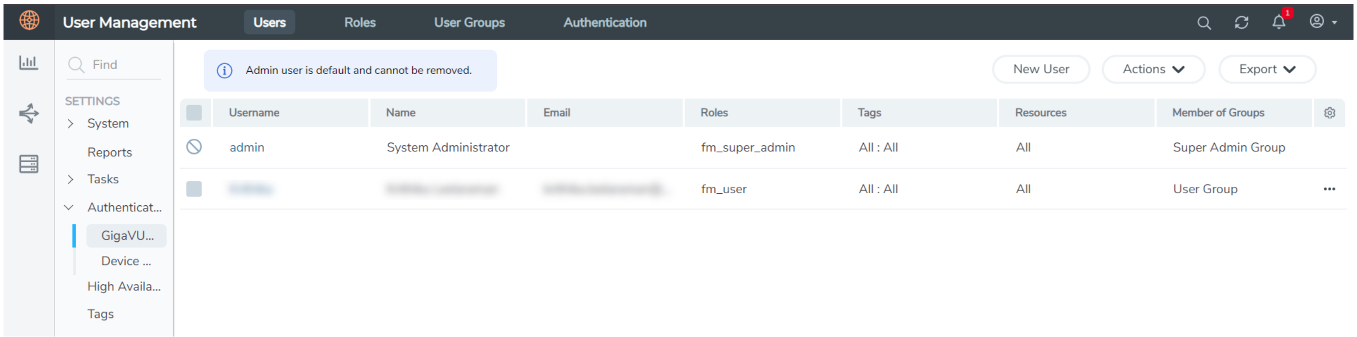
IMPORTANT: It is recommended to create users through GigaVUE-FM:

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

> **NOTE:** Monitor and operator users are not available in GigaVUE-FM. However, if you upgrade from a previous version in which monitor/operator users have been mapped in map default user, then after upgrade:
>
> - **In AAA:** Users authenticated through the external servers will be assigned the fm_user role.
> - **In LDAP:** Remote group based DN entry will not be migrated.

To add users perform the following steps:

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

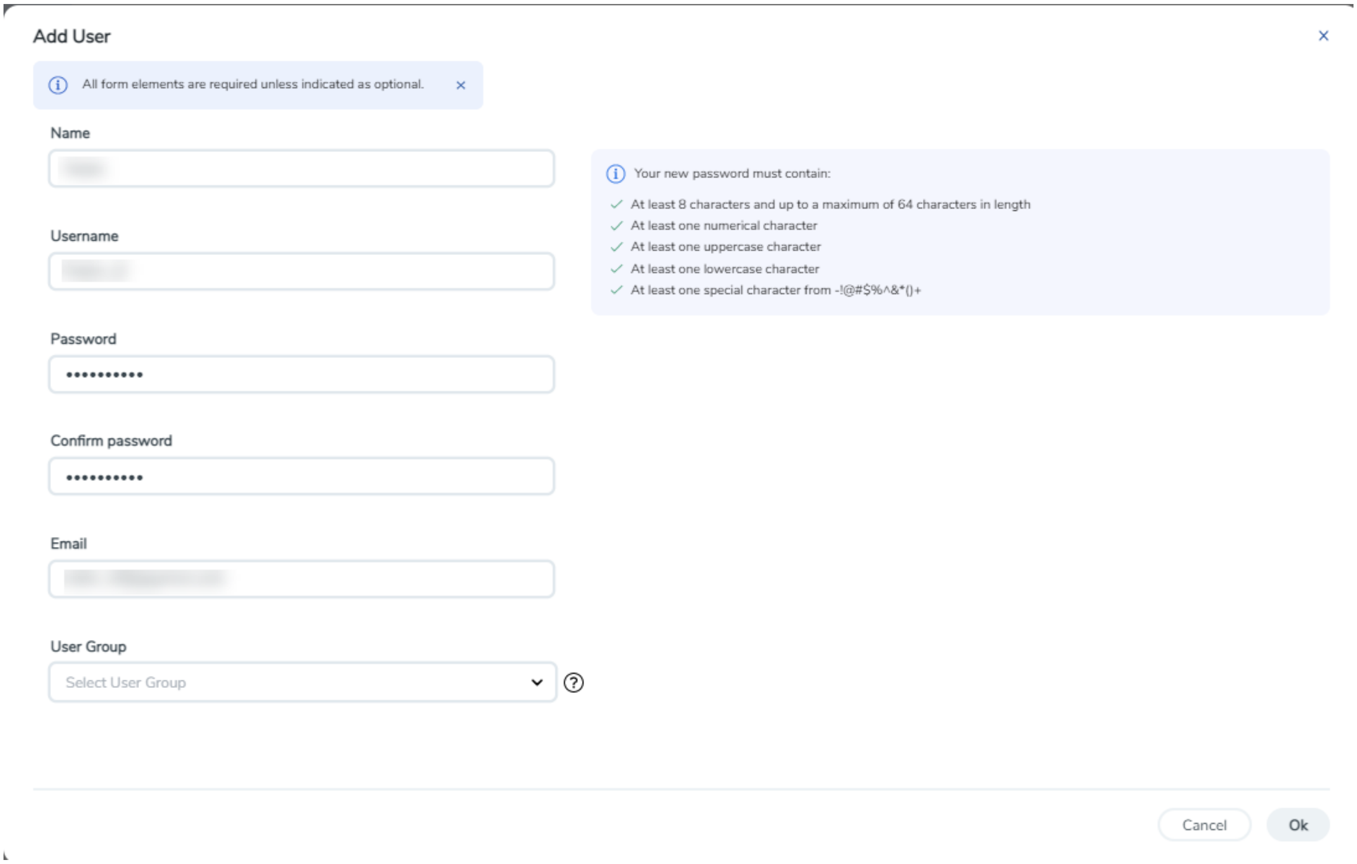


Admin user is default and cannot be removed.

Username	Name	Email	Roles	Tags	Resources	Member of Groups
admin	System Administrator		fm_super_admin	All : All	All	Super Admin Group
[redacted]	[redacted]	[redacted]	fm_user	All : All	All	User Group

Figure 1 *FM Users Page*

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



Add User

All form elements are required unless indicated as optional.

Name

Username

Password

••••••••••

Confirm password

••••••••••

Email

User Group

Select User Group

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 FM security Management category, then click on the ellipsis to:

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

How to Unlock User Account

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

To unlock:

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

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

User Groups

The User Groups page lists the user groups available 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.

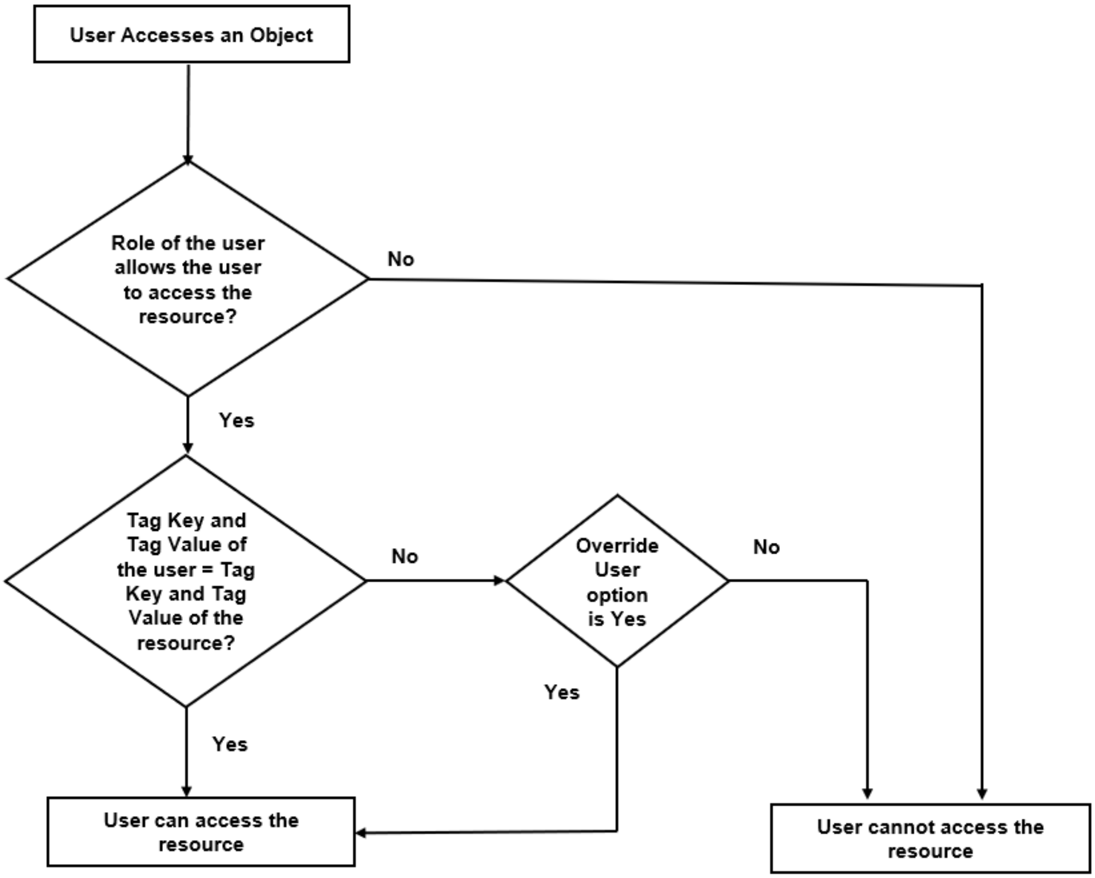
The following user groups are available by default in GigaVUE-FM. You will not be able to edit or change these groups in the system.

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:

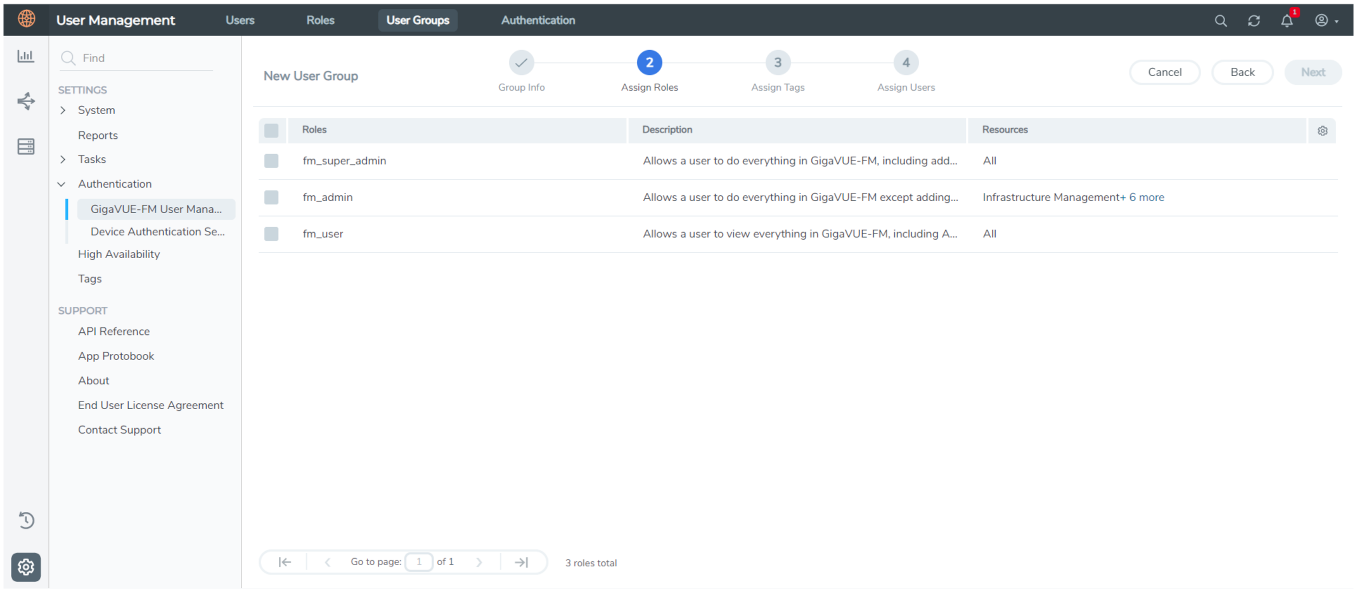
- The category of resources which the user can access, such as the clusters, ports, maps and so on. This is defined using the **Roles** option. Refer to the Roles section for more details.
- The physical and logical resources that the user can access, such as the ports in a cluster that belong to a specific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


User Accesses an Object
Role of the user allows the user to access the resource?
No
Yes
Tag Key and Tag Value of the user = Tag Key and Tag Value of the resource?
No
Override User option is Yes
No
Yes
Yes
User can access the resource
User cannot access the resource

To create a user group:

1. On the left navigation pane, click ⚙, and then select **Authentication> GigaVUE-FMUser 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.



New User Group

Roles	Description	Resources
fm_super_admin	Allows a user to do everything in GigaVUE-FM, including add...	All
fm_admin	Allows a user to do everything in GigaVUE-FM except adding...	Infrastructure Management+ 6 more
fm_user	Allows a user to view everything in GigaVUE-FM, including A...	All

3 roles total

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

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

Click on the ellipses to perform the following operations:

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

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

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

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

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

Category	Associated Resources
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

Category	Associated Resources
	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 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.

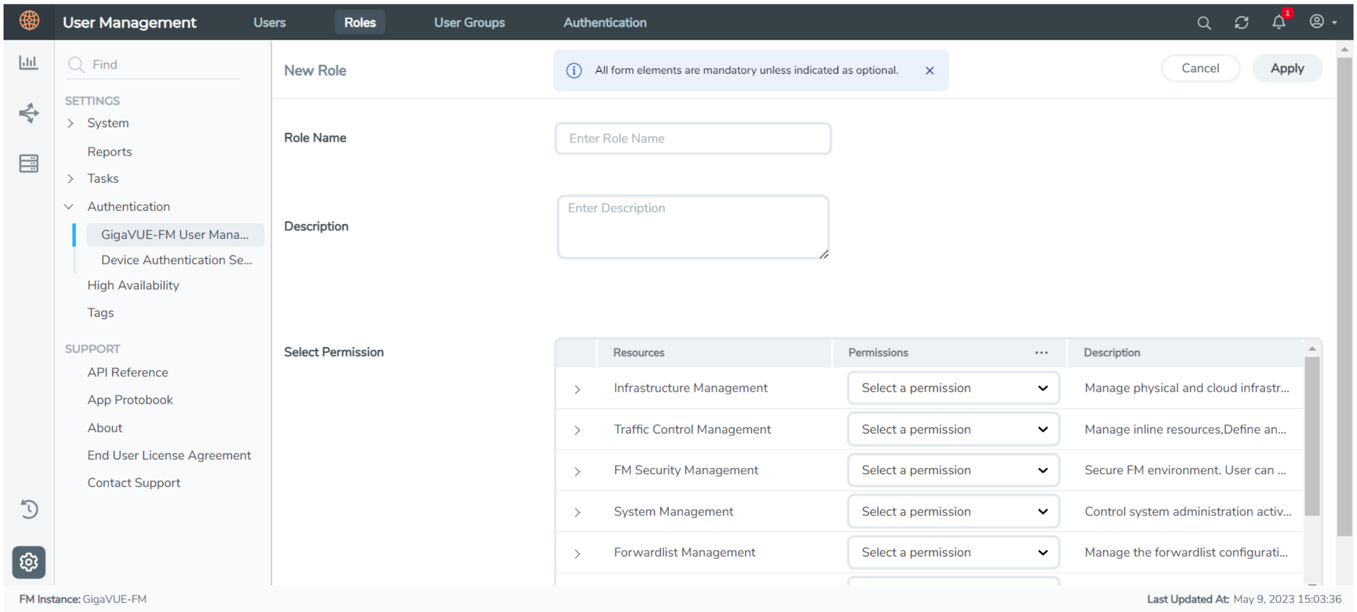
Category	Associated Resources
System Management	Controls system administration activities of GigaVUE-FM. User in this category are allowed to perform operations such as backup/restore of GigaVUE-FM and devices, and upgrade of GigaVUE-FM. The following GigaVUE-FM resources belong to this category: ▪ Backup/restore ▪ 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 ▪ Diameter 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 FM Security Management category.

To create a role

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



New Role

All form elements are mandatory unless indicated as optional.

Role Name: Enter Role Name

Description: Enter Description

Select Permission

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

FM Instance: GigaVUE-FM

Last Updated At: May 9, 2023 15:03:36

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.

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:

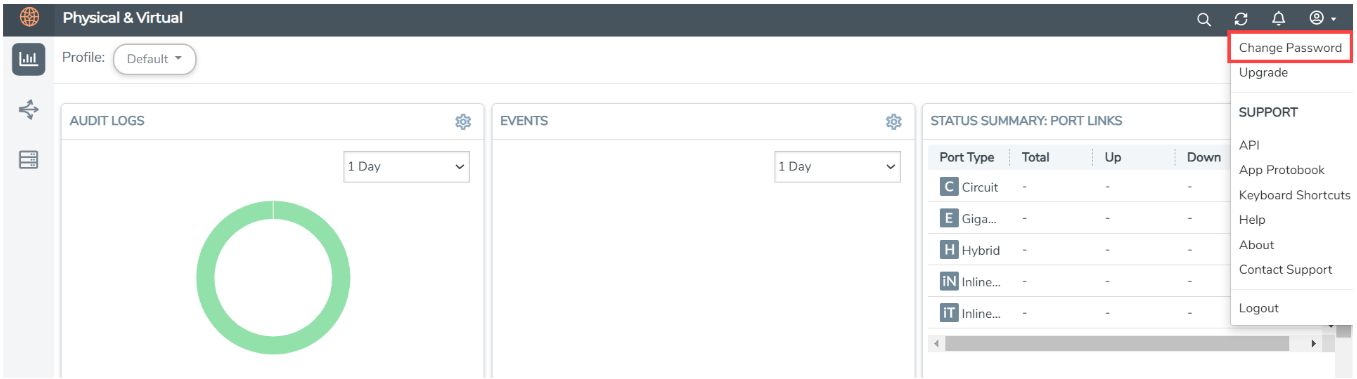
- One numerical character
- One uppercase character
- One lowercase character
- One special character (**!**, **@**, **#**, and so on)

Notes:

- The **Change Your Password** link is available only for locally authenticated users, and will be unavailable for users authenticated against external authentication servers.
- 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**.



Port Type	Total	Up	Down
C Circuit	-	-	-
E Giga...	-	-	-
H Hybrid	-	-	-
iN Inline...	-	-	-
iT Inline...	-	-	-

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 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.

In earlier software versions, you can prioritize the authentication protocols, where in, if one of the authentication mechanism fails GigaVUE-FM will automatically fallback to any of the other methods. Starting in software version 5.8.00, 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*

When upgrading to release 5.8.00, GigaVUE-FM configures the authentication method that was configured with the highest priority in the previous release.

For Example:

In GigaVUE-FM Release 5.7.00 and Previous	In GigaVUE-FM Release 5.8.00 and further
RADIUS, TACACS+, LDAP are configured. RADIUS configured as first priority	RADIUS
RADIUS, LDAP are configured. LDAP is configured as first priority	LDAP

As part of software version 5.8.00, 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 remote. 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's group will be assigned.
TACACS+	tacacsuser1	-	fm_admin	fm_ admin	fm_ admin	The role which has been assigned remotely will be assigned.
TACACS+	tacacsuser3	-	fm_non_exist_group [specified group Does not match any roles in 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 FM]	User Group	User Group	If non-exist group is being assigned

AuthMethod	Logged in User	MapDefaultUserGroup	Remote Roles/Group Base DN (if configured)	Expected Group	Assigned Group	Notes
						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 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 FM]	-	-	If non-exist group is being assigned remotely, then

AuthMethod	Logged in User	MapDefaultUserGroup	Remote Roles/Group Base DN (if configured)	Expected Group	Assigned Group	Notes
						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 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 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.

AuthMethod	Logged in User	MapDefaultUserGroup	Remote Roles/Group Base DN (if configured)	Expected Group	Assigned Group	Notes
LDAP	ldapuser 1	-	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	ldapuser 2	-	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 GigaVUE-FM will check

AuthMethod	Logged in User	MapDefaultUserGroup	Remote Roles/Group Base DN (if configured)	Expected Group	Assigned Group	Notes
						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 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.

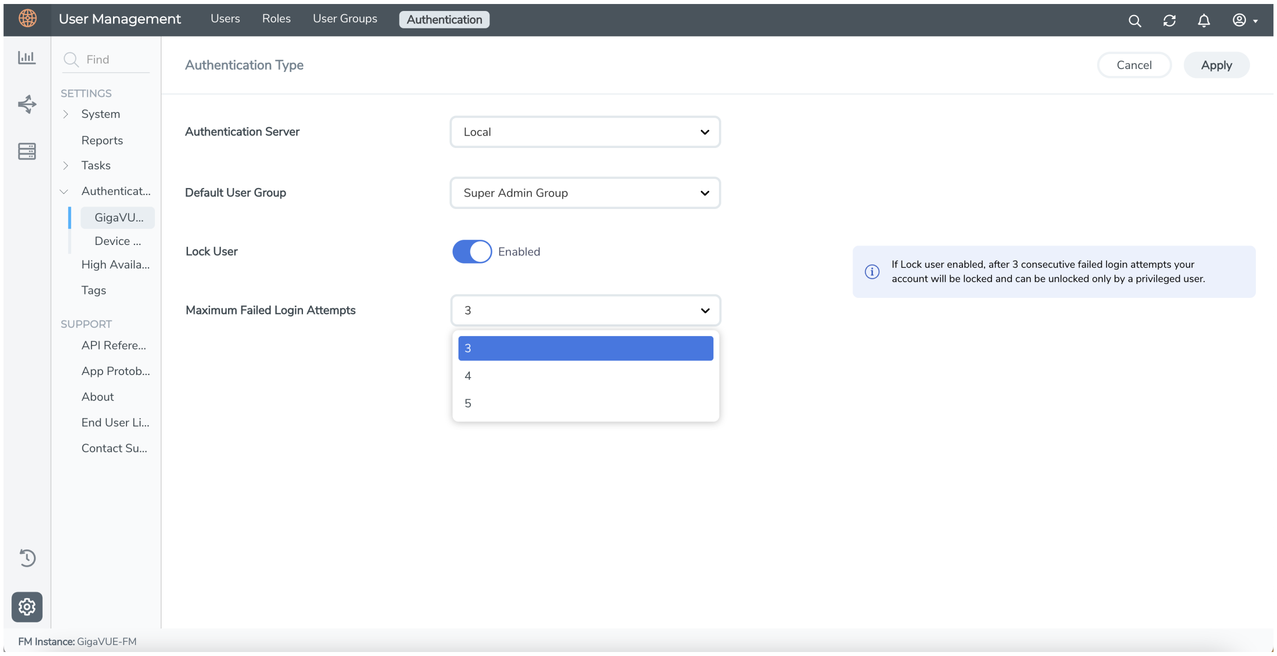
- You can view the status of locked and unlocked users from the GigaVUE-FM User Management page. However, the status in this page does not depict the Near-real Time status. You must manually refresh the screen to know the status. Refer to the Users section for more details.
- Whenever a user account 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 captures 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. On the left navigation pane, click ⚙ , select **Authentication** > **Authentication Type**. In the authentication type page that appears:



Authentication Type

Authentication Server: Local

Default User Group: Super Admin Group

Lock User: Enabled

If Lock user enabled, after 3 consecutive failed login attempts your account will be locked and can be unlocked only by a privileged user.

Maximum Failed Login Attempts: 3

3
4
5

   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 Toggle option to enable and disable the lock-unlock authentication setting.

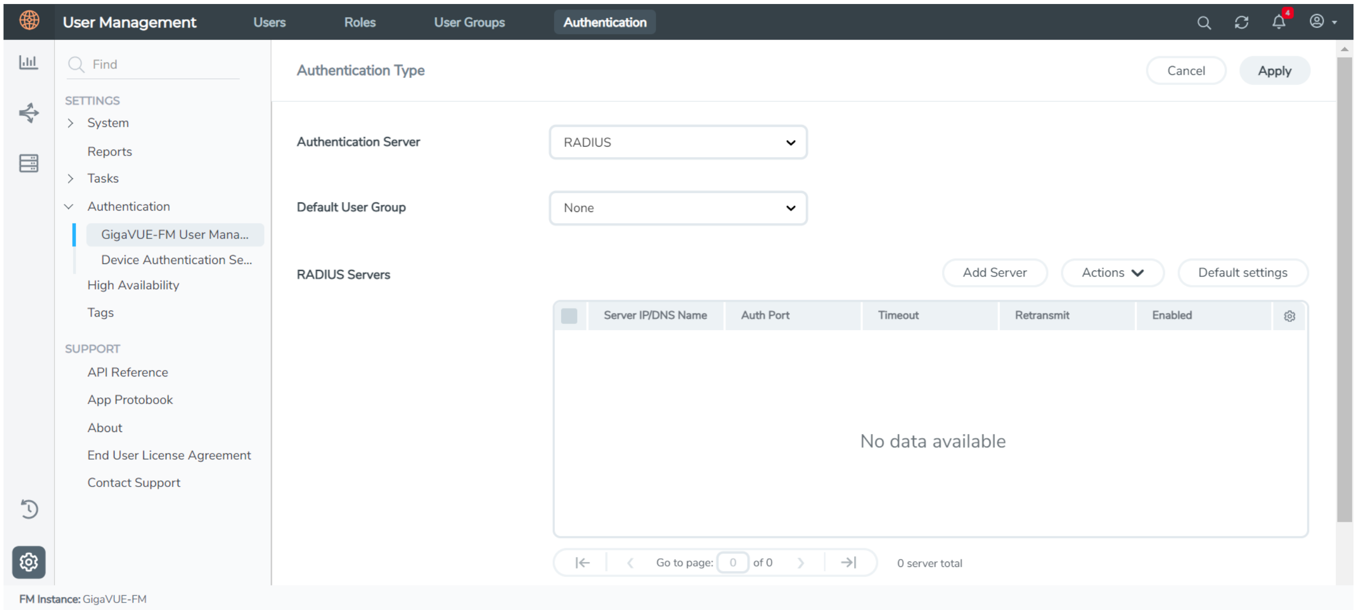
d. Configure the **Maximum Failed Login Attempts**. Allowable range is from 3 to 5. Default is 5. Refer to Configure Lock/Unlock Authentication Setting for Local User Accounts section for more details.

2. Click **Save**.

RADIUS

Only users belonging to the Super Admin User Group or users with write access to 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.



Authentication Type

Authentication Server: RADIUS

Default User Group: None

RADIUS Servers

Server IP/DNS Name	Auth Port	Timeout	Retransmit	Enabled

No data available

Figure 3 *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. For more information about AWS, refer to the *Gigamon Visibility Platform for AWS Getting Started Guide*.

Supported RADIUS Servers

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

RADIUS Server Section: Controls and Fields

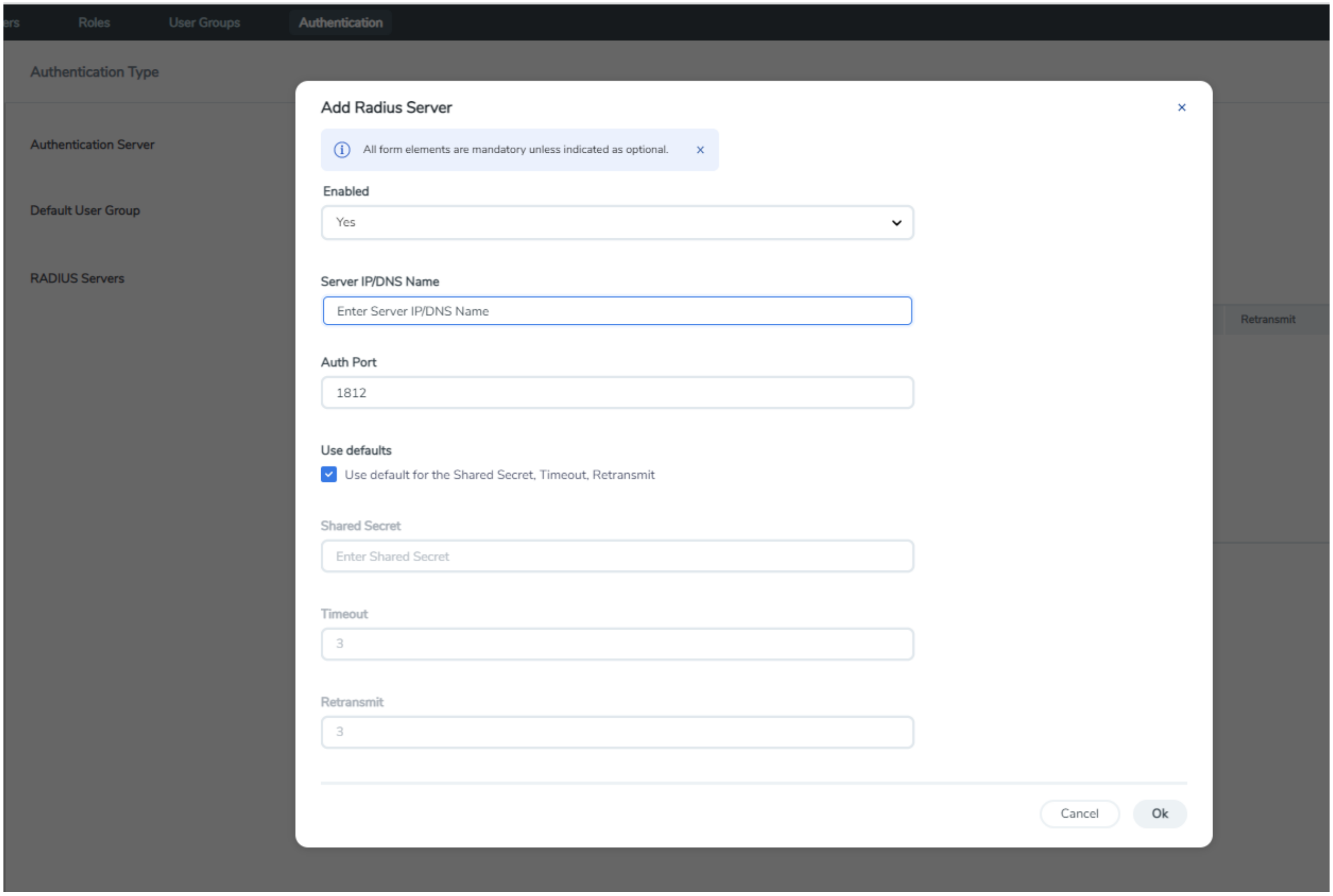
RADIUS Serverssection has the following buttons that allow you to manage the information that appears in the table.

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.

Refer to the Add a New RADIUS Serversection for the description of the fields.

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 4Adding Radius Server.



Add Radius Server

ⓘ All form elements are mandatory unless indicated as optional. ×

Enabled: Yes

Server IP/DNS Name: Enter Server IP/DNS Name

Auth Port: 1812

Use defaults

☑ Use default for the Shared Secret, Timeout, Retransmit

Shared Secret: Enter Shared Secret

Timeout: 3

Retransmit: 3

Figure 4 *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:

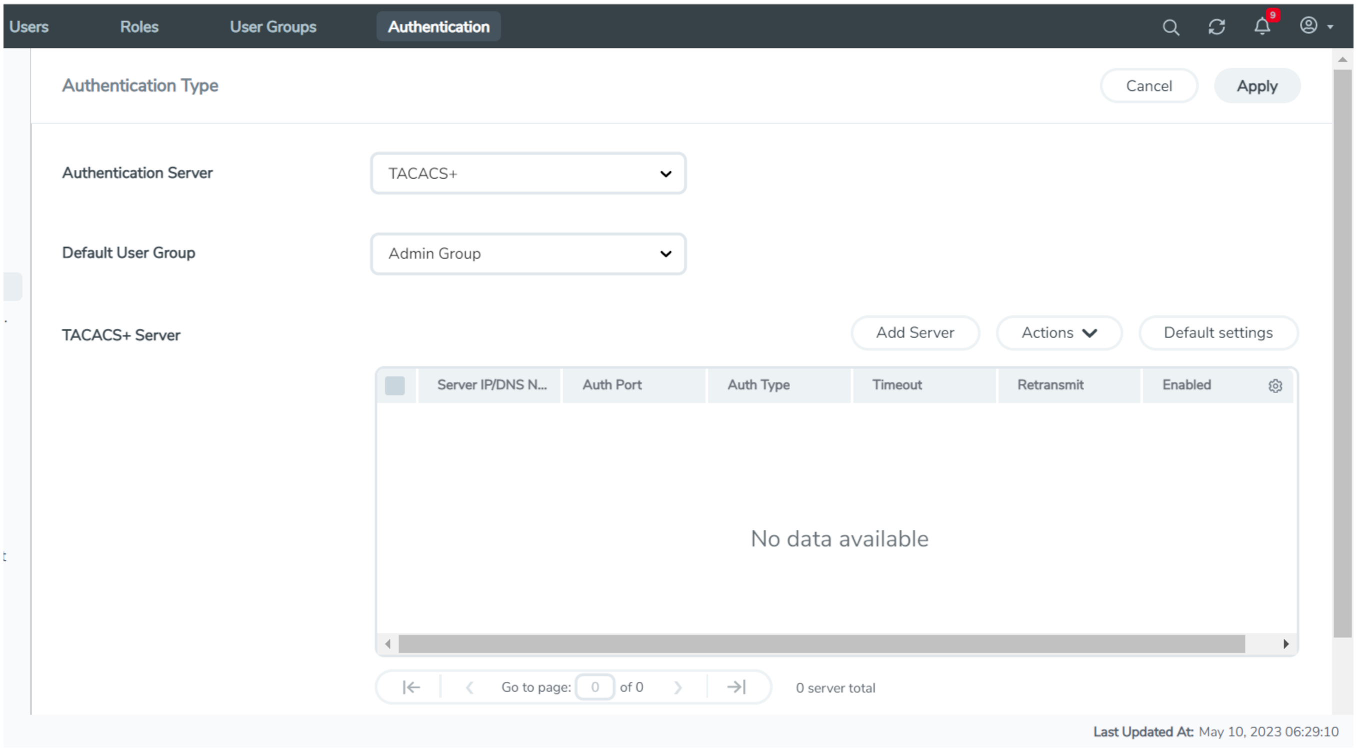
The following table describes the settings.

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.

TACACS+

Only users belonging to the **Super Admin User Group** or users with write access to 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.



Authentication Type

Authentication Server: TACACS+

Default User Group: Admin Group

TACACS+ Server

Server IP/DNS N...	Auth Port	Auth Type	Timeout	Retransmit	Enabled

No data available

Go to page: 0 of 0

0 server total

Last Updated At: May 10, 2023 06:29:10

Figure 5 *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. For more information about AWS, refer to the *Gigamon Visibility Platform for AWS Getting Started Guide*.

Supported TACACS+ Servers

GigaVUE-FM has been tested with the TACACS+ implementation provided by Cisco Secure ACS v5.4.0.46.0. 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.

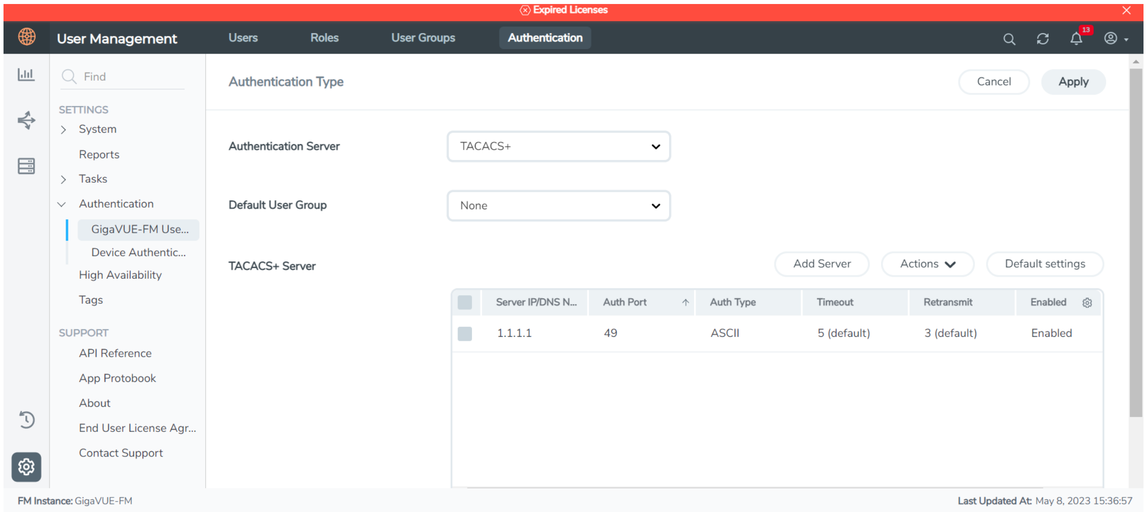
Controls	Description
Add Server	Allows you to add a new TACACS+ Server to the list. See Add a New TACACS+ Server for details.
Actions	Click the Actions drop-down to perform the following: **Edit:** Allows you to change the settings for an existing TACACS+ Server entry. Select a server's entry and click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

Controls	Description	
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.	

Refer to the Add a New TACACS+ Server section for the description of the fields.

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 6 Adding TACACS+ Server Settings.



Authentication Type

Authentication Server: TACACS+

Default User Group: None

TACACS+ Server

Server IP/DNS N...	Auth Port	Auth Type	Timeout	Retransmit	Enabled
1.1.1.1	49	ASCII	5 (default)	3 (default)	Enabled

FM Instance: GigaVUE-FM

Last Updated At: May 8, 2023 15:36:57

Figure 6 *Adding TACACS+ Server Settings*

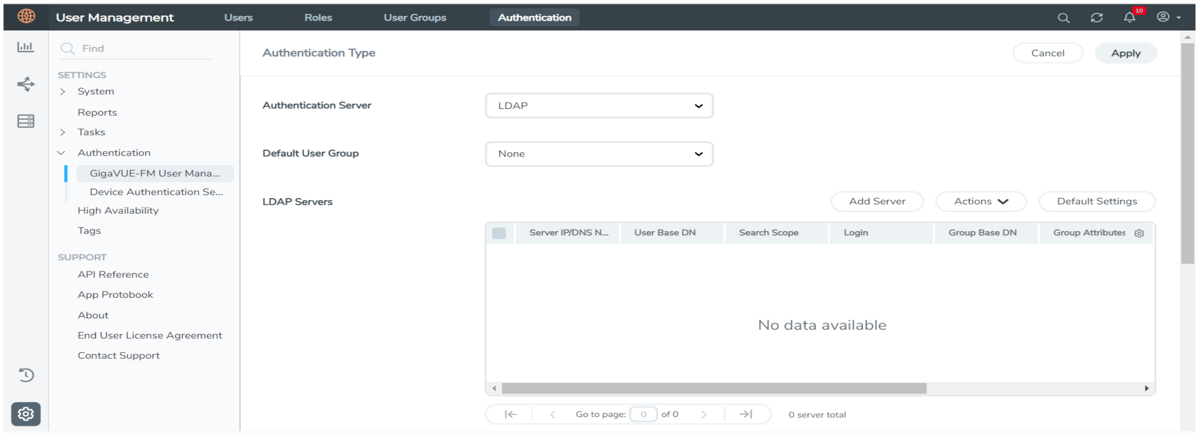
The following table describes the settings.

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 Secret	Specifies a shared secret string to be used for encryption of authentication packets sent

Field	Description
	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.

LDAP

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



Authentication Server: LDAP

Default User Group: None

LDAP 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.

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.

aLDAP 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 LDAP server's schema. 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 Attribut**e 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. 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

Setting	Description
	● 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.

NOTE: Only users belonging to the **Super Admin User Group** or users with write access to the 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>	Class=<comma separated FM groups>	Class=Super Admin Group,Admin Group

Remote Server	In GigaVUE-FM Release 5.7 and earlier (Role Mapping)	In GigaVUE-FM Release 5.8 and further(User Group Mapping)	Example
	[role-<mapping_local_role_2>[...]]]		

> **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.

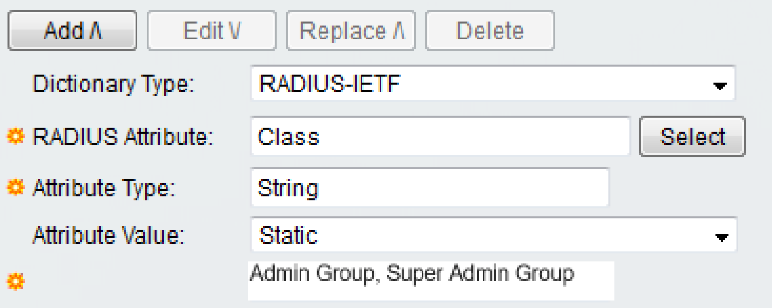
The default groups can be assigned based on the groups assigned in the external authentication server. Refer to Use AAA Server Role Assignments for details.

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



Dictionary Type: RADIUS-IETF

✱ RADIUS Attribute: Class

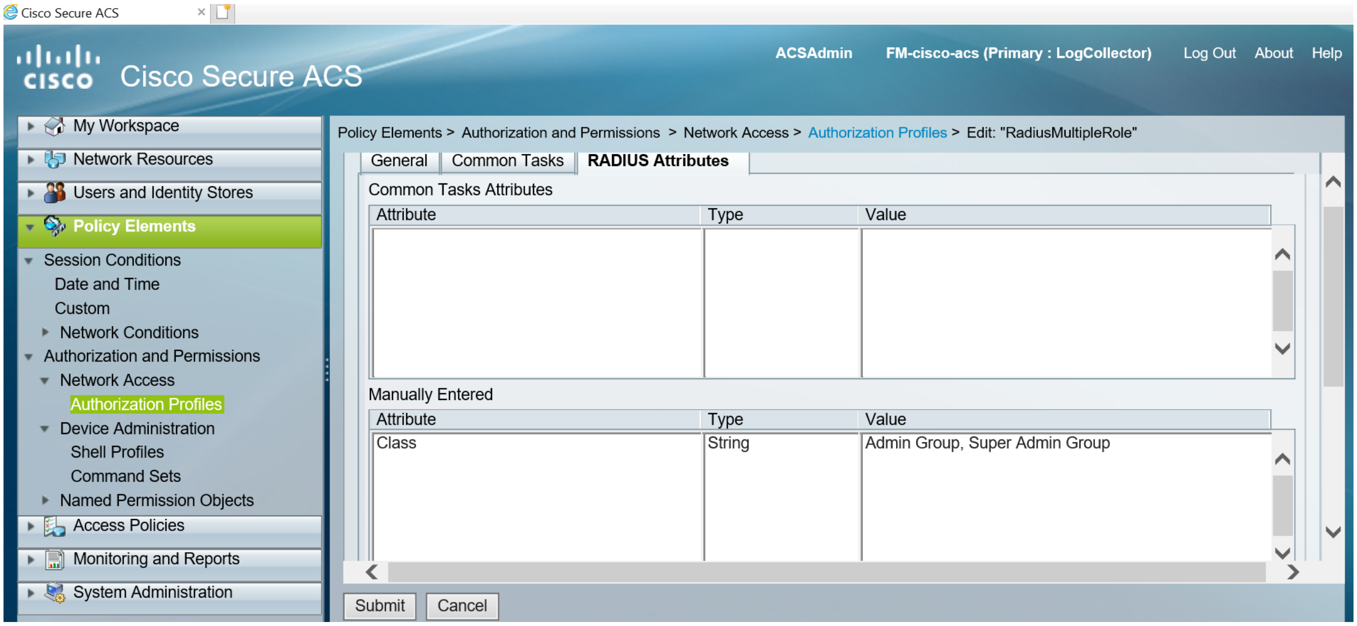
✱ Attribute Type: String

Attribute Value: Static

✱ Admin Group, Super Admin Group

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

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



Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "RadiusMultipleRole"

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value
Class	String	Admin Group, Super Admin Group

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.

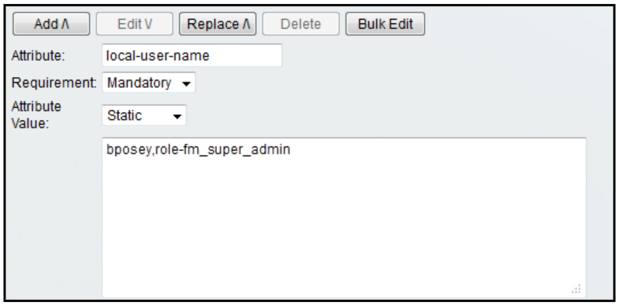
   b. Click the **Custom Attributes** page.

   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



Attribute: local-user-name

Requirement: Mandatory

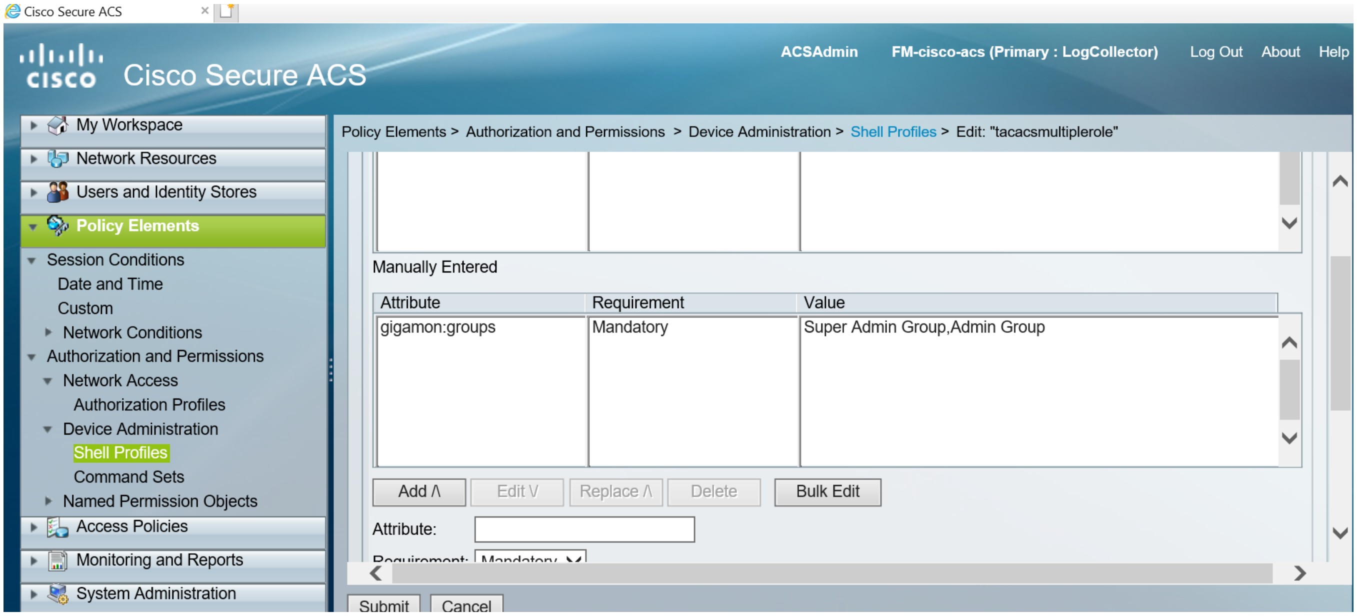
Attribute Value: Static

bposey,role-fm_super_admin

4. Click the **Add** button Add Λ 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 9Supplying 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.



Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "tacacsmultiplerole"

Manually Entered

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

Attribute:

Requirement: Mandatory

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

Device Authentication Services

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

- Default
- LDAP

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. On the left navigation pane, click ⚙ 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 to...
Authentication Priority	Configure AAA Authentication Options
User mapping	User Mapping

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. On the left navigation pane, click ⚙ 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	User Mapping

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.

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:

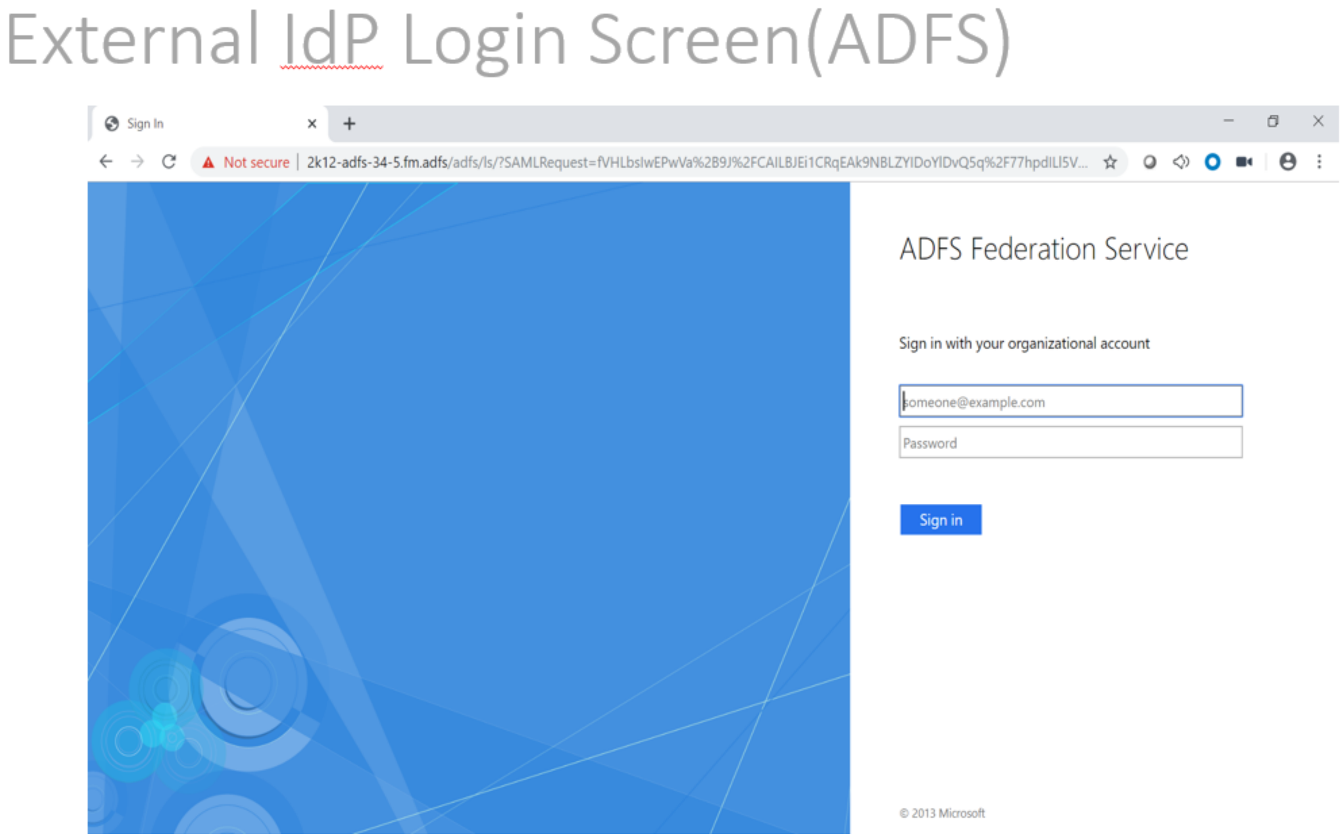
- ADFS
- OKTA
- Microsoft Azure

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)

Not secure | 2k12-adfs-34-5.fm.adfs/adfs/ls/?SAMLRequest=fVHLbslwEPwVa%2B9J%2FCAILBJEi1CRqEAk9NBLZYIDoYIDvQ5q%2F77hpdlLl5V...

ADFS Federation Service

Sign in with your organizational account

someone@example.com

Password

Figure 10 *External IdP Login Screen (ADFS):*

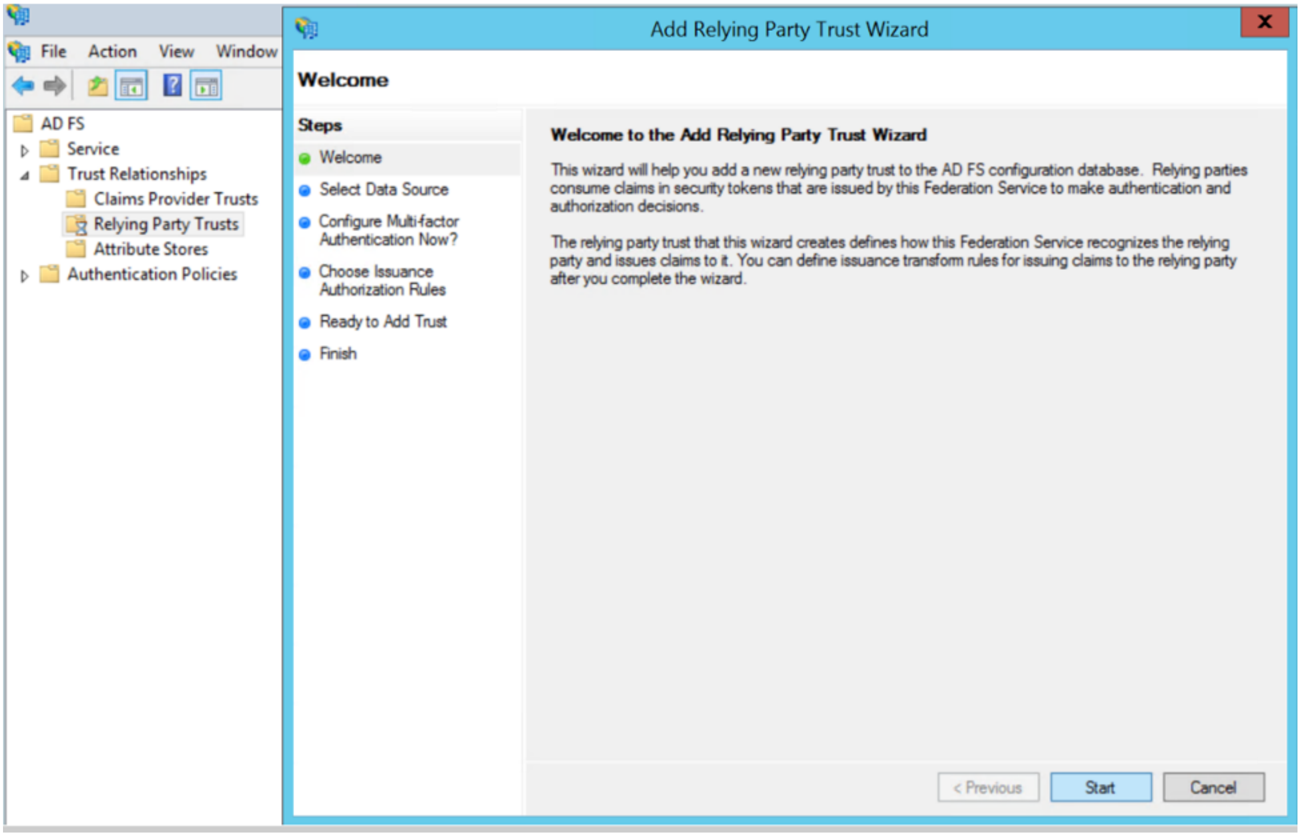
Configure GigaVUE-FM in ADFS

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**.

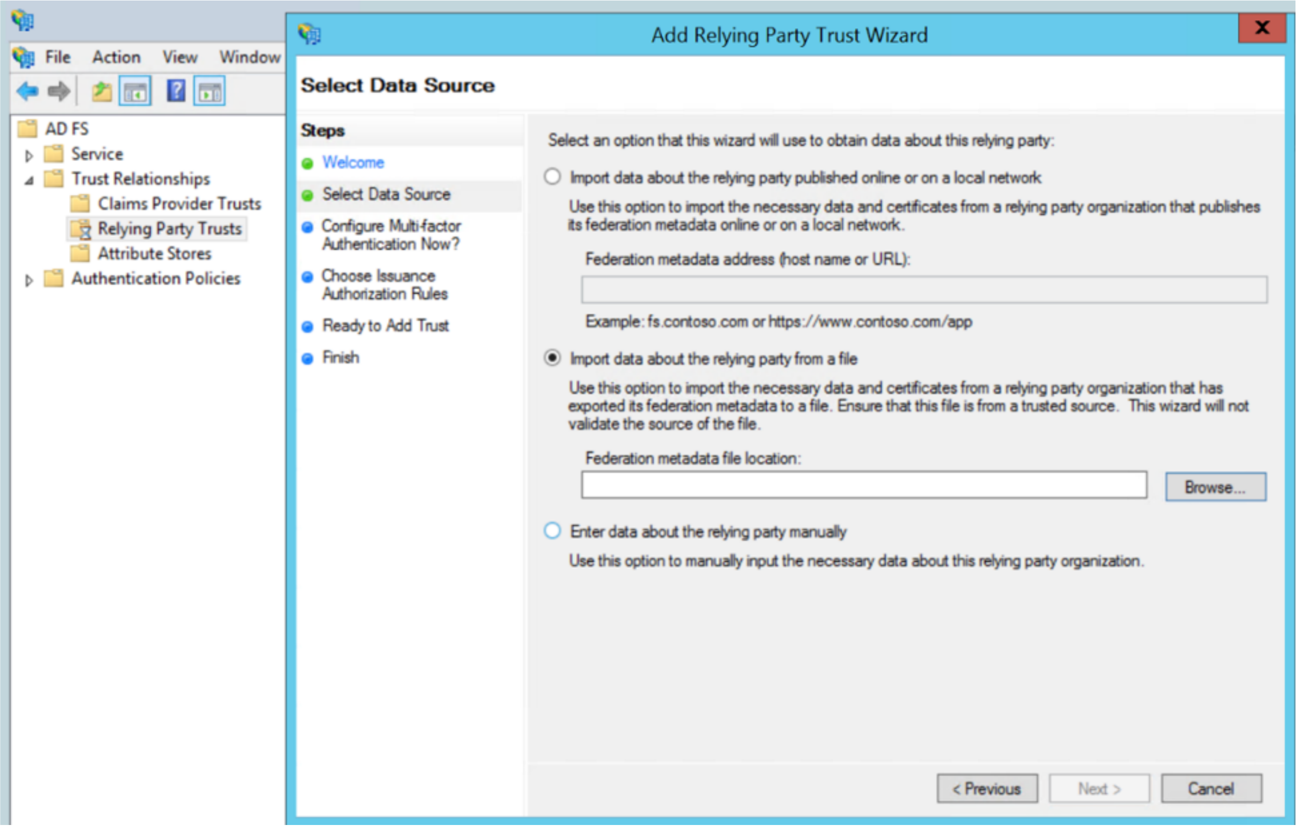


Welcome to the Add Relying Party Trust Wizard

This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.

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.



Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

● Import data about the relying party from a file

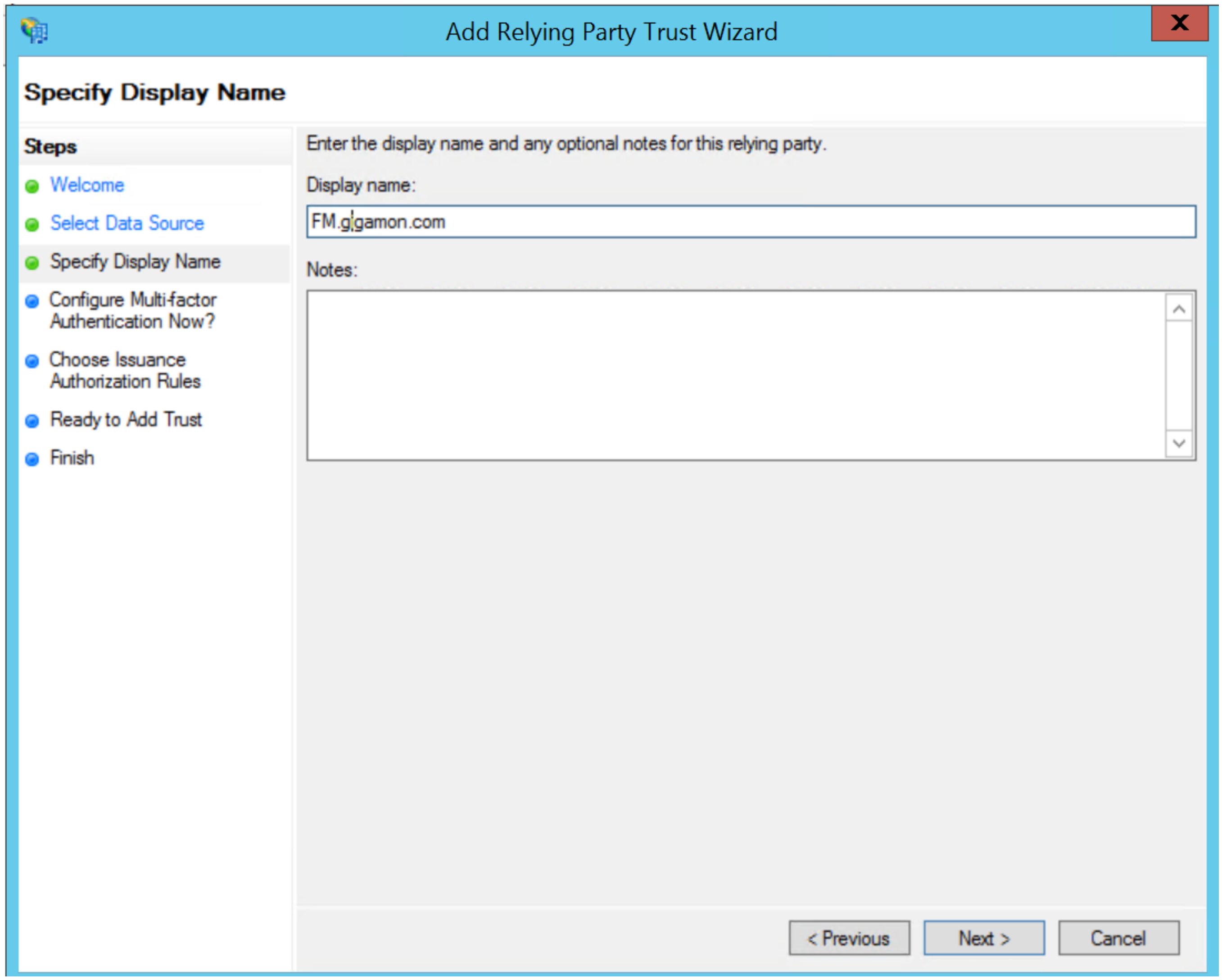
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

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

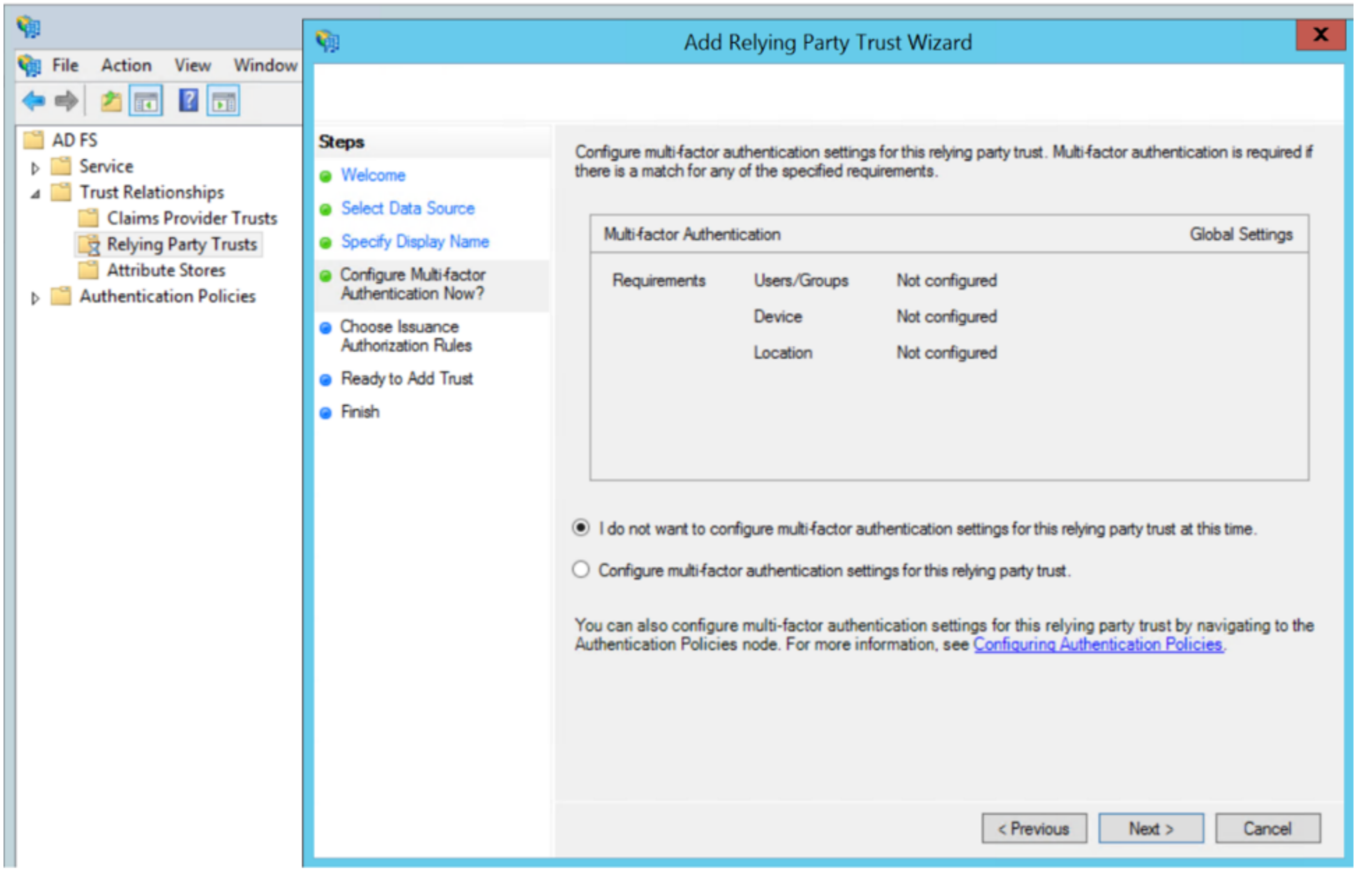


Enter the display name and any optional notes for this relying party.

Display name: FM.gigamon.com

Notes:

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



Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

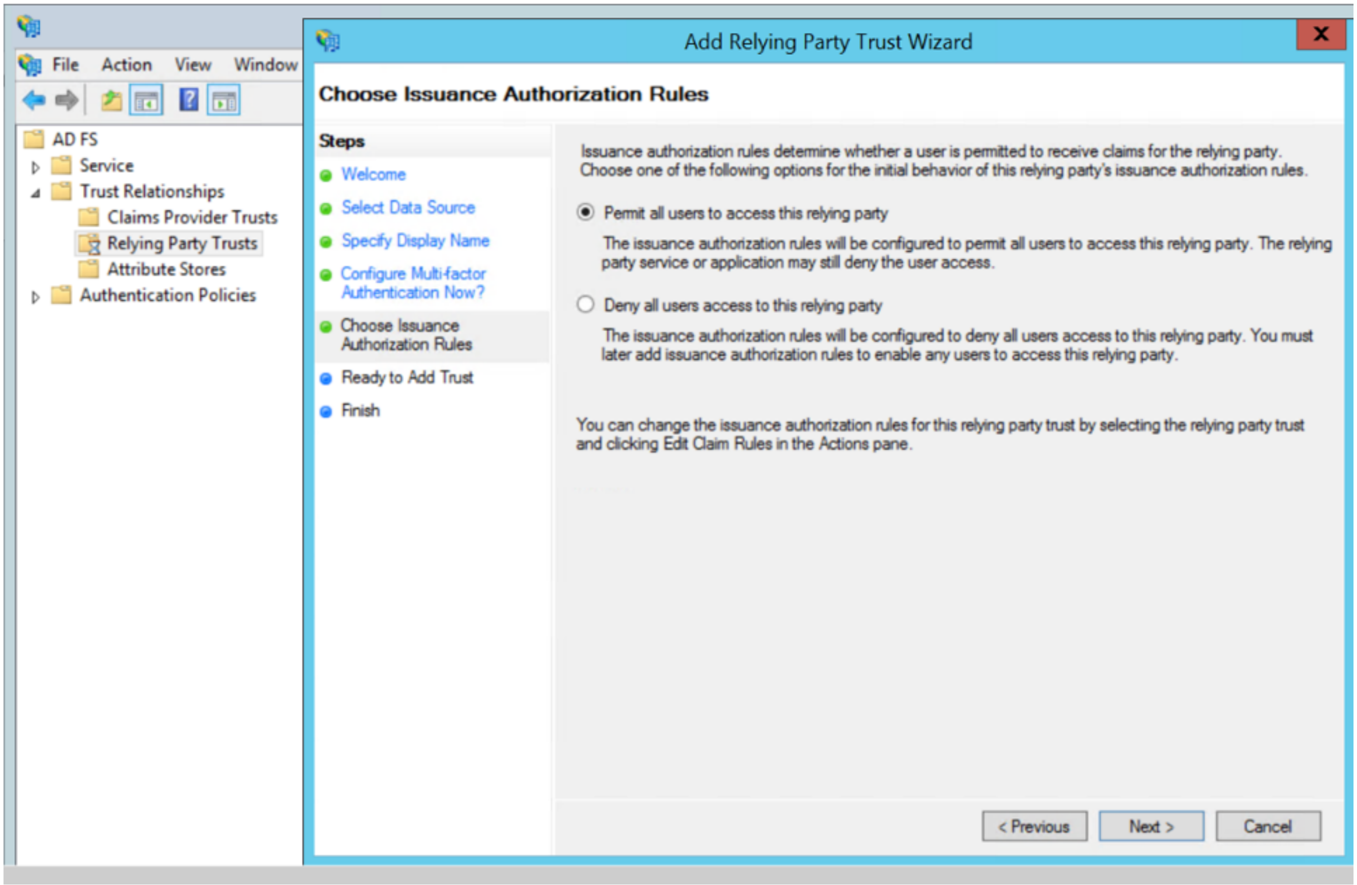
Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

● I do not want to configure multi-factor authentication settings for this relying party trust at this time.

○ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see Configuring Authentication Policies.

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



Choose Issuance Authorization Rules

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

● Permit all users to access this relying party

The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

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 NameId:
   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 NameId.
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 *Use this for Recipient and Destination Address* check box.
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 am on OKTA Customer adding an internal app.*	

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 Consumer Service URL)	https://xx.xx.xx.xx:xxx/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
Unique User Identifier	Enter ***user.userprincipalname.***
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 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 **Settings** -> **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
- How Single Sign-on Works

GigaVUE-FM Configured with Internal IdP

If GigaVUE-FM is configured with internal IdP:

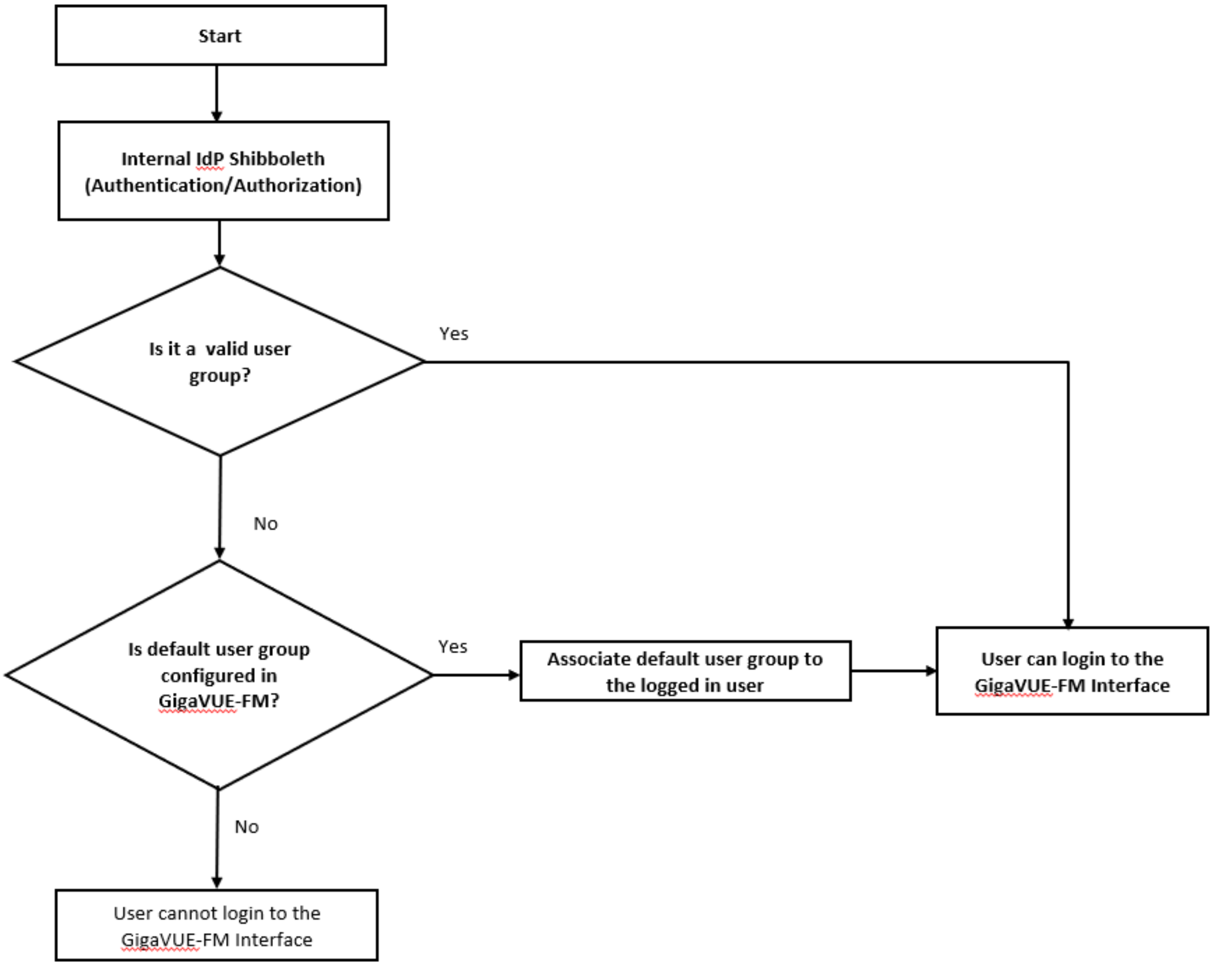
1. GigaVUE-FM sends a request to Shibboleth for authentication.

> **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:


Start
Internal IdP Shibboleth (Authentication/Authorization)
Is it a valid user group?
Yes
No
Is default user group configured in GigaVUE-FM?
Yes
Associate default user group to the logged in user
User can login to the GigaVUE-FM Interface
No
User cannot login to the GigaVUE-FM Interface

GigaVUE-FM Configured with External IdP

If GigaVUE-FM is configured with external IdP:

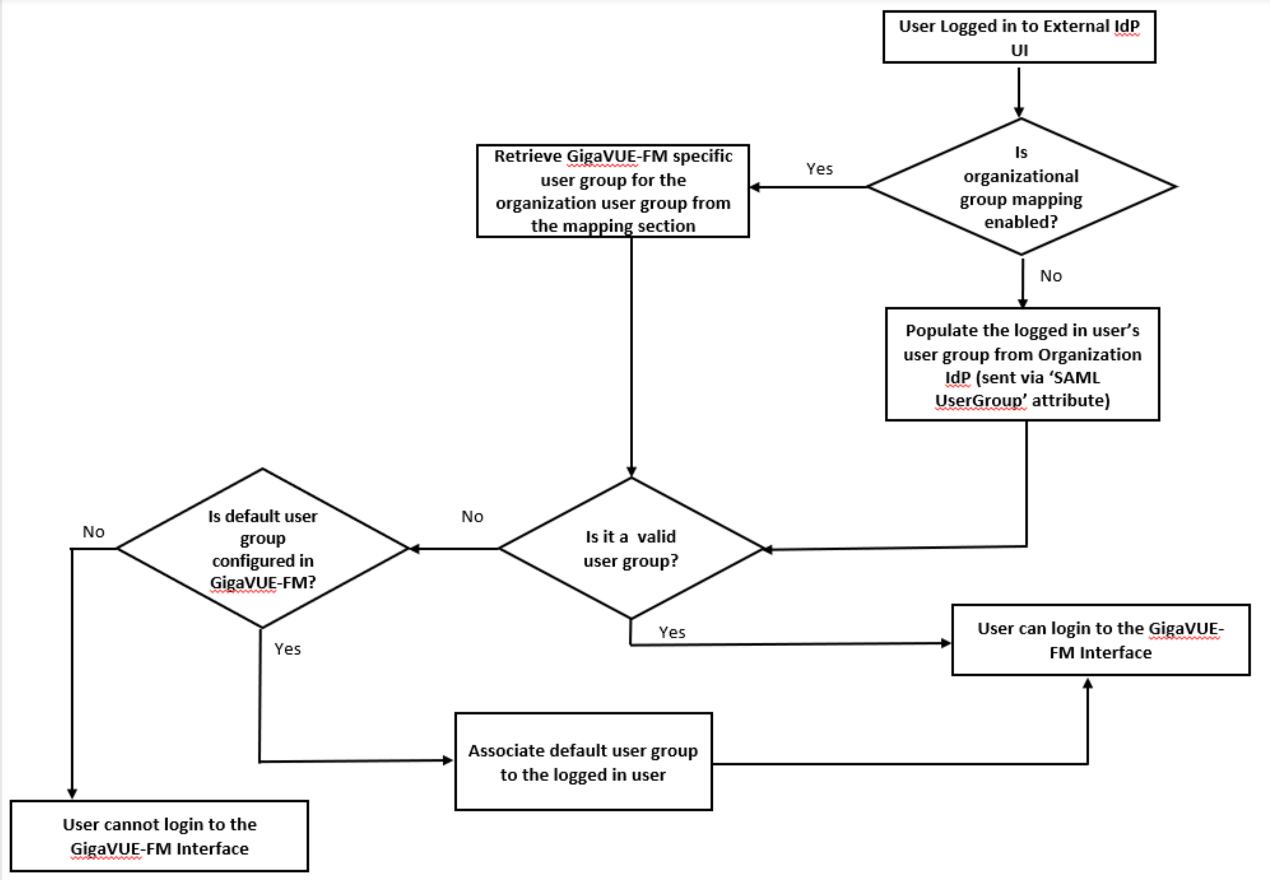
1. GigaVUE-FM sends a request to external organization IdP for authentication and authorization.

> **NOTE:** ADFS is the only qualified external IdP.

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:


User Logged in to External IdP UI
Is organizational group mapping enabled?
Yes
Retrieve GigaVUE-FM specific user group for the organization user group from the mapping section
No
Populate the logged in user's user group from Organization IdP (sent via 'SAML UserGroup' attribute)
Is it a valid user group?
No
Is default user group configured in GigaVUE-FM?
No
Yes
Yes
User can login to the GigaVUE-FM Interface
Associate default user group to the logged in user
User cannot login to the GigaVUE-FM Interface

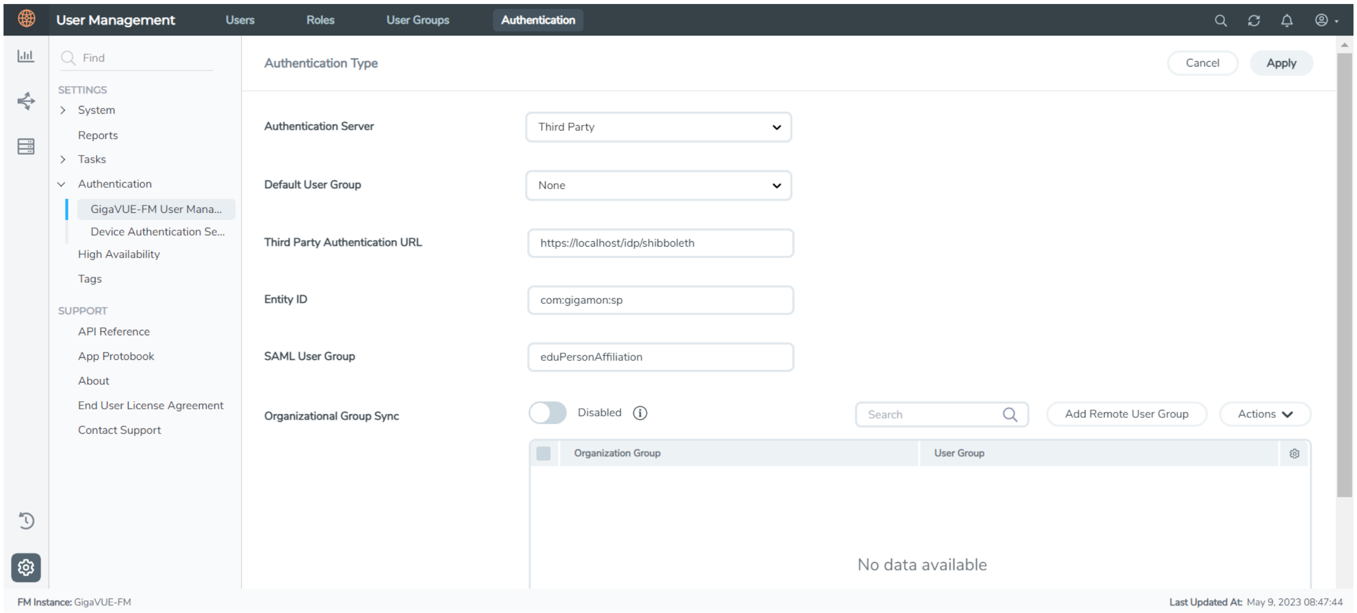
Refer to the **Authentication Type** for more details about the authentication types.

Configure External IdP in GigaVUE-FM

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. *Example:* For ADFS: https://<<ADFS_HOSTNAME>>/FederationMetadata/2007-06/FederationMetadata.xml
Entity ID	Service provider's entity ID (GigaVUE-FM). Fetch the Service Provider metadata (which is GigaVUE-FM’s metadata) from https://<FM IP Address>/saml/metadata.
SAML User Group	SAML User Group
Default User Group	Default User Group
Organizational Group Sync	Map the GigaVUE-FM group to the corresponding organizational groups in ADFS/OKTA/Microsoft Azure.



Authentication Type

Authentication Server: Third Party

Default User Group: None

Third Party Authentication URL: https://localhost/idp/shibboleth

Entity ID: com:gigamon:sp

SAML User Group: eduPersonAffiliation

Organizational Group Sync: Disabled

Organization Group	User Group

No data available

FM Instance: GigaVUE-FM

Last Updated At: May 9, 2023 08:47:44

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 6.3.00 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 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 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.

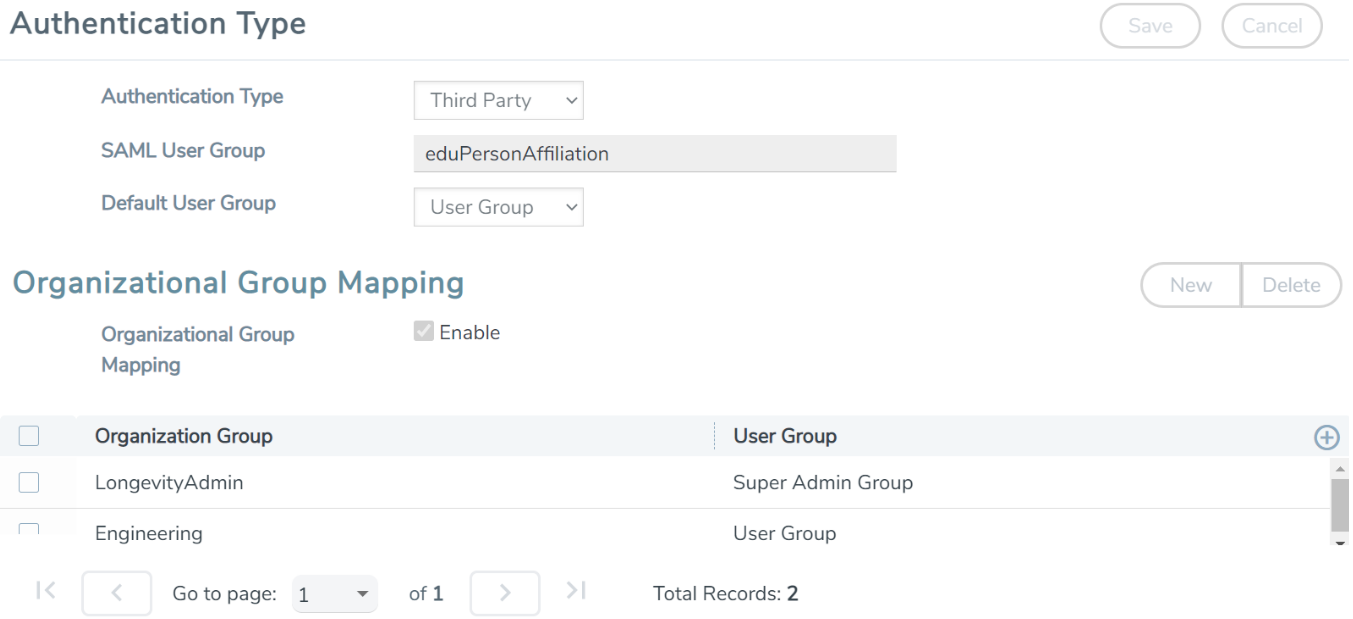
External IdP

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

Authentication Type	Third Party
SAML User Group	eduPersonAffiliation
Default User Group	User Group

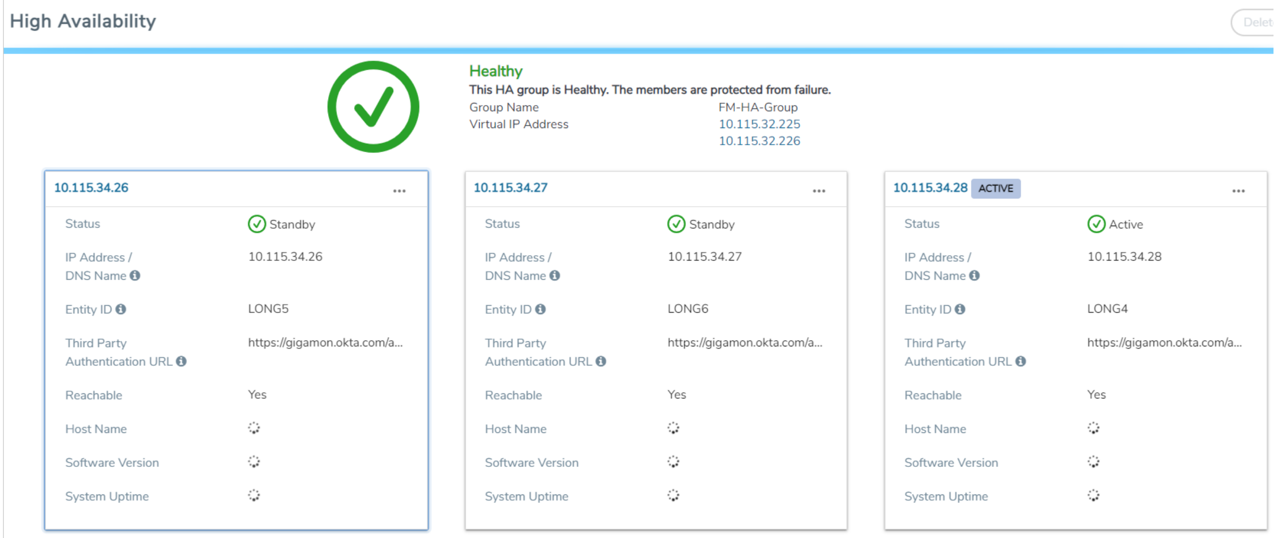
Organizational Group Mapping

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
   - Third Party Authentication URL



High Availability

Delet

Healthy

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

Group Name FM-HA-Group

Virtual IP Address 10.115.32.225
10.115.32.226

10.115.34.26 ...		10.115.34.27 ...		10.115.34.28 ACTIVE ...	
Status	Standby	Status	Standby	Status	Active
IP Address / DNS Name	10.115.34.26	IP Address / DNS Name	10.115.34.27	IP Address / DNS Name	10.115.34.28
Entity ID	LONG5	Entity ID	LONG6	Entity ID	LONG4
Third Party Authentication URL	https://gigamon.okta.com/a...	Third Party Authentication URL	https://gigamon.okta.com/a...	Third Party Authentication URL	https://gigamon.okta.com/a...
Reachable	Yes	Reachable	Yes	Reachable	Yes
Host Name		Host Name		Host Name	
Software Version		Software Version		Software Version	
System Uptime		System Uptime		System Uptime	

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.

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

RBAC 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.

> After the user logs in to GigaVUE-FM and has the required privileges to modify the configurations in GigaVUE-FM, the operations done by GigaVUE-FM uses the credentials that is provided while adding a node to GigaVUE-FM. Refer to Add New Physical Node or Cluster to GigaVUE-FM in the Fabric Management Guide.

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 FM security Management category.

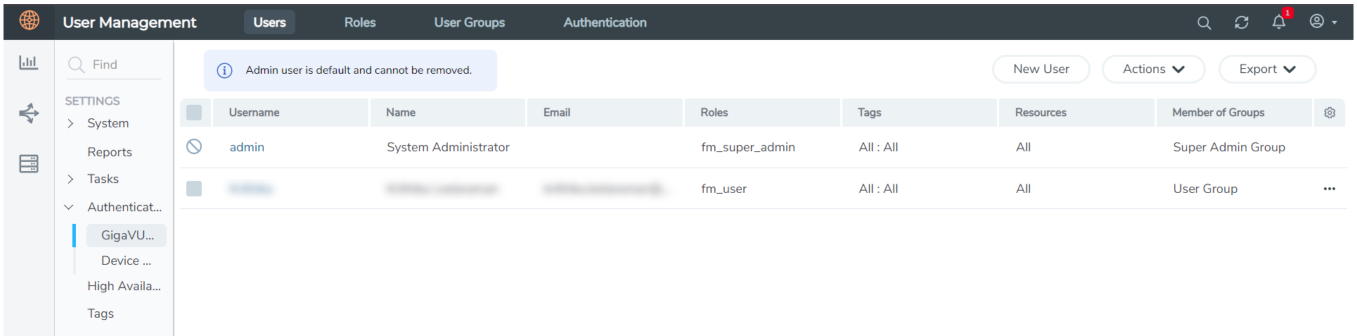
IMPORTANT: It is recommended to create users through GigaVUE-FM:

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

> **NOTE:** Monitor and operator users are not available in GigaVUE-FM. However, if you upgrade from a previous version in which monitor/operator users have been mapped in map default user, then after upgrade:
>
> - **In AAA:** Users authenticated through the external servers will be assigned the fm_user role.
> - **In LDAP:** Remote group based DN entry will not be migrated.

To add users perform the following steps:

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

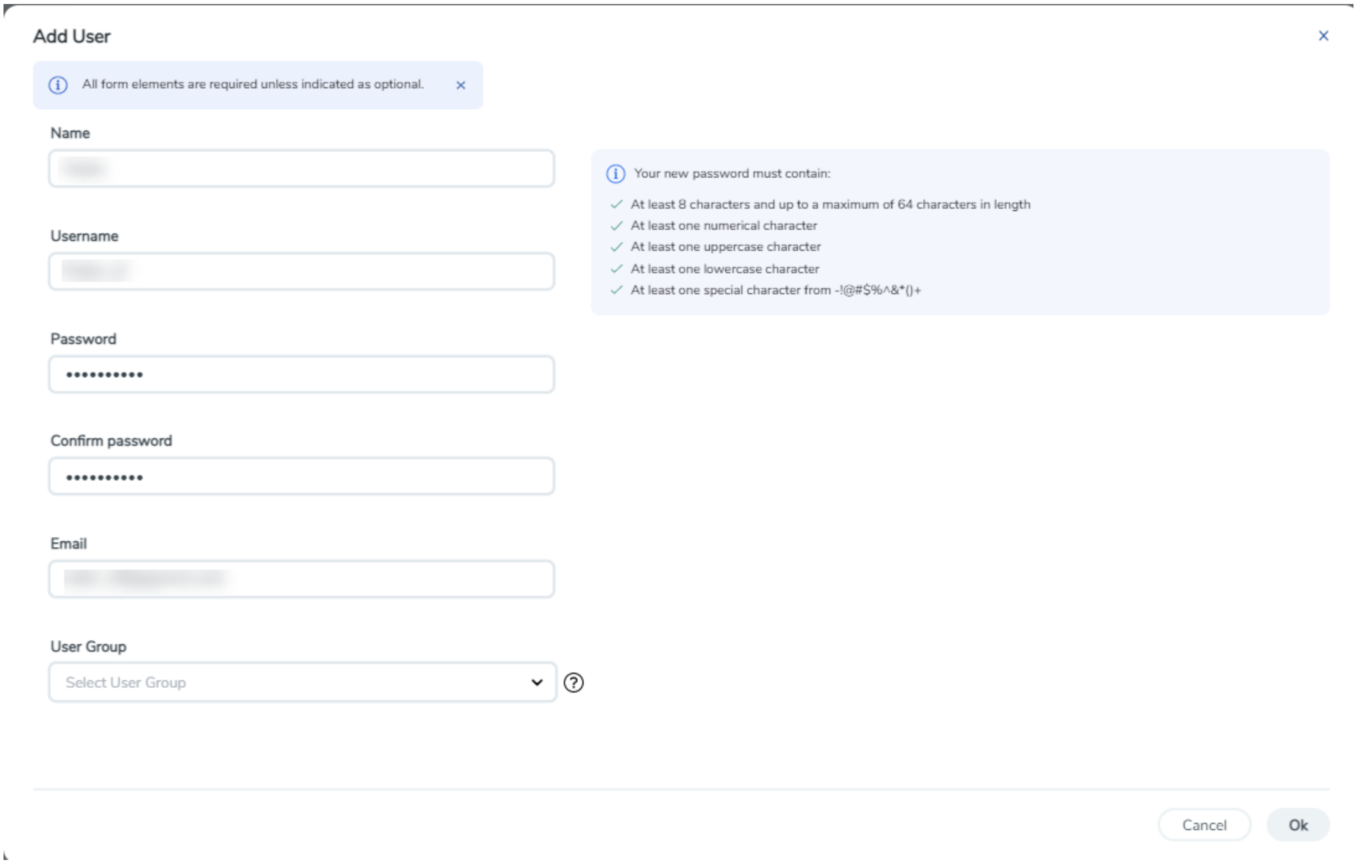
   

   Admin user is default and cannot be removed.

Username	Name	Email	Roles	Tags	Resources	Member of Groups
admin	System Administrator		fm_super_admin	All : All	All	Super Admin Group
[redacted]	[redacted]	[redacted]	fm_user	All : All	All	User Group

   Figure 11 *FM Users Page*

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


Add User

All form elements are required unless indicated as optional.

Name

Username

Password

••••••••••

Confirm password

••••••••••

Email

User Group

Select User Group

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 12 *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 FM security Management category, then click on the ellipsis to:

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

How to Unlock User Account

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

To unlock:

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

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

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.

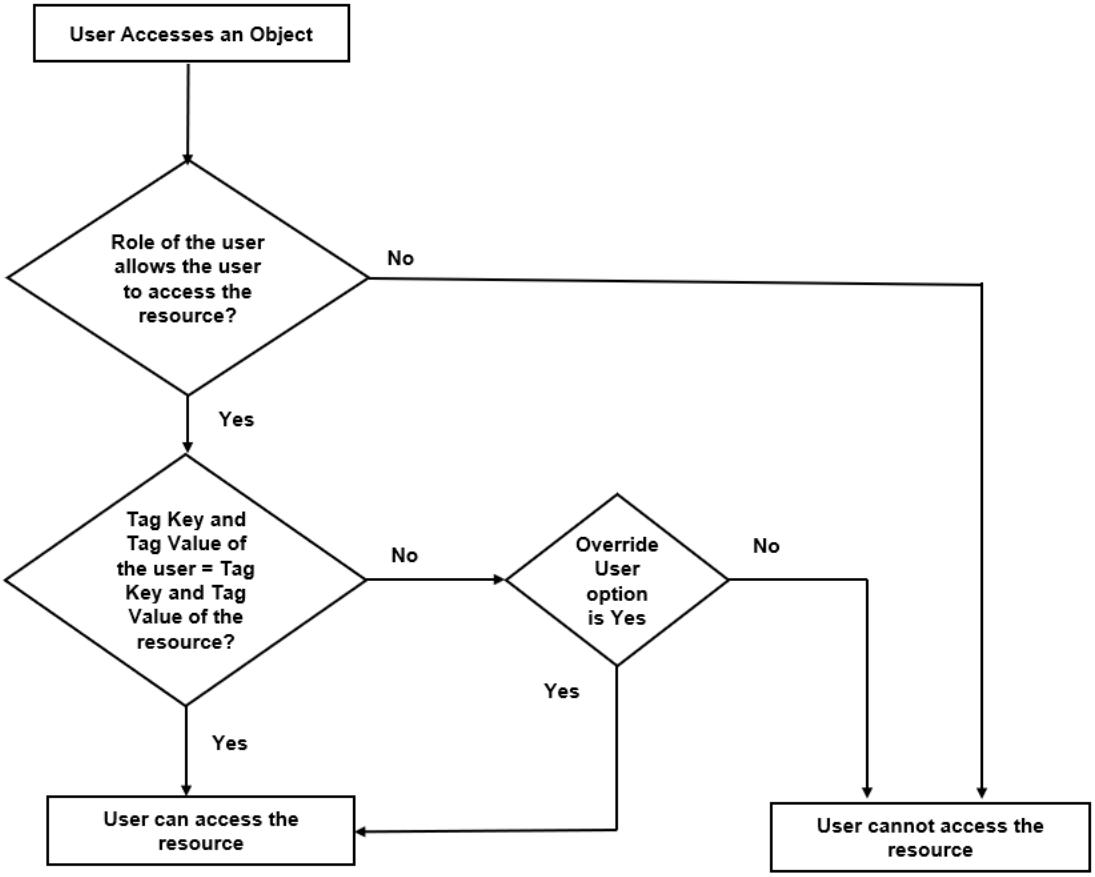
The following user groups are available by default in GigaVUE-FM. You will not be able to edit or change these groups in the system.

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:

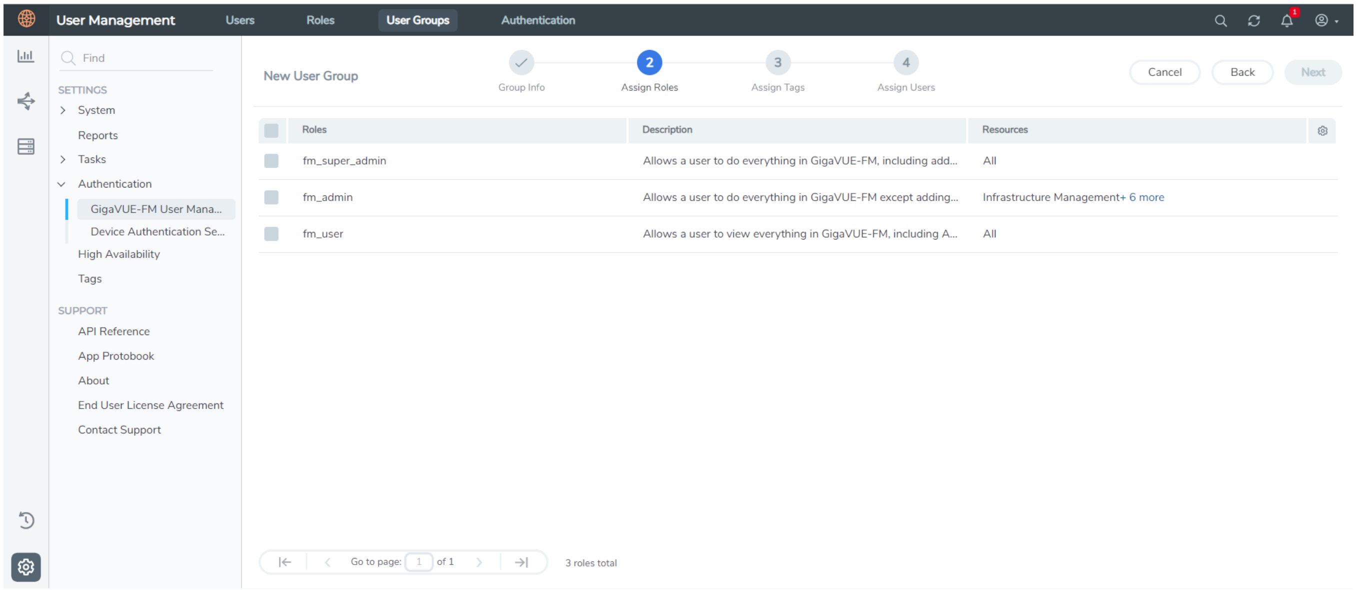
- The category of resources which the user can access, such as the clusters, ports, maps and so on. This is defined using the **Roles** option. Refer to the Roles section for more details.
- The physical and logical resources that the user can access, such as the ports in a cluster that belong to a specific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


User Accesses an Object
Role of the user allows the user to access the resource?
No
Yes
Tag Key and Tag Value of the user = Tag Key and Tag Value of the resource?
No
Override User option is Yes
No
Yes
Yes
User can access the resource
User cannot access the resource

To create a user group:

1. On the left navigation pane, click ⚙ , and then select **Authentication> GigaVUE-FMUser 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.



Roles	Description	Resources
fm_super_admin	Allows a user to do everything in GigaVUE-FM, including add...	All
fm_admin	Allows a user to do everything in GigaVUE-FM except adding...	Infrastructure Management+ 6 more
fm_user	Allows a user to view everything in GigaVUE-FM, including A...	All

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.

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 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 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.

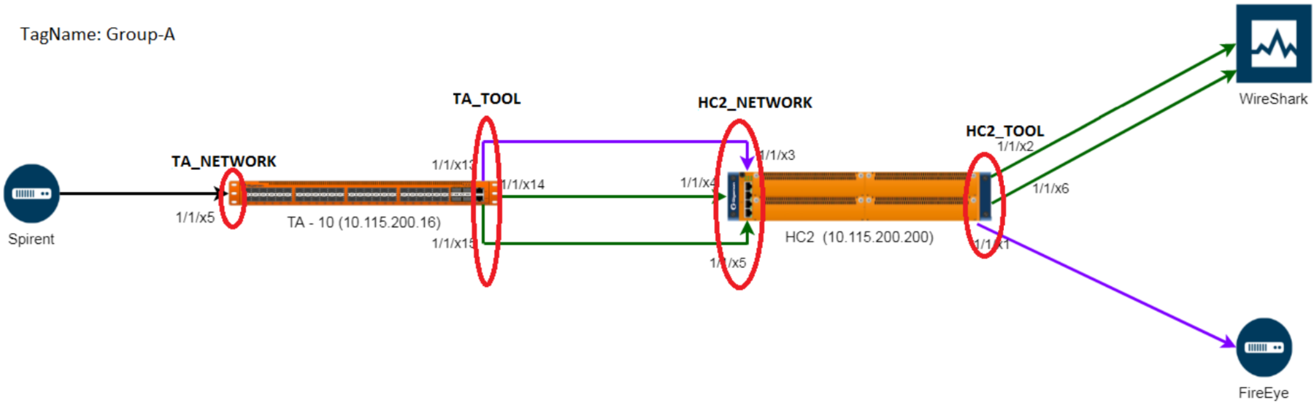
User	User Group	Role	Tag Key and Tag Value	Accessibility
User 3	View only user group	fm_user [Read access to all resources]	Tag Key = All Tag Value = All	The user • can only view all the resources. The role does not allow the user to add, edit or delete resources • cannot associate tag keys to the resources
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	HC2_NETWORK
1/1/X2, 1/1/x6, 1/1/x1	HC2_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 HC2_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:

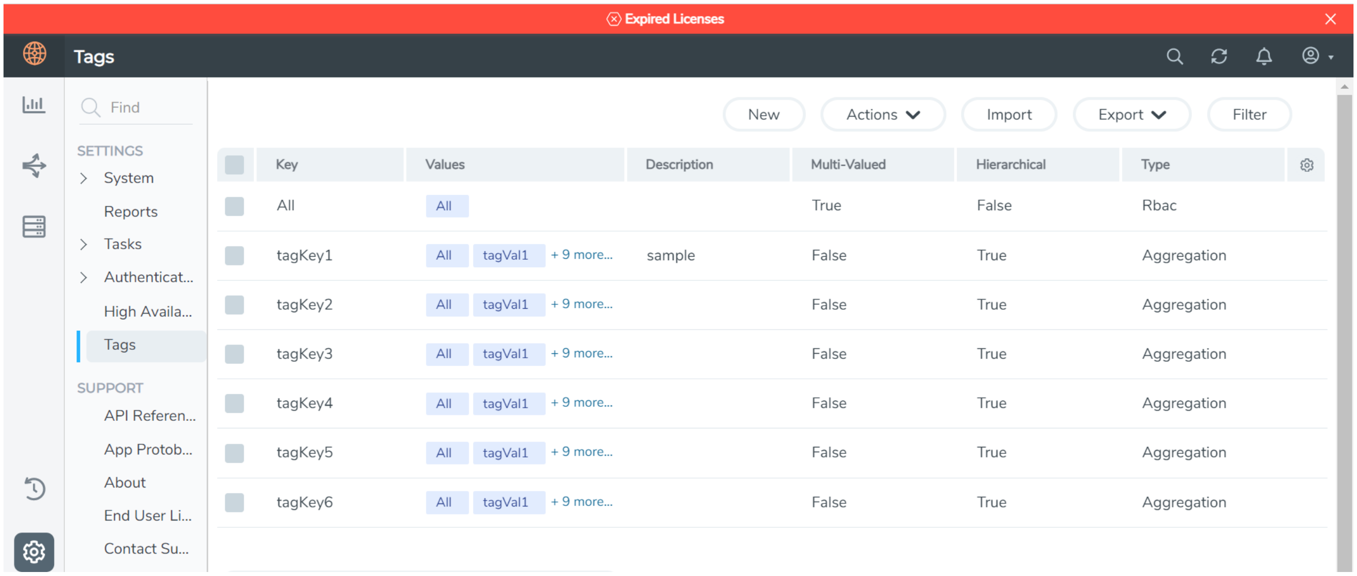
- Cluster
  - Device
    - Port

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

On the left navigation pane, click ,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.

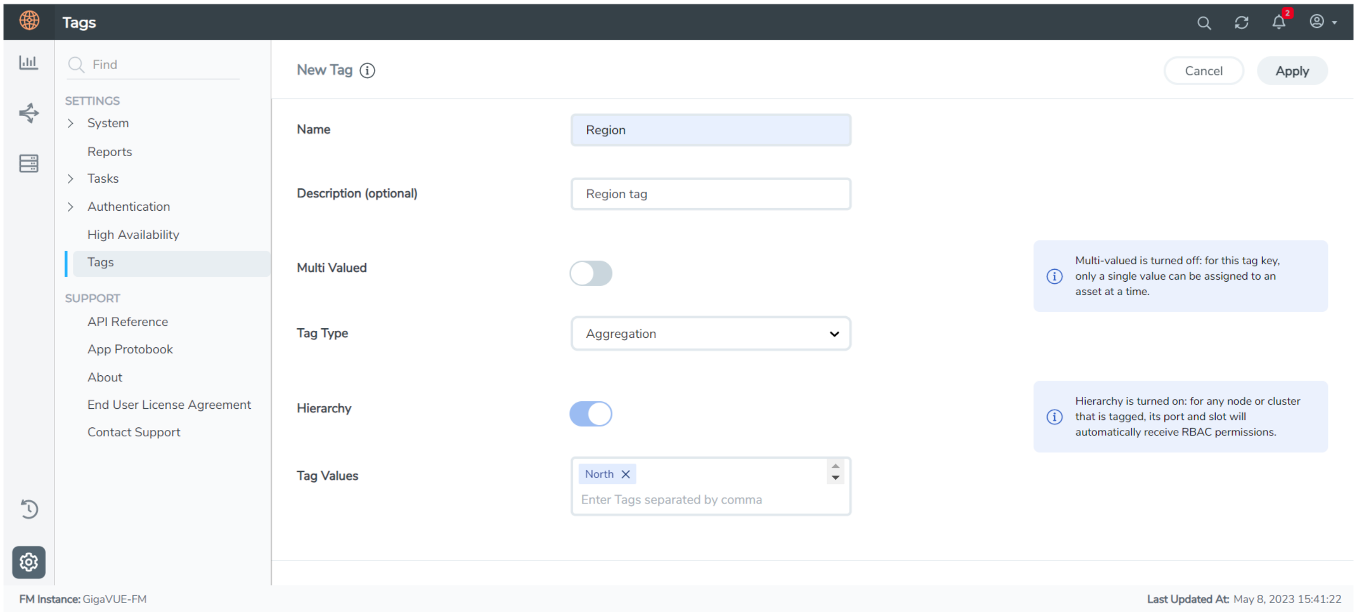
Create User-defined Tag

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

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

To create a tag:

1. On the left navigation pane, click ⚙ and select **Tags**.
2. In the Tag page, click **New**.



Name: Region

Description (optional): Region tag

Multi Valued: off

Multi-valued is turned off: for this tag key, only a single value can be assigned to an asset at a time.

Tag Type: Aggregation

Hierarchy: on

Hierarchy is turned on: for any node or cluster that is tagged, its port and slot will automatically receive RBAC permissions.

Tag Values: North
Enter Tags separated by comma

FM Instance: GigaVUE-FM

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.
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. Select **Physical** > **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**.

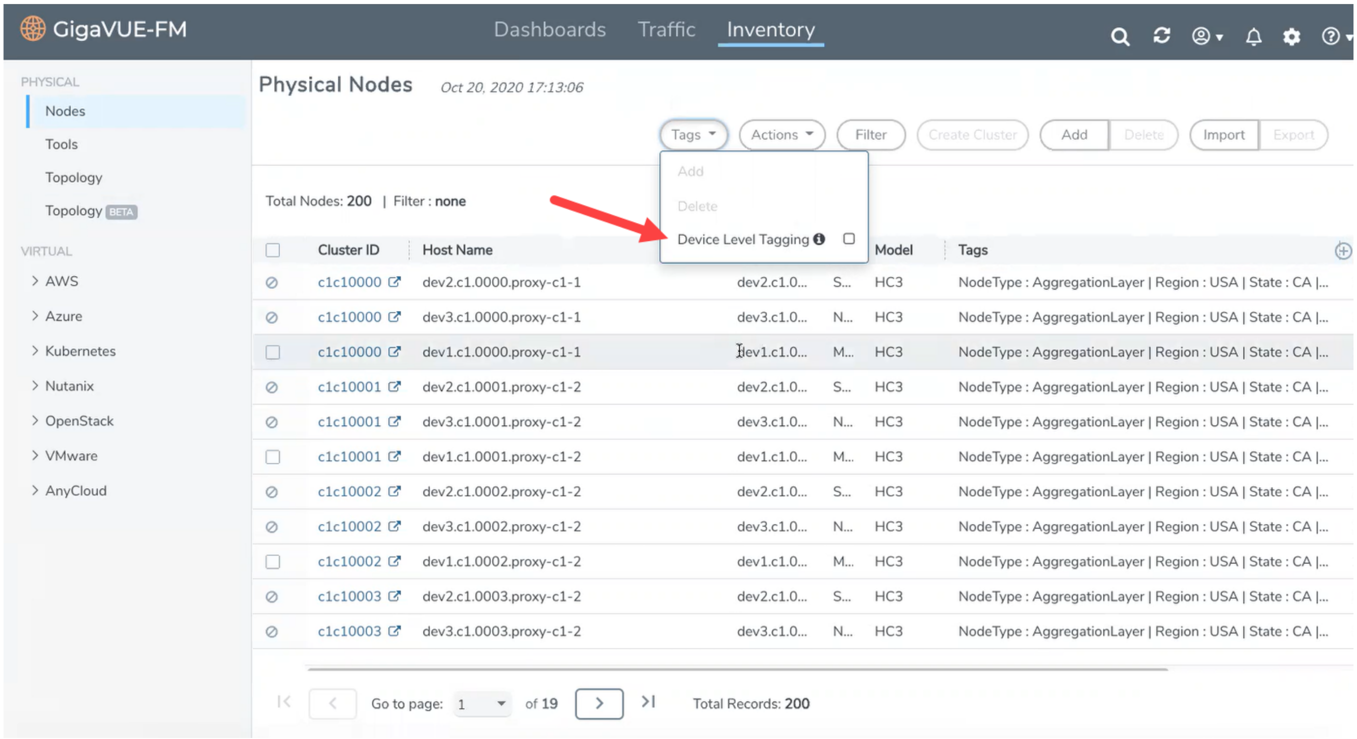
> **NOTE:** The Tag Keys and the Tag Values that are displayed depend on the role of the user.

4. Select the required **Tag Key** and **Tag Value** option in the top navigation bar and select **Add**.

Node Level Tagging

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

1. On the left navigation pane, click on ☰ go to **Physical** > **Nodes**.
2. Click on **Tags** and select **Device Level Tagging**.
3. Select the required nodes/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**.



Physical Nodes *Oct 20, 2020 17:13:06*

Total Nodes: **200** | Filter : **none**

☐	Cluster ID	Host Name			Model	Tags
⊘	c1c10000	dev2.c1.0000.proxy-c1-1	dev2.c1.0...	S...	HC3	NodeType : AggregationLayer | Region : USA | State : CA |...
⊘	c1c10000	dev3.c1.0000.proxy-c1-1	dev3.c1.0...	N...	HC3	NodeType : AggregationLayer | Region : USA | State : CA |...
☐	c1c10000	dev1.c1.0000.proxy-c1-1	dev1.c1.0...	M...	HC3	NodeType : AggregationLayer | Region : USA | State : CA |...
⊘	c1c10001	dev2.c1.0001.proxy-c1-2	dev2.c1.0...	S...	HC3	NodeType : AggregationLayer | Region : USA | State : CA |...
⊘	c1c10001	dev3.c1.0001.proxy-c1-2	dev3.c1.0...	N...	HC3	NodeType : AggregationLayer | Region : USA | State : CA |...
☐	c1c10001	dev1.c1.0001.proxy-c1-2	dev1.c1.0...	M...	HC3	NodeType : AggregationLayer | Region : USA | State : CA |...
⊘	c1c10002	dev2.c1.0002.proxy-c1-2	dev2.c1.0...	S...	HC3	NodeType : AggregationLayer | Region : USA | State : CA |...
⊘	c1c10002	dev3.c1.0002.proxy-c1-2	dev3.c1.0...	N...	HC3	NodeType : AggregationLayer | Region : USA | State : CA |...
☐	c1c10002	dev1.c1.0002.proxy-c1-2	dev1.c1.0...	M...	HC3	NodeType : AggregationLayer | Region : USA | State : CA |...
⊘	c1c10003	dev2.c1.0003.proxy-c1-2	dev2.c1.0...	S...	HC3	NodeType : AggregationLayer | Region : USA | State : CA |...
⊘	c1c10003	dev3.c1.0003.proxy-c1-2	dev3.c1.0...	N...	HC3	NodeType : AggregationLayer | Region : USA | State : CA |...

Go to page: 1 of 19 Total Records: 200

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

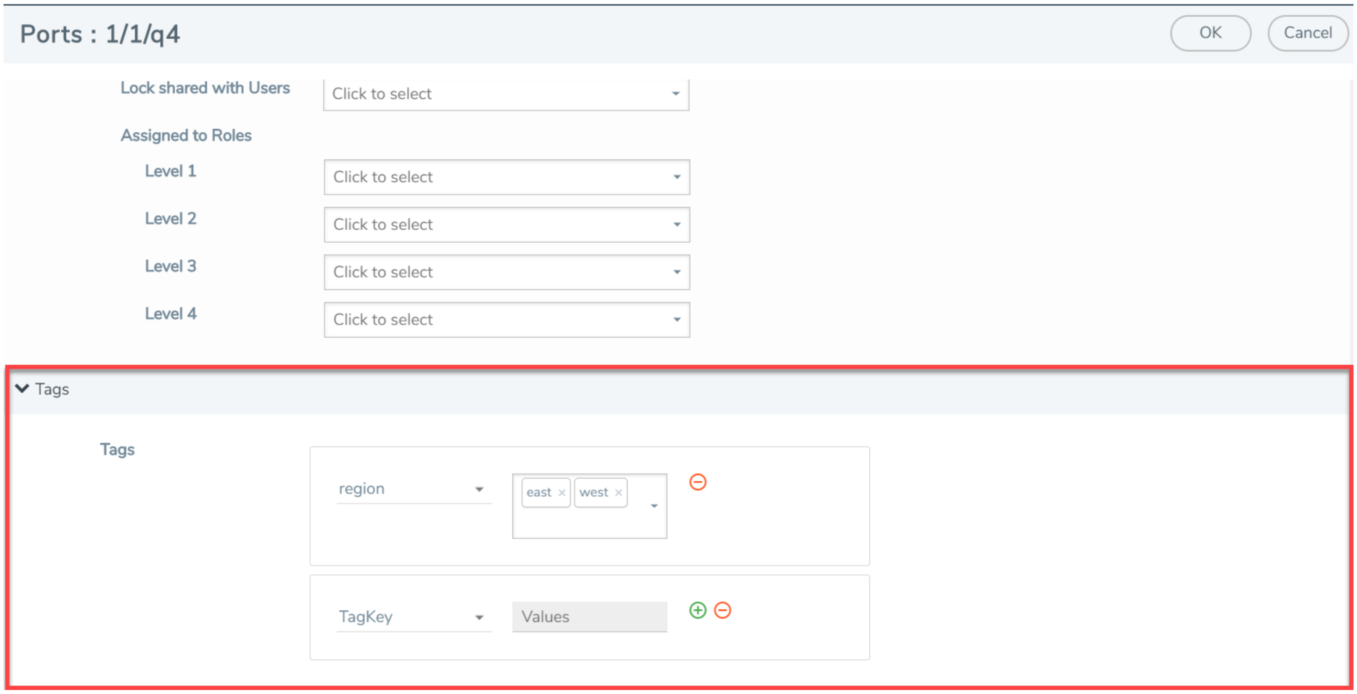
Tagging Ports

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. Go to **Ports** > **All Ports**.

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

2. Select the port for which you need to associate tags.
3. Click **Edit**.
4. Scroll down to the **Tags** option.
5. Select the required **Tag ID**s and **Tag Values** that must be associated to the ports.



Ports : 1/1/q4

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**.

> **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. Go to **Ports** > **All Ports**.
2. Select the port for which you need to remove the tags.
3. Click **Edit**.
4. Scroll down to the **Tags** option.
5. Select the required **Tag ID**s and **Tag Values** that must be removed from the ports.

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 value 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. On the left navigation pane, click ⚙ 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. On the left navigation pane, click ⚙ and select **Tags**.
2. In the Tags page, click **Filter** to filter the tags. The Filter quick view is displayed. Refer to Figure 14 Tag Filters.

Figure 14 *Tag Filters*

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 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.
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. On the left navigation pane, click ⚙ 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.

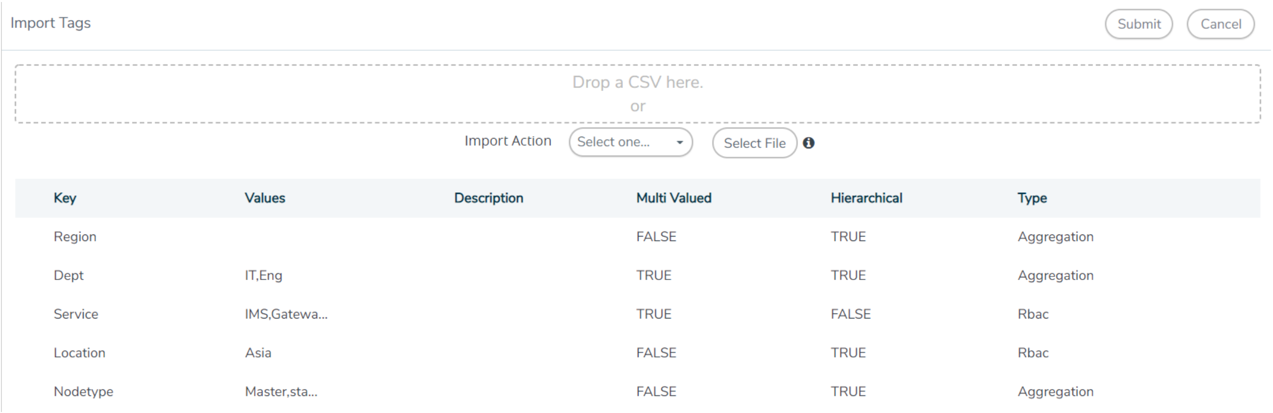
   > **NOTE:** Refer to table in the previous section to understand the conditions based on which the tags will be appended, deleted or replaced.

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

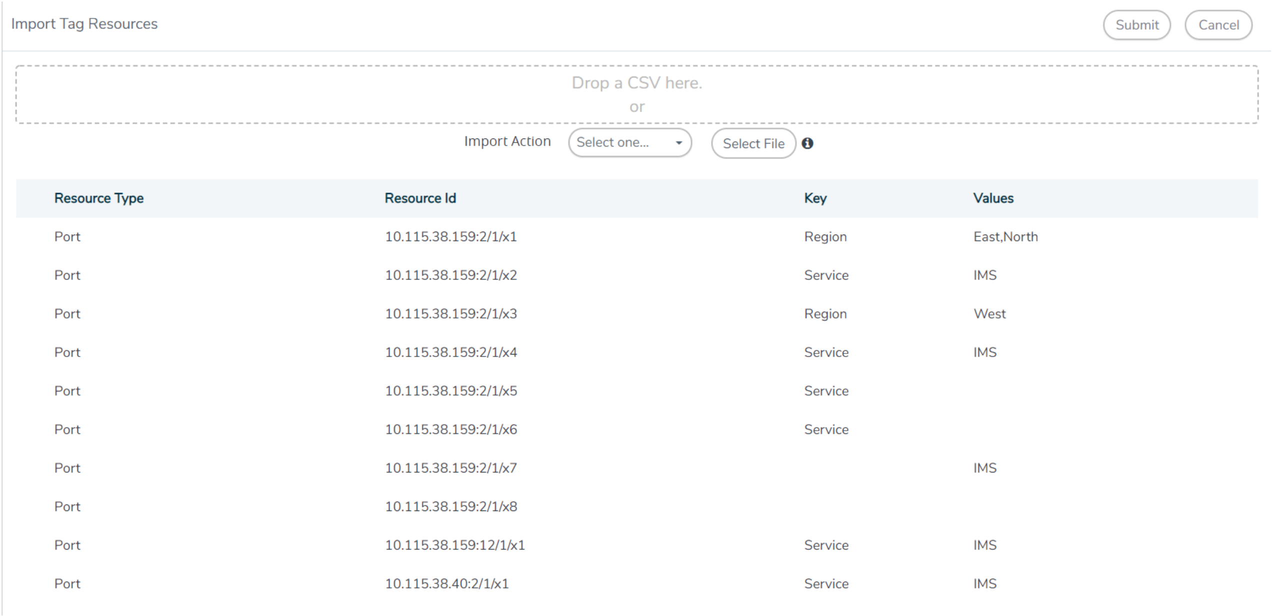
   See the following image:



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



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

5. Click **Done**. A pop-up appears in the bottom right corner of the page with the status.
6. 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

1. On the left navigation pane, click ⚙ and select **Tags**.
2. 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, click on 🗄 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's RBAC Persmissions
- Manage Alarms
- Manage Multiple Alarms
- Alarm Correlation
- Filter Alarms
- Alarms for Fabric Maps and Policies
- Alarms for GigaVUE-FM Configurations
- 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 gives 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.

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 reason 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, click on ☰ 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

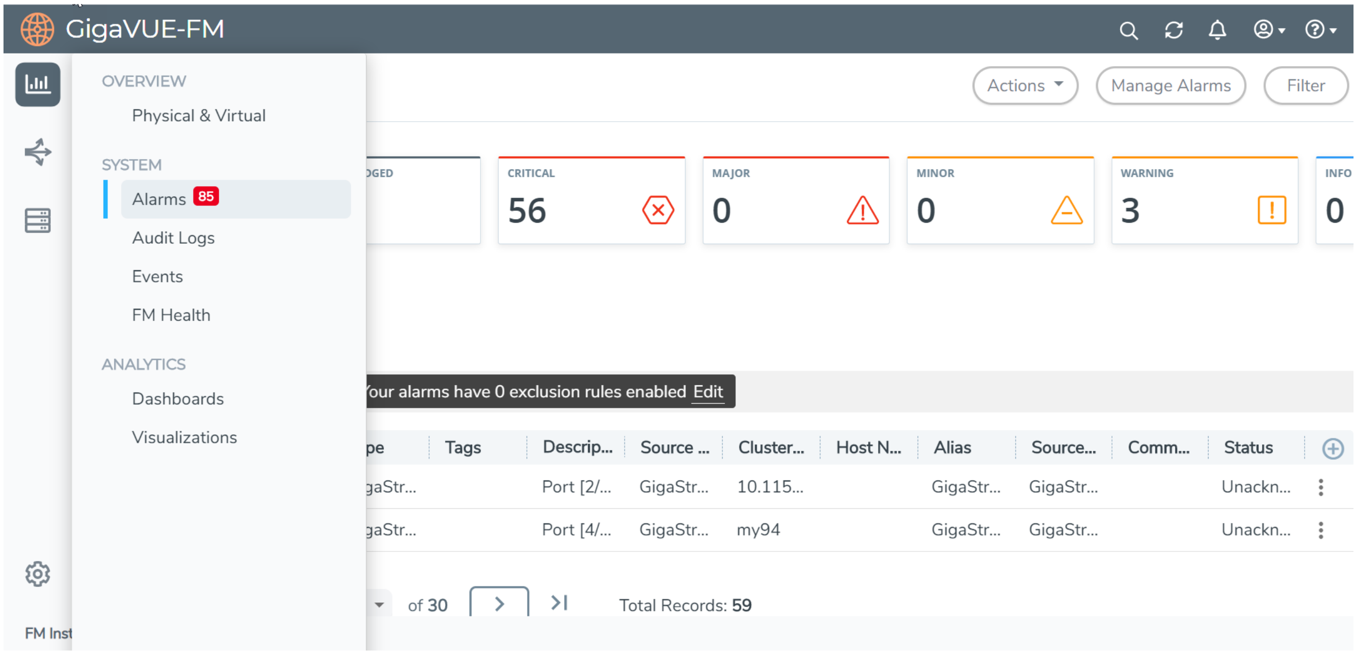
To view the alarms triggered in GigaVUE-FM:

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.



Your alarms have 0 exclusion rules enabled Edit

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

Figure 15 *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.

Permission Level	Description
	▪ Unacknowledged
Cluster ID	Cluster Id
Host Name	Host name
Alias	Alias name
Last Acknowleged By	User who acknowledged the alarm.
Acknowledged Time	Time the alarm was acknowledged.
Last unAcknowleged 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's RBAC Persmissions

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 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 Francisco

  If 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 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 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

You can acknowledge, unacknowledge and delete multiple alarms at a time. To acknowledge multiple alarms at a time:

1. Select the alarms that you want to acknowledge.
2. Click **Actions** > **Acknowledge**.

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

> **NOTE:** This option is available only for unacknowledged alarms.

You can also unacknowledge and delete alarms by selecting multiple alarms.

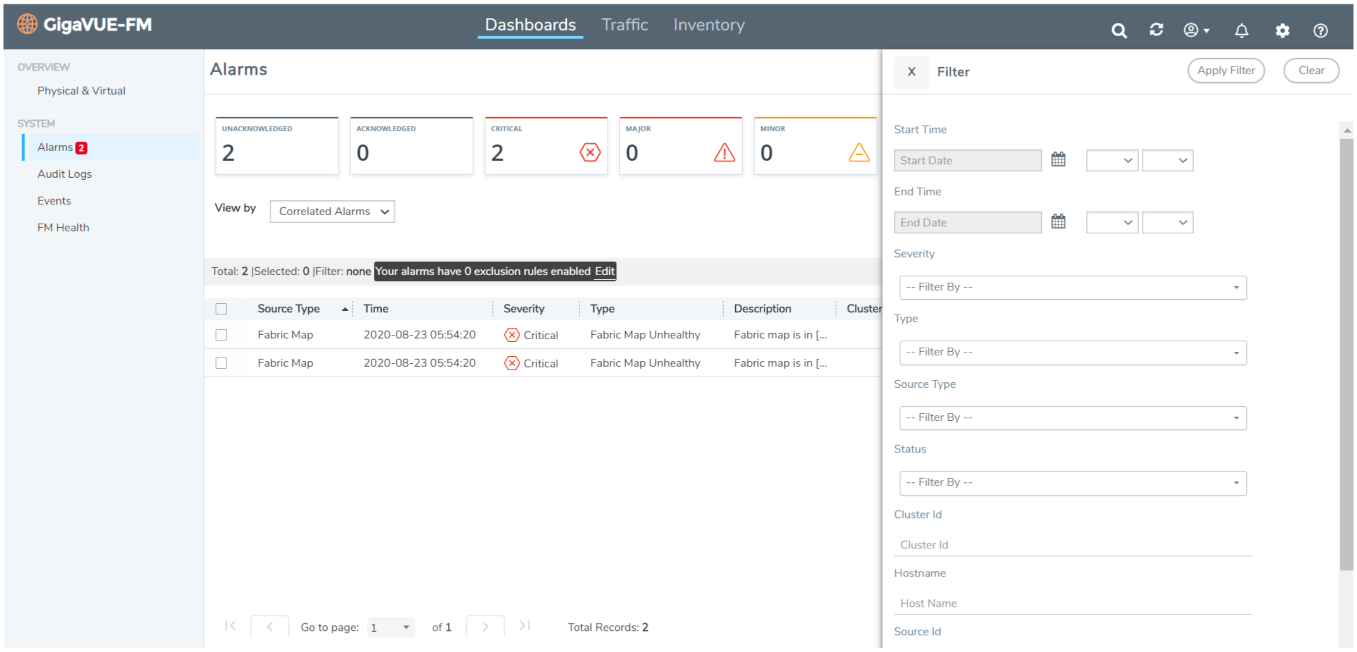
Filter Alarms

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.



UNACKNOWLEDGED	ACKNOWLEDGED	CRITICAL	MAJOR	MINOR
2	0	2	0	0

View by: Correlated Alarms

Total: 2 |Selected: 0 |Filter: none Your alarms have 0 exclusion rules enabled Edit

□	Source Type	Time	Severity	Type	Description	Cluster
□	Fabric Map	2020-08-23 05:54:20	⊗ Critical	Fabric Map Unhealthy	Fabric map is in [...	
□	Fabric Map	2020-08-23 05:54:20	⊗ Critical	Fabric Map Unhealthy	Fabric map is in [...	

Go to page: 1 of 1 Total Records: 2

Start Time: Start Date

End Time: End Date

Severity: -- Filter By --

Type: -- Filter By --

Source Type: -- Filter By --

Status: -- Filter By --

Cluster Id: Cluster Id

Hostname: Host Name

Source Id

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 Mapsand internal cluster maps are created using circuit ports, stack ports and other type of ports.

OrchestratedPolicies	Fabric Maps	Cluster LevelMaps	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.

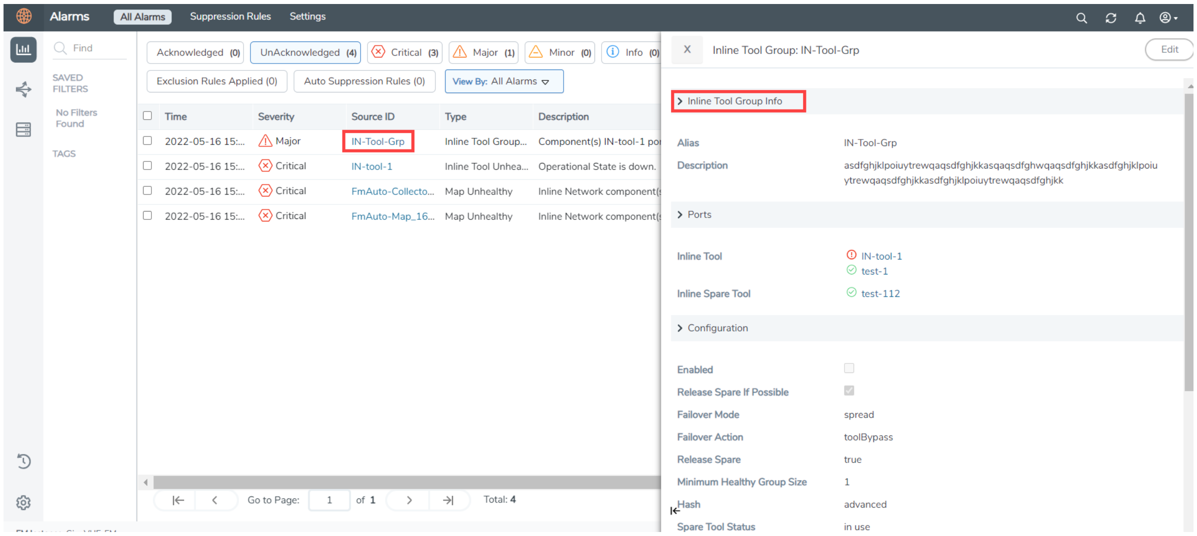
The source-ID field of the following alarm types are configured as hyperlinks which when clicked opens the quick view of the resource or navigates to the respective resource pages.

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.



☐	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(

Inline Tool Group: IN-Tool-Grp

Inline Tool Group Info

Alias	IN-Tool-Grp
Description	asdfghjklpoiuytrewqaqsdfghjkkasqaqsdfghwqaqsdfghjkkasdfghjklpoiuytrewqaqsdfghjkkasdfghjklpoiuytrewqaqsdfghjkk

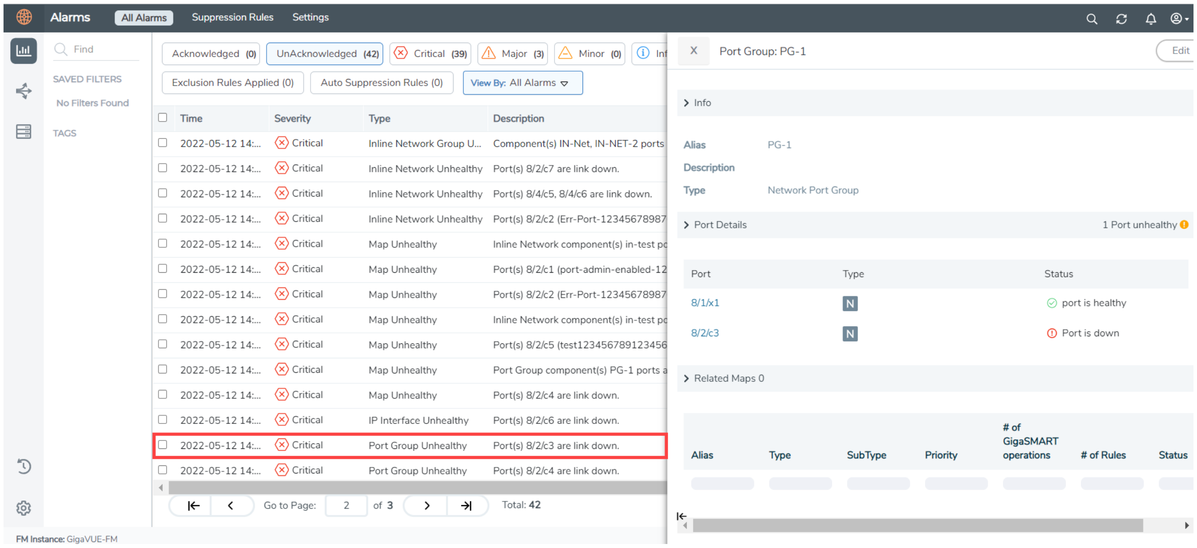
Ports

Inline Tool	IN-tool-1 test-1
Inline Spare Tool	test-112

Configuration

Enabled	☐
Release Spare If Possible	☑
Failover Mode	spread
Failover 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.



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.

Go to Page: 2 of 3 Total: 42

FM Instance: GigaVUE-FM

Port Group: PG-1

Info

Alias PG-1
Description
Type Network Port Group

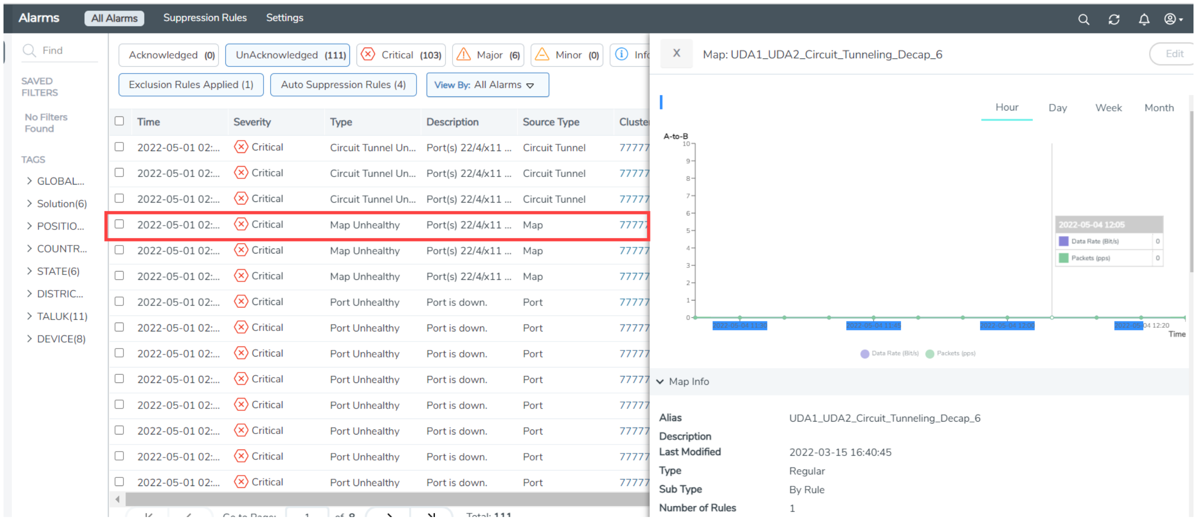
Port Details 1 Port unhealthy

Port	Type	Status
8/1/x1	N	port is healthy
8/2/c3	N	Port is down

Related Maps 0

Alias	Type	SubType	Priority	# of GigaSMART operations	# of Rules	Status

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



Time	Severity	Type	Description	Source Type	Cluste
2022-05-01 02:...	Critical	Circuit Tunnel Un...	Port(s) 22/4/x11 ...	Circuit Tunnel	77777
2022-05-01 02:...	Critical	Circuit Tunnel Un...	Port(s) 22/4/x11 ...	Circuit Tunnel	77777
2022-05-01 02:...	Critical	Circuit Tunnel Un...	Port(s) 22/4/x11 ...	Circuit Tunnel	77777
2022-05-01 02:...	Critical	Map Unhealthy	Port(s) 22/4/x11 ...	Map	77777
2022-05-01 02:...	Critical	Map Unhealthy	Port(s) 22/4/x11 ...	Map	77777
2022-05-01 02:...	Critical	Map Unhealthy	Port(s) 22/4/x11 ...	Map	77777
2022-05-01 02:...	Critical	Port Unhealthy	Port is down.	Port	77777
2022-05-01 02:...	Critical	Port Unhealthy	Port is down.	Port	77777
2022-05-01 02:...	Critical	Port Unhealthy	Port is down.	Port	77777
2022-05-01 02:...	Critical	Port Unhealthy	Port is down.	Port	77777
2022-05-01 02:...	Critical	Port Unhealthy	Port is down.	Port	77777
2022-05-01 02:...	Critical	Port Unhealthy	Port is down.	Port	77777
2022-05-01 02:...	Critical	Port Unhealthy	Port is down.	Port	77777
2022-05-01 02:...	Critical	Port Unhealthy	Port is down.	Port	77777

Go to Page: 1 of 8 Total: 111

Map: UDA1_UDA2_Circuit_Tunneling_Decap_6

Map Info

Alias UDA1_UDA2_Circuit_Tunneling_Decap_6
Description
Last Modified 2022-03-15 16:40:45
Type Regular
Sub Type By Rule
Number of Rules 1

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.

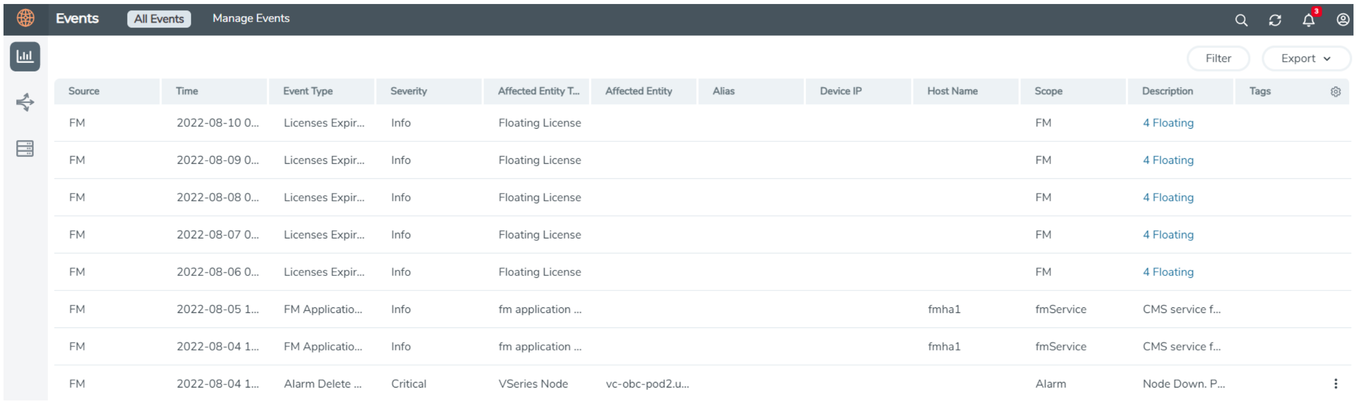
This chapter covers the following topics:

- Overview of Events
- View Events based on User's 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.



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 Fabric Manager. ▪ IP address - is the address of the GigaVUE HC Series or GigaVUE G Series node that detected the event. For a node to be able to send notifications to the Fabric Manager, the SNMP_TRAP must be configured with the Fabric Manager's IP address specified as a host. Refer to the GigaVUE-Administration Guide for instructions on adding a destination for SNMP traps. ▪ 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

Controls/ Parameters	Description
	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's 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 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 Francisco

  If 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:

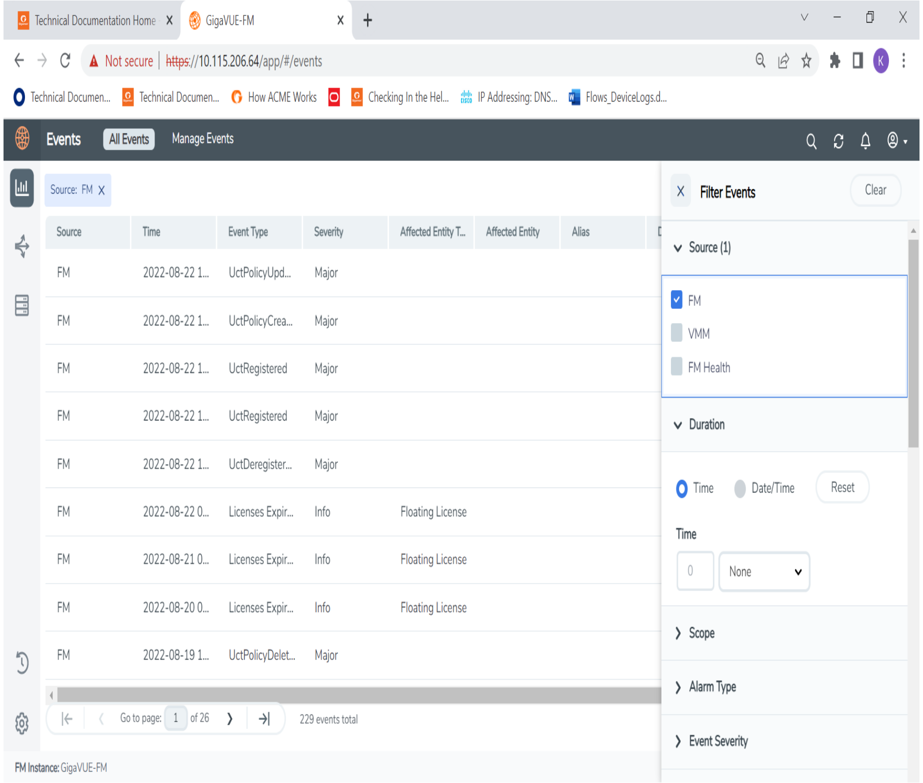
Controls/ Parameters	Description
Source	Displays the events generated by a specific source. **NOTE:** This option is not available in the Virtual Events page.
Duration	Displays the events occurred within a specific date range.
Scope	Displays the events associated with the selected category. For example, 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.

Controls/ Parameters	Description
	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.



Source	Time	Event Type	Severity	Affected Entity T...	Affected Entity	Alias
FM	2022-08-22 1...	UctPolicyUpd...	Major			
FM	2022-08-22 1...	UctPolicyCrea...	Major			
FM	2022-08-22 1...	UctRegistered	Major			
FM	2022-08-22 1...	UctRegistered	Major			
FM	2022-08-22 1...	UctDeregister...	Major			
FM	2022-08-22 0...	Licenses Expir...	Info	Floating License		
FM	2022-08-21 0...	Licenses Expir...	Info	Floating License		
FM	2022-08-20 0...	Licenses Expir...	Info	Floating License		
FM	2022-08-19 1...	UctPolicyDelet...	Major			

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 Filter Audit Logs.

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.

Parameters	Description
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 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**.

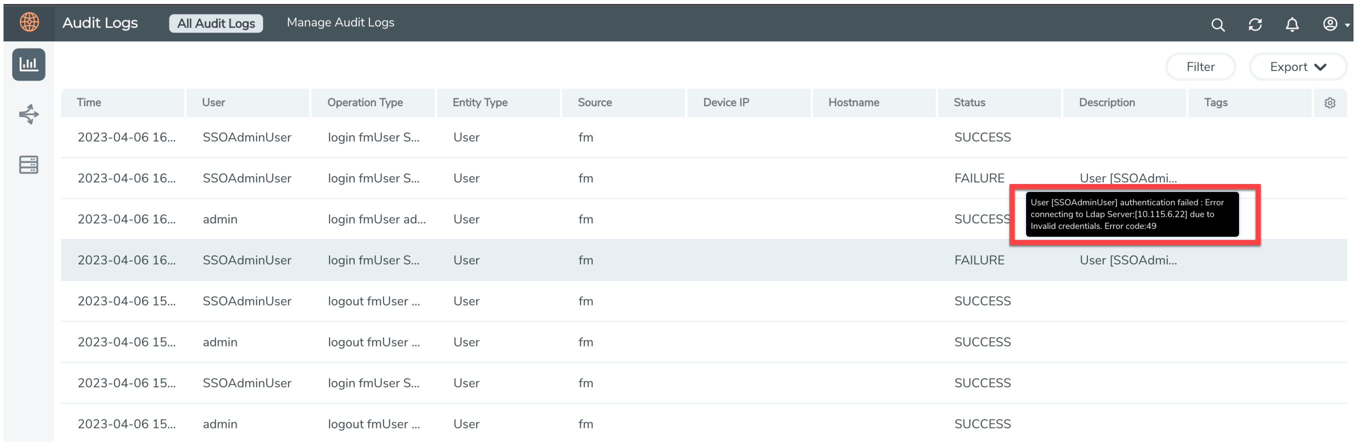
   The quick view for Audit Log Filters displays.
2. Specify any or all of the following:

- **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 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.



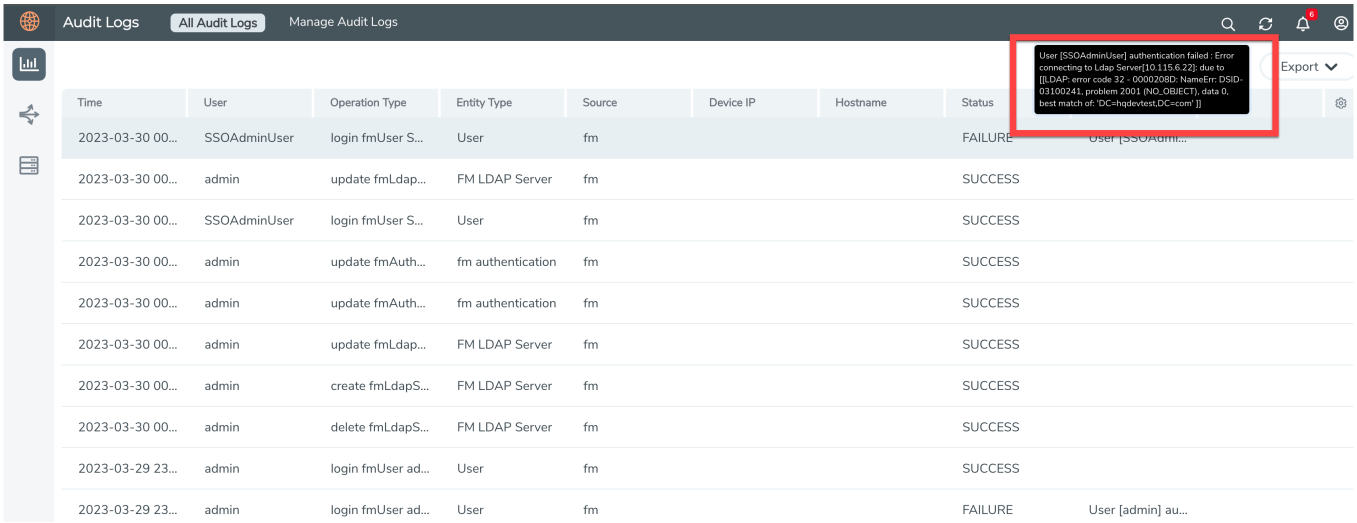
Time	User	Operation Type	Entity Type	Source	Device IP	Hostname	Status	Description	Tags
2023-04-06 16...	SSOAdminUser	login fmUser S...	User	fm			SUCCESS		
2023-04-06 16...	SSOAdminUser	login fmUser S...	User	fm			FAILURE	User [SSOAdmi...	
2023-04-06 16...	admin	login fmUser ad...	User	fm			SUCCESS		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

User [SSOAdminUser] authentication failed : Error connecting to Ldap Server:[10.115.6.22] due to Invalid credentials. Error code:49

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’]



User [SSOAdminUser] authentication failed : Error connecting to Ldap Server[10.115.6.22]: due to [[LDAP: error code 32 - 0000208D: NameErr: DSID-03100241, problem 2001 (NO_OBJECT), data 0, best match of: 'DC=hqdevtest,DC=com']]

Time	User	Operation Type	Entity Type	Source	Device IP	Hostname	Status	
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

LDAP Status Code	Meaning	Exception or Action
		"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
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

LDAP Status Code	Meaning	Exception or Action
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.

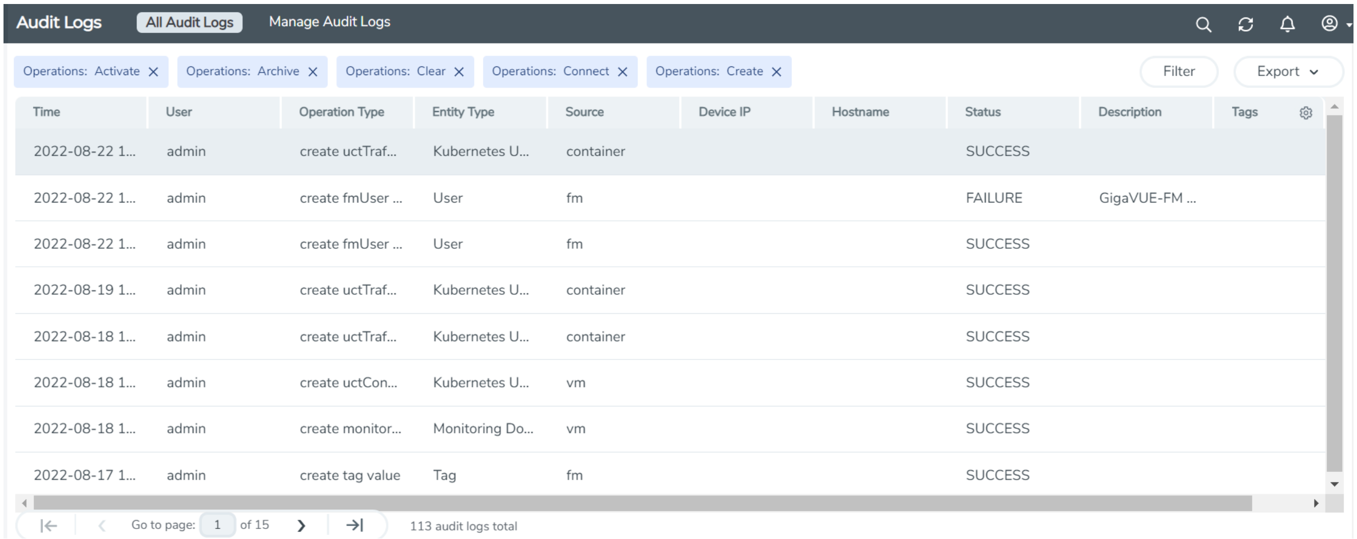
The records are archived as a CSV file with a timestamp appended. For example, audit_20151005105607.csv. The file is compressed to a zip file before exporting to the server.

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.



Operations: Activate ✕ Operations: Archive ✕ Operations: Clear ✕ Operations: Connect ✕ Operations: Create ✕

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 Audit Log Records

Audit log records can be purged by performing the following:

1. Select **Audit Logs** in the navigation pane.
2. Click **Manage Audit Logs**.
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 Audit Log Records

You can export the audit log records to an external server or download them as CSV or XLSX file.

To export the audit log records to an external server:

1. Select **Audit Logs** in the navigation pane.
2. Click **Export to Server**.
3. 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 the audit logs records as a CSV or XLSX file:

1. Select **Audit Logs** in the navigation pane.
2. Click **Export All** and specify the required format. The 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.

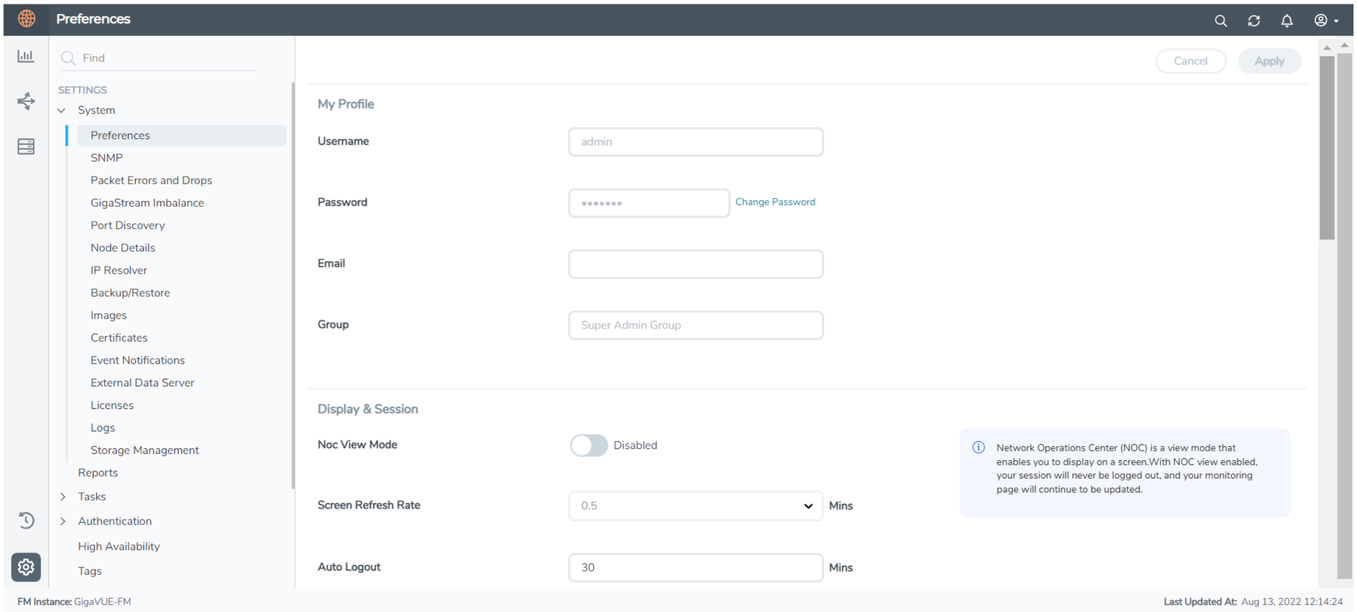
On the left navigation pane, click ⚙ and click **System**, to access the system pages.

System provides access to the following pages:

- Preferences
- SNMP Traps
- Port Packet Errors and Drops
- GigaStream Imbalance Notification
- Port Discovery
- Node Details
- IP Resolver
- Backup/Restore
- Images
- Certificates
- Event Notifications
- Export Data to External Data Server
- Licenses
- System Logs
- Storage Management

Preferences

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



My Profile

Username: admin

Password: •••••••

Email:

Group: Super Admin Group

Display & Session

Noc View Mode: Disabled

Network Operations Center (NOC) is a view mode that enables you to display on a screen.With NOC view enabled, your session will never be logged out, and your monitoring page will continue to be updated.

Screen Refresh Rate: 0.5 Mins

Auto Logout: 30 Mins

FM Instance: GigaVUE-FM

Last Updated At: Aug 13, 2022 12:14:24

Figure 16 *Preferences for GigaVUE-FM*

To change the GigaVUE-FM preferences:

On the left navigation pane, click 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.)
- Email
- Group

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 auto-logout time using the the **Auto-Logout (min)**[1] option. You can configure the auto-logout time to a minimum of 5 minutes and a maximum of 300 minutes. The auto-logout time becomes immediately effective.
- 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.

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

- 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”*.

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**: Events category based on which the events will be forwarded 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 FIPS 140-2 Compliance in GigaVUE-FM

Image Upgrade: For image upgrade, refer to Upgrade GigaVUE-FM from the UI

FIPS 140-2 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 is compliant with FIPS 140-2 Level 1 and was validated by the National Institute of Standards and Technology (NIST). The certificate number is 4066.

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.

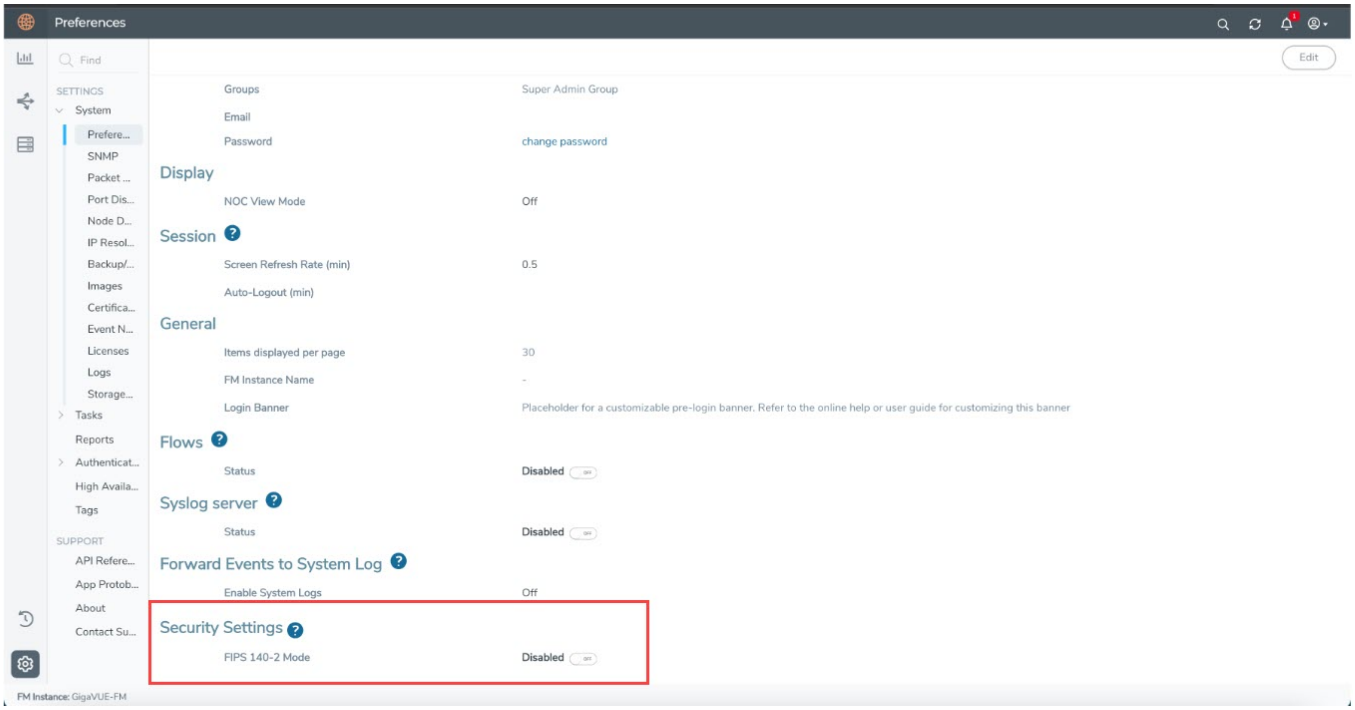
Configure FIPS in GigaVUE-FM

To configure FIPS in GigaVUE-FM:

1. On the left navigation pane, click ⚙ and go to **System** > **Preferences**.

2. Click **Edit**.
3. Under **Security Settings**, the **FIPS 140-2 Mode** option is available. Use the toggle button to enable FIPS.
4. GigaVUE-FM reboots after switching to FIPS mode. Clear the browser cache and cookies so that GigaVUE-FM IDP URL loads without any issues.

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



Groups Super Admin Group
Email
Password change password

Display

NOC View Mode Off

Session

Screen Refresh Rate (min) 0.5
Auto-Logout (min)

General

Items displayed per page 30
FM Instance Name -
Login Banner Placeholder for a customizable pre-login banner. Refer to the online help or user guide for customizing this banner

Flows

Status Disabled

Syslog server

Status Disabled

Forward Events to System Log

Enable System Logs Off

Security Settings

FIPS 140-2 Mode Disabled

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.

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?

The following software versions are validated for FIPS:

- 5.12.00.01
- 5.16.00, 6.0.00, 6.1.00, 6.2.00, 6.3.00

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 Traps

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

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

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 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:

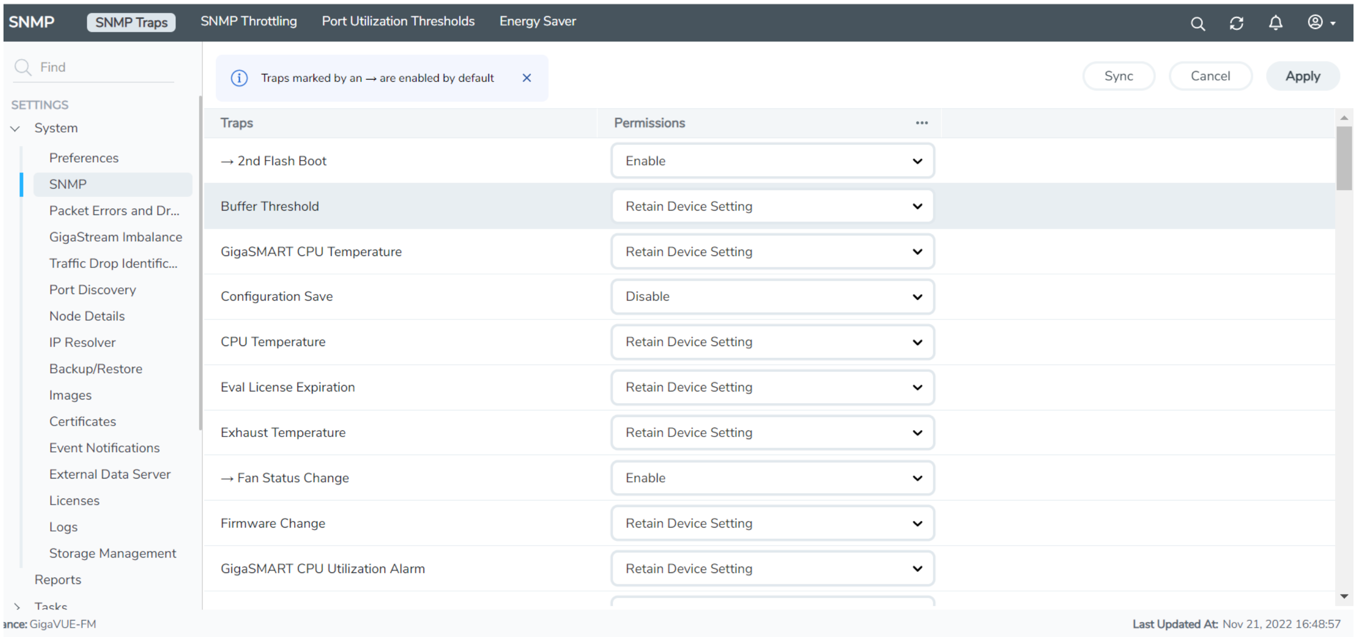
- If GigaVUE-FM receives any of the traffic health related traps mentioned above: Port state is set to yellow or red.
- If no further traps are received within the configured interval, which is 5 minutes: Port state is set to green.
    - For utilization thresholds, the health status will be reset as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

On the left navigation pane, click ⚙ to access SNMP Traps and select **System > SNMP Traps**.



Traps marked by an → are enabled by default

Traps	Permissions
→ 2nd Flash Boot	Enable
Buffer Threshold	Retain Device Setting
GigaSMART CPU Temperature	Retain Device Setting
Configuration Save	Disable
CPU Temperature	Retain Device Setting
Eval License Expiration	Retain Device Setting
Exhaust Temperature	Retain Device Setting
→ Fan Status Change	Enable
Firmware Change	Retain Device Setting
GigaSMART CPU Utilization Alarm	Retain Device Setting

ance: GigaVUE-FM

Last Updated At: Nov 21, 2022 16:48:57

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.

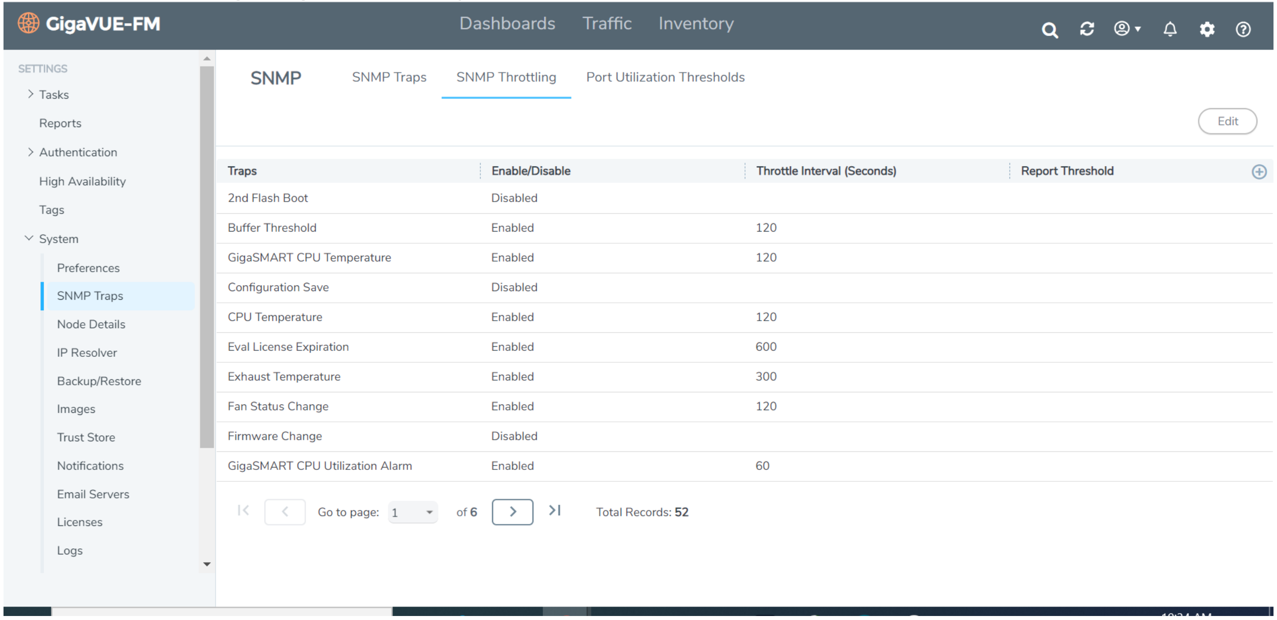
If a trap has been forcefully enabled/disabled on a device because of the global configuration setting, then an event is raised with the appropriate details in the Events page.

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.

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	

Go to page: 1 of 6 Total Records: 52

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:

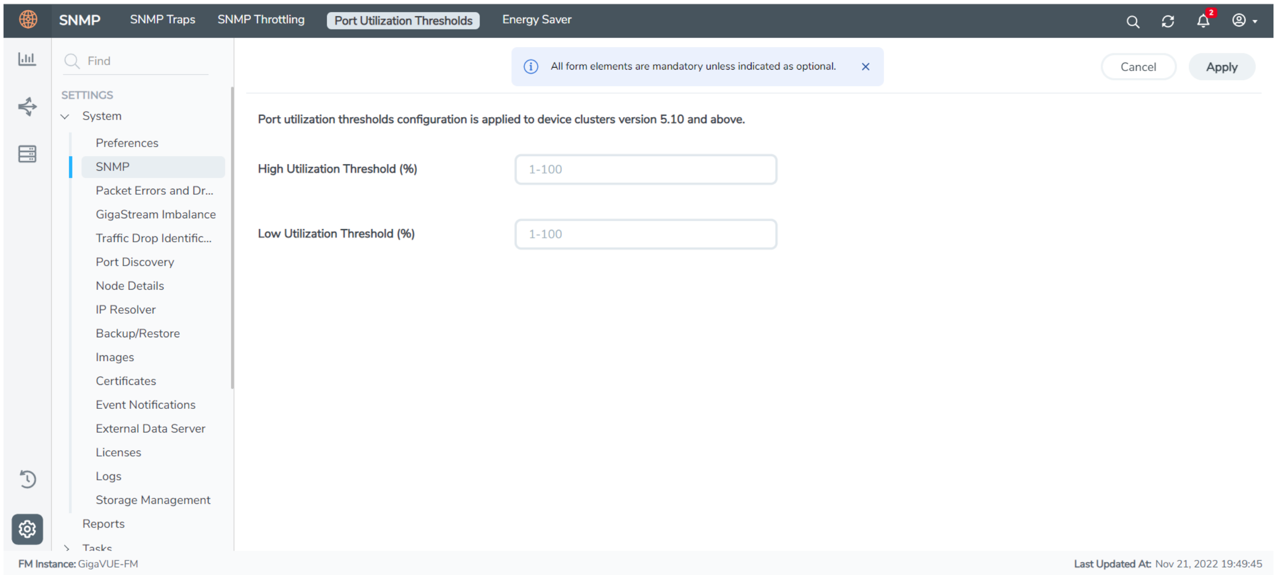
Throttle Level	GUI Screens	Count and Interval	Description
Cluster	GUI screens related to cluster	2 events per 5 second	Events to the particular cluster will be throttled
Summary	Dashboard, Physical nodes		Events across all the cluster will be throttled
Global	GUI screens related to solutions		Events 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. On the left navigation pane, click ⚙ and select **System > SNMP Traps** > **Port Utilization Threshold**.



All form elements are mandatory unless indicated as optional.

Port utilization thresholds configuration is applied to device clusters version 5.10 and above.

High Utilization Threshold (%) 1-100

Low Utilization Threshold (%) 1-100

FM Instance: GigaVUE-FM

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.

Port Packet Errors and Drops

GigaVUE HC series and 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.

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

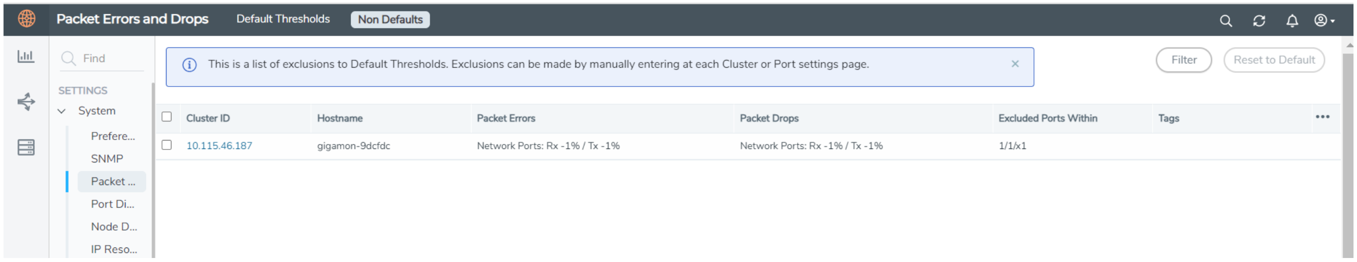
You can configure the port packet drop/error threshold globally for all the devices managed by GigaVUE-FM. To configure the port packet drop/error in GigaVUE-FM:

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

Field	Description
Port Type	Port type for which the threshold is to be configured. Configuration for *All Ports* will be applied to all the ports (this is equivalent to the global level in device CLI).
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.

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.



This is a list of exclusions to Default Thresholds. Exclusions can be made by manually entering at each Cluster or Port settings page.

☐	Cluster ID	Hostname	Packet Errors	Packet Drops	Excluded Ports Within	Tags
☐	10.115.46.187	gigamon-9dcfdc	Network Ports: Rx -1% / Tx -1%	Network Ports: Rx -1% / Tx -1%	1/1/x1	

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 Threshold in Devices
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	GigaStream Imbalance trap is triggered in the device and sent to GigaVUE-FM and the corresponding

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

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.

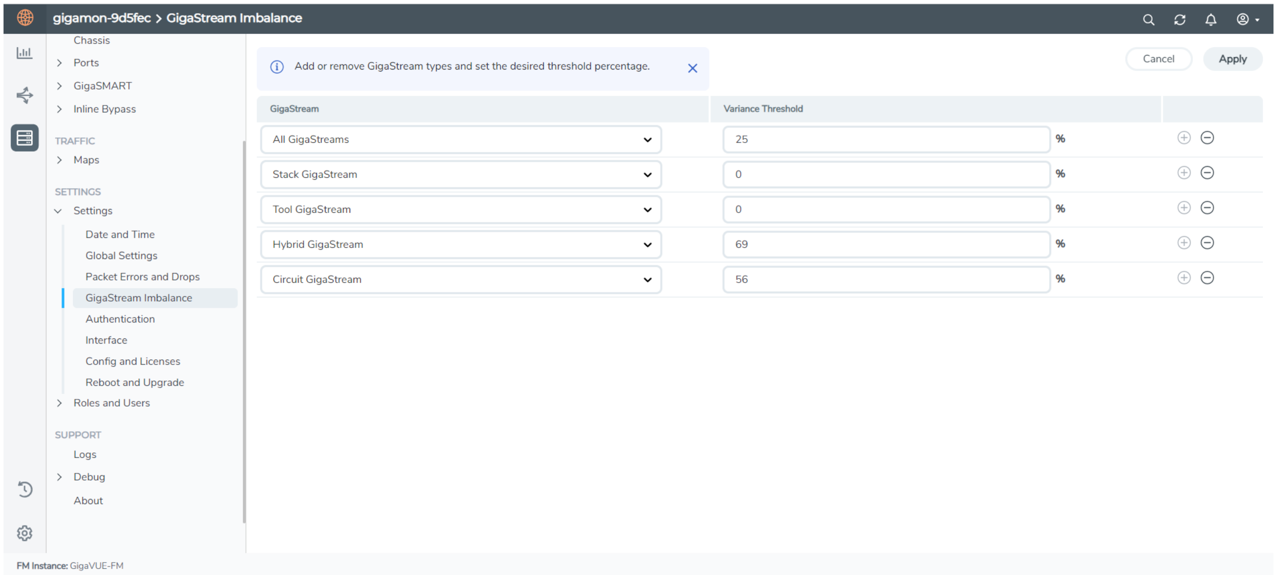
- Supported polling interval is 30s only.

Configure GigaStream Imbalance Threshold in Devices

To configure GigaStream Imbalance threshold through the device settings page:

1. On the left navigation pane, click on 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 *All GigaStreams* 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.



Add or remove GigaStream types and set the desired threshold percentage.

GigaStream	Variance Threshold
All GigaStreams	25 %
Stack GigaStream	0 %
Tool GigaStream	0 %
Hybrid GigaStream	69 %
Circuit GigaStream	56 %

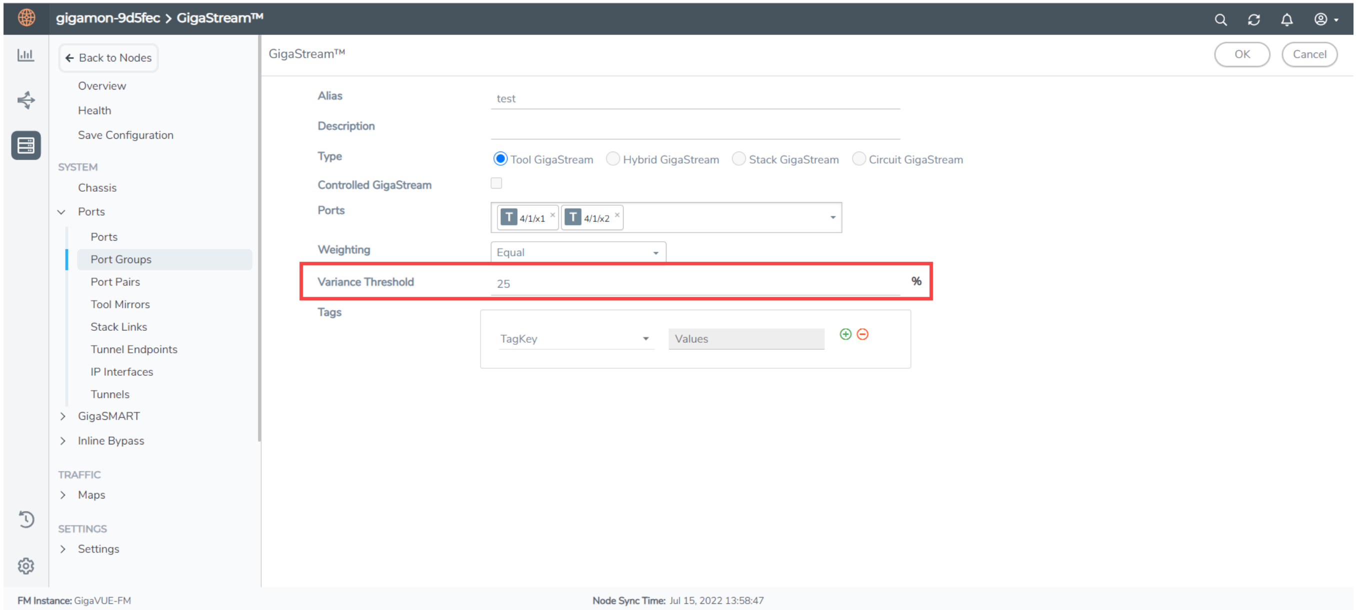
4. Click **Save** and **Apply** to save and apply the configuration.

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



Alias: test

Description:

Type: ● Tool GigaStream ○ Hybrid GigaStream ○ Stack GigaStream ○ Circuit GigaStream

Controlled GigaStream: □

Ports: T 4/1/x1 × T 4/1/x2 ×

Weighting: Equal

Variance Threshold: 25 %

Tags: TagKey Values

FM Instance: GigaVUE-FM

Node Sync Time: Jul 15, 2022 13:58:47

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

The configuration is applied to that specific GigaStream.

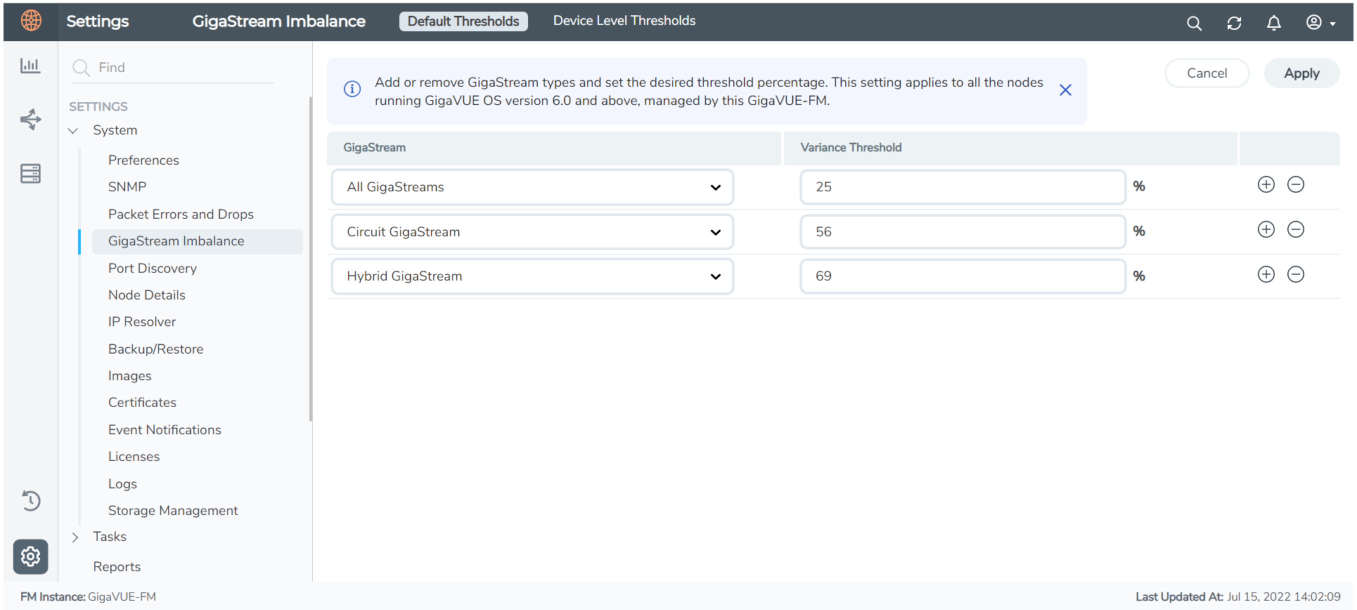
> **NOTE:** To configure the threshold values globally for all the devices managed by GigaVUE-FM refer to Configure GigaStream Imbalance Threshold in GigaVUE-FM.

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:

1. On the left navigation bar, click ⚙.

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



Add or remove GigaStream types and set the desired threshold percentage. This setting applies to all the nodes running GigaVUE OS version 6.0 and above, managed by this GigaVUE-FM.

GigaStream	Variance Threshold
All GigaStreams	25 %
Circuit GigaStream	56 %
Hybrid GigaStream	69 %

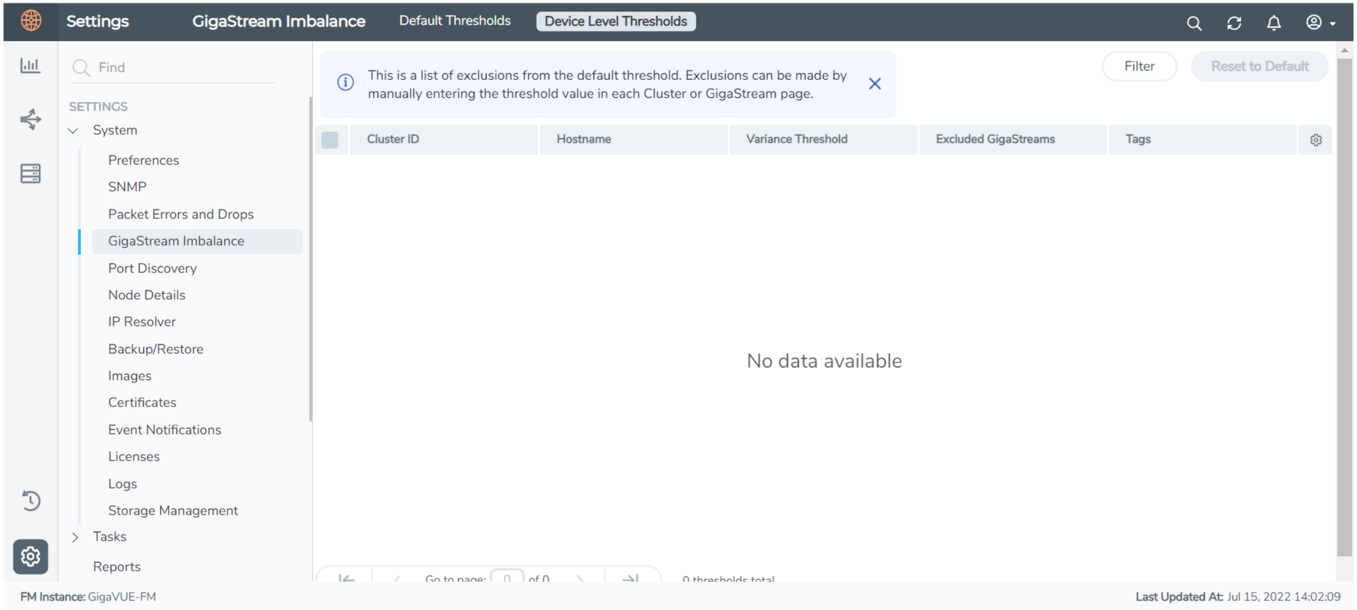
FM Instance: GigaVUE-FM

Last Updated At: Jul 15, 2022 14:02:09

Field	Description
GigaStream	GigaStream type for which the threshold is to be configured. Configuration for *All GigaStreams* 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.



This is a list of exclusions from the default threshold. Exclusions can be made by manually entering the threshold value in each Cluster or GigaStream page.

Cluster ID	Hostname	Variance Threshold	Excluded GigaStreams	Tags

No data available

Go to page: 0 of 0

0 thresholds total

FM Instance: GigaVUE-FM

Last Updated At: Jul 15, 2022 14:02:09

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 used 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 V Series 2 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:

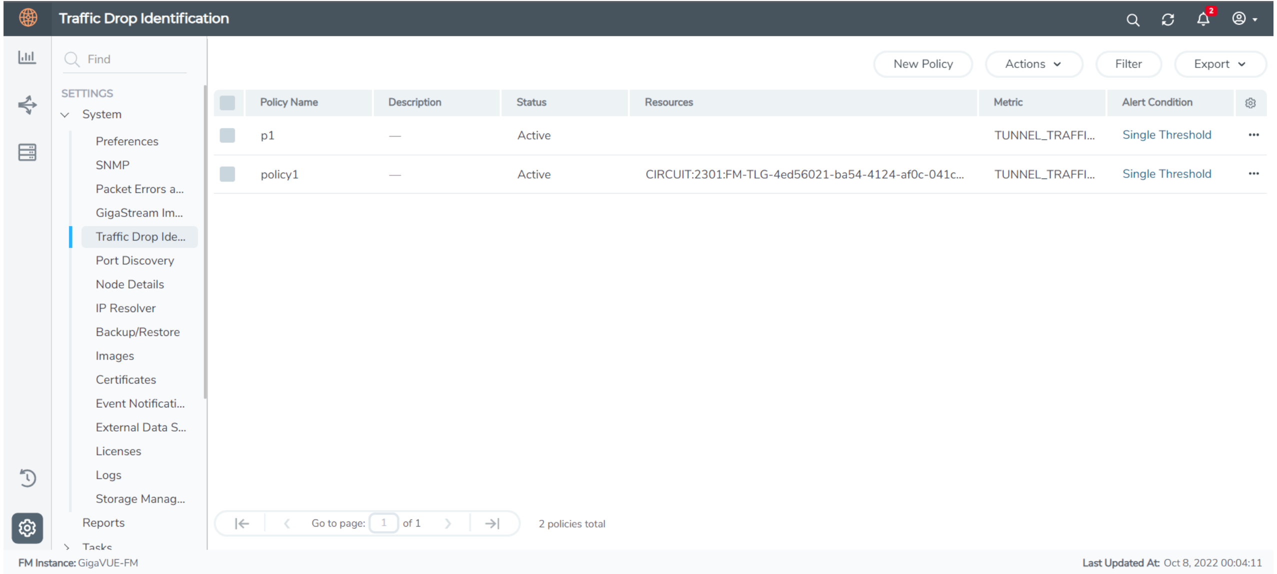
- For software version 6.1.00, traffic drop alert policies can be created only for tunnels discovered by GigaVUE-FM. Refer to Tunnel Monitoring section for details.
- For the tunnels discovered and listed in the Tunnel Monitoring page, Alert Policies can be configured only if the Tunnel Discovery State 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. On the left navigation pane, click ⚙ and select **System**> **Traffic Drop Identification**. The Traffic Drop Identification page appears.
2. Click **New Policy**.



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

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. - 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.

Port Discovery

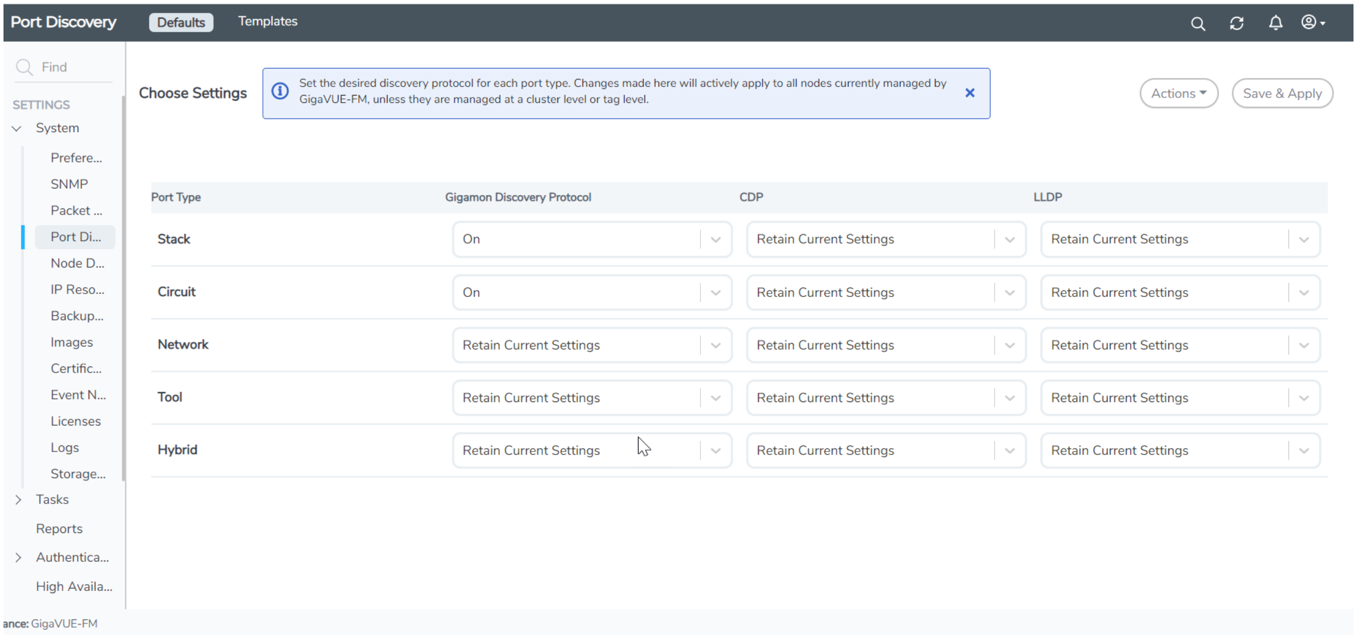
GigaVUE-FM allows you to configure the discovery protocols (CDP, LLDP and GDP) on each of the individual ports. However, in a scaled environment, where GigaVUE-FM manages a large number of devices, it is difficult and time-consuming to configure the protocols on each and every individual port. The Port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



Set the desired discovery protocol for each port type. Changes made here will actively apply to all nodes currently managed by GigaVUE-FM, unless they are managed at a cluster level or tag level.

Port Type	Gigamon Discovery Protocol	CDP	LLDP
Stack	On	Retain Current Settings	Retain Current Settings
Circuit	On	Retain Current Settings	Retain Current Settings
Network	Retain Current Settings	Retain Current Settings	Retain Current Settings
Tool	Retain Current Settings	Retain Current Settings	Retain Current Settings
Hybrid	Retain Current Settings	Retain Current Settings	Retain Current Settings

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

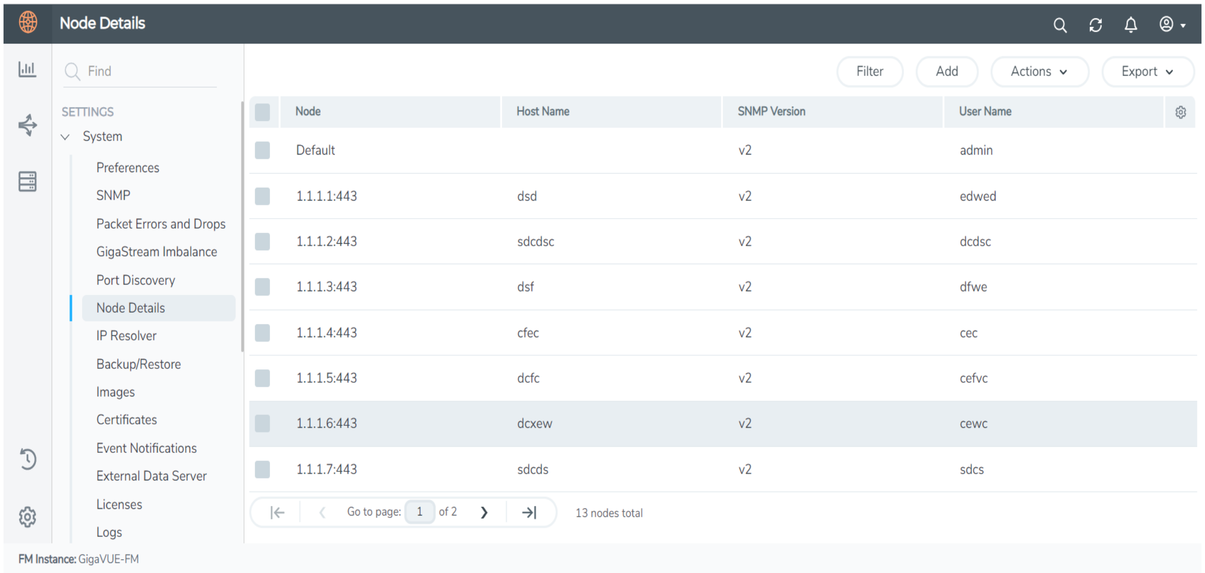
To edit a custom template:

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.

On the left navigation pane, click ⚙ 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	sdcdsc	v2	dcdsc
1.1.1.3:443	dsf	v2	dfwe
1.1.1.4:443	cfec	v2	cec
1.1.1.5:443	dcfc	v2	cefvc
1.1.1.6:443	dcxew	v2	cewc
1.1.1.7:443	sdcds	v2	sdcs

Figure 17 *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:

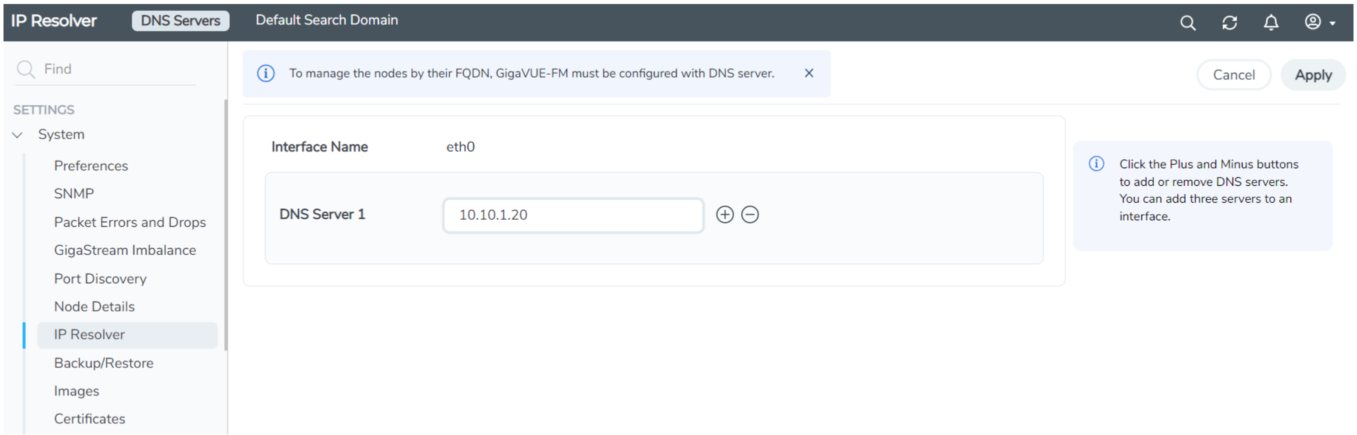
Controls	Description
Add	Allows you to add a node and its login credentials. - Clicking **Add** opens a dialog where you specify the following details: - Node IP address and port number - Host Name - User name - Password and Confirm Password options - SNMP Version - Only one node can be added each time. - 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.



To manage the nodes by their FQDN, GigaVUE-FM must be configured with DNS server.

Interface Name: eth0

DNS Server 1: 10.10.1.20

Click the Plus and Minus buttons to add or remove DNS servers. You can add three servers to an interface.

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. On the left navigation pane, click ⚙ 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. On the left navigation pane, click ⚙ 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.

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.

GigaVUE-FM Appliance

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.

Rules and Notes for Backup and Restore

- Backup and restore of GigaVUE-FM is only supported for users with super admin privileges.
- When you backup GigaVUE-FM, you will not be allowed to perform any non-get operations in GigaVUE-FM 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.
- 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 and regenerate the licenses.
- When creating a backup file, do not include the following special characters: **space * " ? ; : , / % @** in the alias.

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 Fabric Manager.
- User credentials needed to access the nodes
- Node level user account and RBAC configurations
- vMaps
- GigaVUE-FM credentials and preferences
- System configuration of GigaVUE-FM
- 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
- DHCP, NTP, and DNS configurations

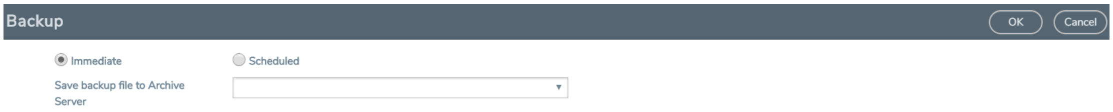
These are configured through the jump-start configuration when configuring a new GigaVUE-FM.

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 18Immediate Backup to an Archive Server.

   To add an archive server, refer to Add an Archive Server.
6. Click **OK**.



● Immediate ○ Scheduled

Save backup file to Archive Server

Figure 18 *Immediate Backup to an Archive Server*

Schedule Backups

To create a schedule for backing up GigaVUE-FM, do the following:

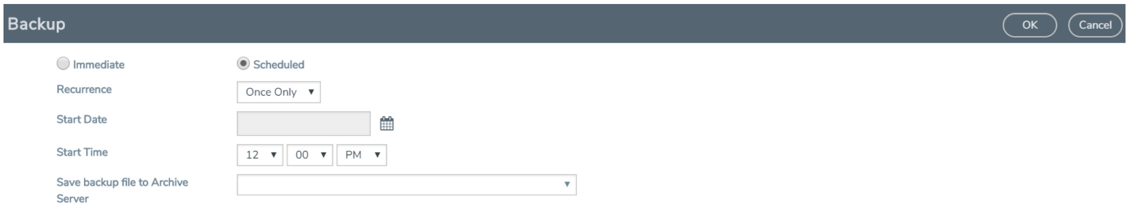
1. On the right side of the top navigation bar, click ⚙.
2. On the left navigation pane, select **System > Backup/Restore > GigaVUE FM Appliance.**
   a. Click **Backup**.
   b. Select **Scheduled**.

   The GigaVUE-FM time clock is based on ESX host time. Make sure that you have synchronized clock before any scheduling operation.

3. 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 19Scheduled 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.



Backup

○ Immediate ● Scheduled

Recurrence: Once Only

Start Date:

Start Time: 12 00 PM

Save backup file to Archive Server:

Figure 19 *Scheduled Backup for GigaVUE-FM*

4. 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:

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 **Restore**.

   The Restore page displays, showing the file names from which to restore.
4. Select the Archive Server from which to retrieve the backup file.
5. 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.
6. Click **OK**.

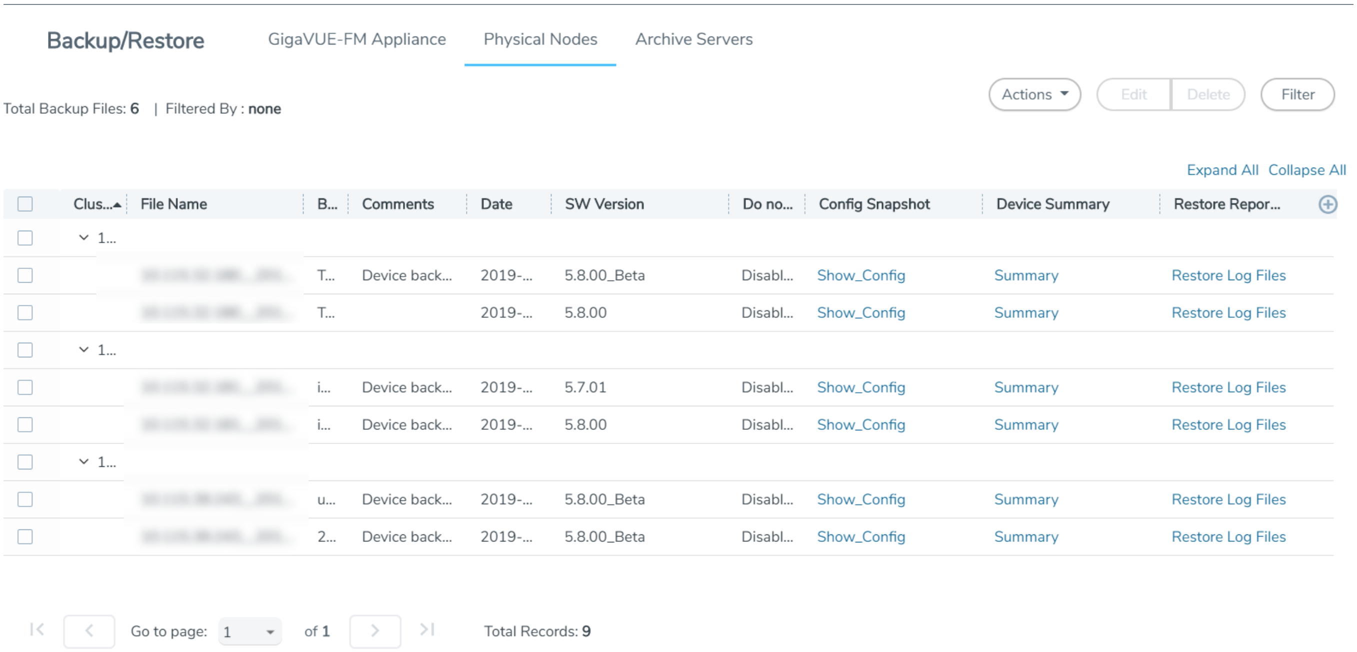
> **NOTE:** GigaVUE-FM will reboot once after successful restore operation. Logs will be recorded in the Audit Logs page with Restore Complete/Success Message.

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.

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.



Total Backup Files: **6** | Filtered By : **none**

□	Clus...	File Name	B...	Comments	Date	SW Version	Do no...	Config Snapshot	Device Summary	Restore Repor...
□	1...									
□		[redacted]	T...	Device back...	2019-...	5.8.00_Beta	Disabl...	Show_Config	Summary	Restore Log Files
□		[redacted]	T...		2019-...	5.8.00	Disabl...	Show_Config	Summary	Restore Log Files
□	1...									
□		[redacted]	i...	Device back...	2019-...	5.7.01	Disabl...	Show_Config	Summary	Restore Log Files
□		[redacted]	i...	Device back...	2019-...	5.8.00	Disabl...	Show_Config	Summary	Restore Log Files
□	1...									
□		[redacted]	u...	Device back...	2019-...	5.8.00_Beta	Disabl...	Show_Config	Summary	Restore Log Files
□		[redacted]	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 20 *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.

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

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**.

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

NOTE:

- 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. Redeploy the solutions.

Images

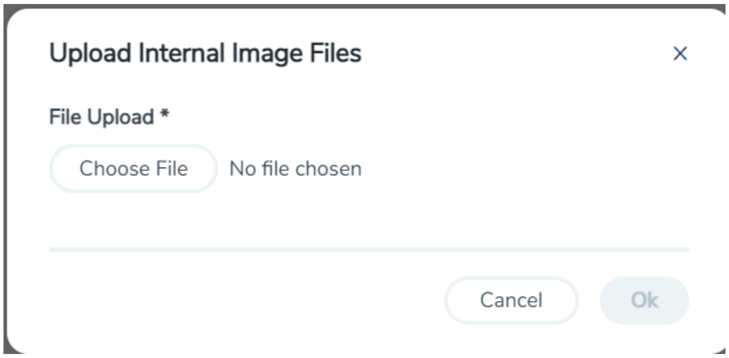
The Images page is used to specify the servers where you will store image files for upgrading your nodes. You obtain images for your nodes by contacting Technical Support. Once you have the images, you can use an external server or use GigaVUE-FM as the image server.

On the left navigation pane, click ⚙ 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-HC2 node selected for uploading. To upload the file, click **OK**.



Upload Internal Image Files

File Upload *

Choose File No file chosen

Figure 21 *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 ● **Usernameand 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 server was 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:

- Trust Store
- 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.
- ACME Certificate
- Configure ACME Server
- 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.

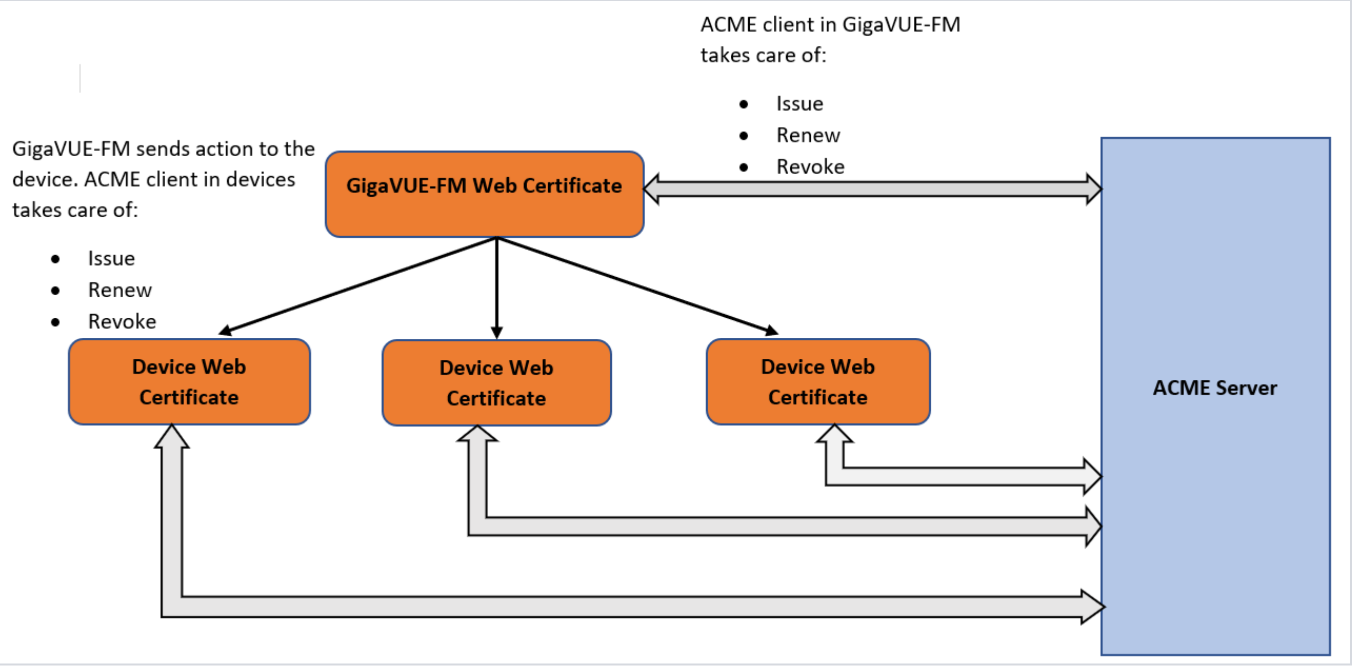
> **NOTE:** For more details about the Automatic Certificate Management Environment protocol, refer to RFC 8555.

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:


ACME client in GigaVUE-FM takes care of:
Issue
Renew
Revoke
GigaVUE-FM sends action to the device. ACME client in devices takes care of:
Issue
Renew
Revoke
GigaVUE-FM Web Certificate
Device Web Certificate
Device Web Certificate
Device Web Certificate
ACME Server

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). **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.	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. - 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.
- ACME server's root 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. Mltiple 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:

- ACME Certificate
- 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: `openssl pkcs12 -export -name CMS -out cms.p12 -inkey localhost.key -in localhost.crt -passout pass:cms123` • 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 Configure ACME Server 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's web certificate server certificate is handled as follows:	Refer to Certificate Renewal.

Task	Description	Refer to...
	- **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. - 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 to do the following:

- 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.
- Login to GigaVUE-FM CLI and add the private key and certificate of GigaVUE-FM through CLI/Console (into GigaVUE-FM).

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.

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.

GigaVUE-OS Version	Customer Trust Store	Gigamon Trust Store (CC*) *with Custom Certificates*	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

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.

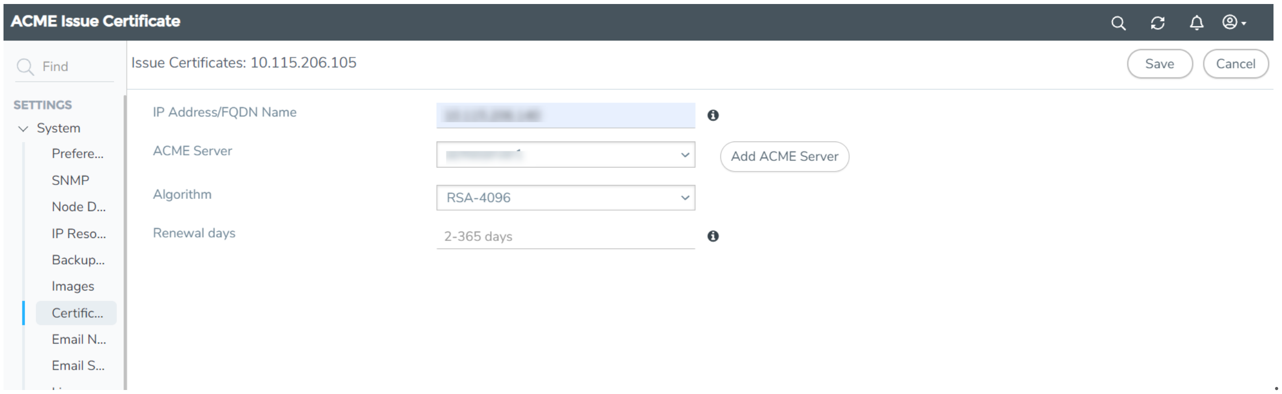
Refer to the following sections for details.

Certificate Issuance

For certificate issuance by the ACME server:

> **NOTE:** Ensure to configure the ACME server before performing these steps.

1. On the left navigation pane, click ⚙ 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.



Issue Certificates: 10.115.206.105

IP Address/FQDN Name: [redacted]

ACME Server: [redacted]

Algorithm: RSA-4096

Renewal days: 2-365 days

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.

Field	Description
	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. On the left navigation pane, click ⚙ 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. On the left navigation pane, click ⚙ 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

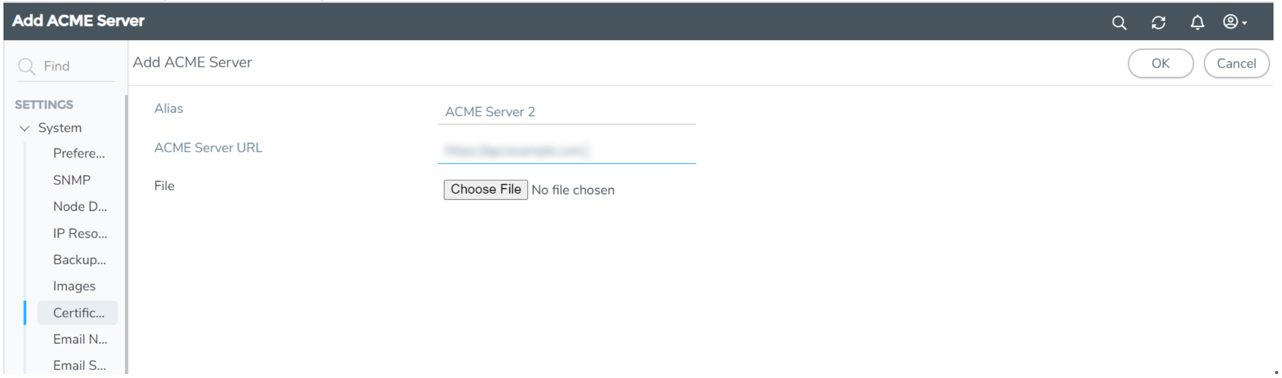
Click Delete Certificates to delete a certificate. GigaVUE-FM will fall back to the default certificate process.

Configure ACME Server

The ACME server page allows you to configure the ACME server details in GigaVUE-FM.

To add a server:

1. On the left navigation pane, click and select **Certificates** > **ACME Server**. The **ACME Server** page is displayed.



Alias: ACME Server 2

ACME Server URL: [redacted]

File: No file chosen

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
File	Choose the CA file from the required location.

3. Click **OK**. The server will get added to the list view.

Notes

Refer to the following notes:

- 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.

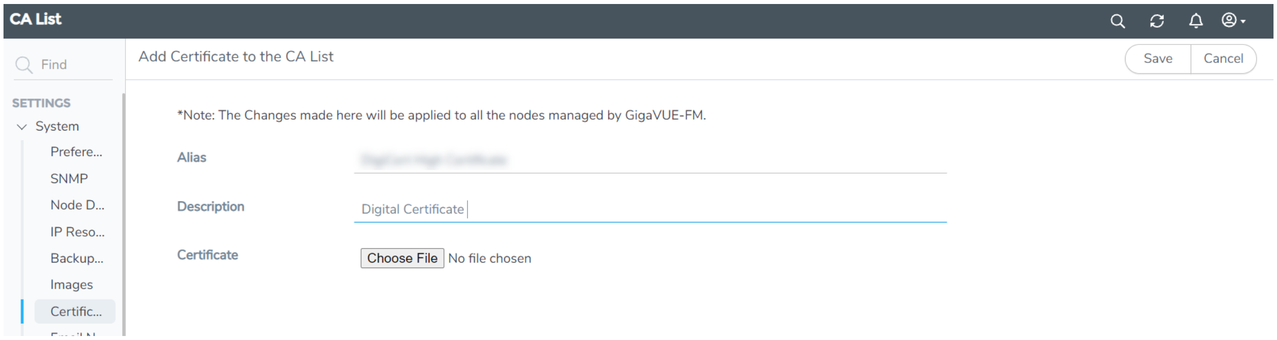
CA List

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. On the left navigation pane, click ⚙ and select **Certificates** > **CA List**.
2. Click **Add**.



Add Certificate to the CA List

*Note: The Changes made here will be applied to all the nodes managed by GigaVUE-FM.

Alias [redacted]

Description Digital Certificate

Certificate Choose File No file chosen

3. Select or enter the following details:

Field	Description
Alias	Alias name of the CA.
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:

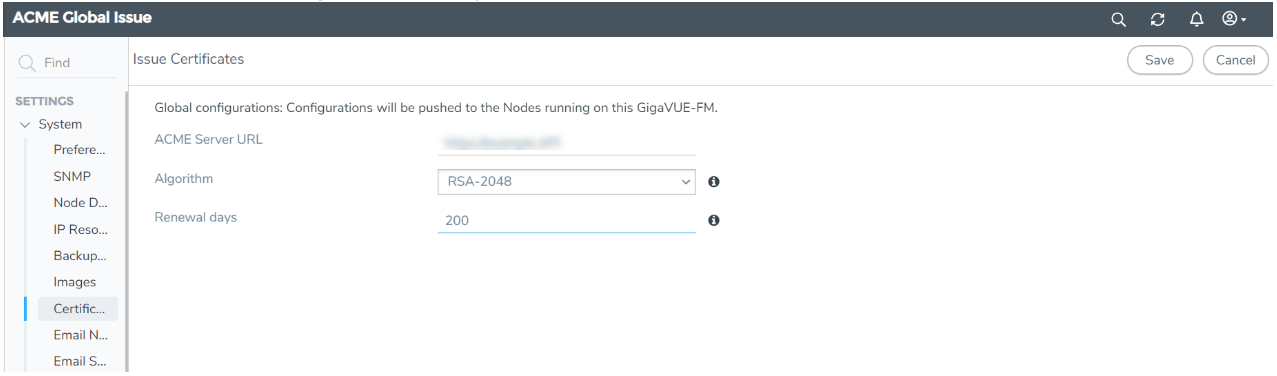
From GigaVUE-FM	Go to **Settings** > **System** > **Certificate** > **ACME Certificate**	Use this for global configuration of all the devices managed by GigaVUE-FM
From Devices	Go to **Inventory > Node** > **Settings** > **Global Settings** > **ACME Certificate**	Use this for configuration of individual 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. On the left navigation pane, click ⚙ and select **Certificates** > **ACME Certificate**. The **ACME Certificate** page is displayed.



Global configurations: Configurations will be pushed to the Nodes running on this GigaVUE-FM.

ACME Server URL [redacted]

Algorithm RSA-2048

Renewal days 200

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.

Field	Description
	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.
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. On the left navigation pane, click ⚙ 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.

Event Notifications

GigaVUE-FM provides powerful email notification capabilities, automatically sending emails to specified addresses when any of 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 TA Series, and the notifications are forwarded to the Fabric Manager. For a node to be able to send notifications to the Fabric Manager, the node's SNMP notifications must be configured with the Fabric Manager's IP address. 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 Email Servers.
- 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	Refer to..
Tags	Get notified about the events based on the tags (both RBAC and Aggregation tags)	Tags
Recipients	Add the email address 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 SNMP Traps Notification
Events	List of events for which the notification should be sent. Refer to Events

Tags

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 the 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 is to 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
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.

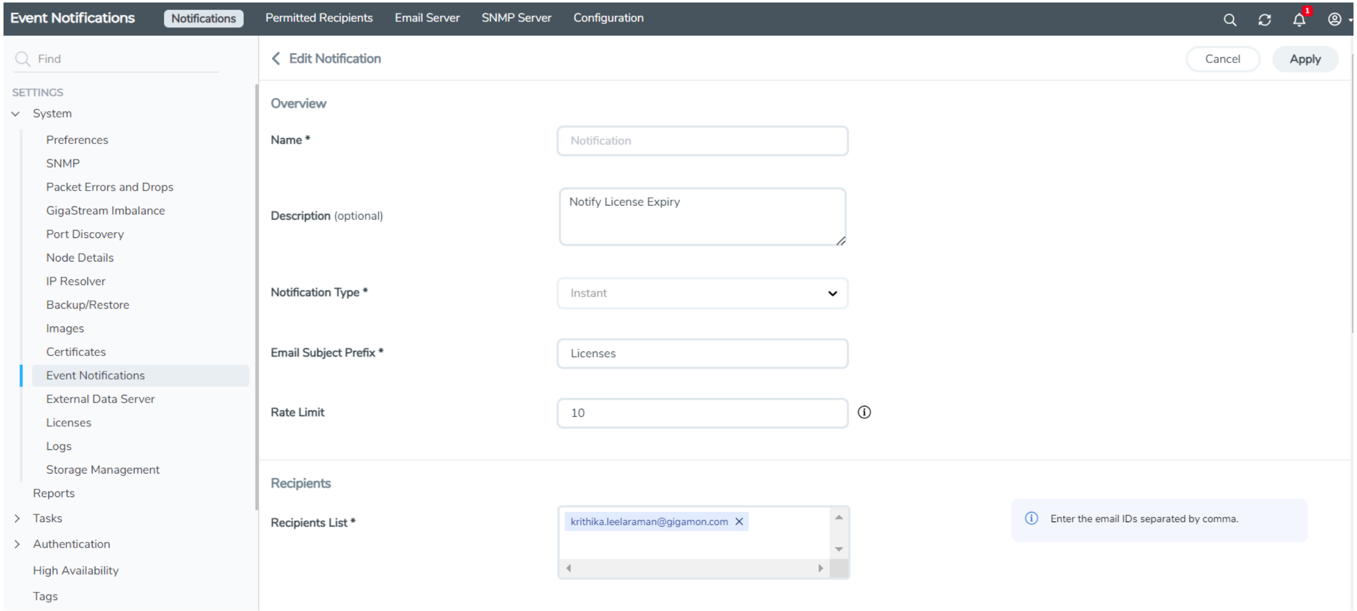
Buttons

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:



Name * Notification

Description (optional) Notify License Expiry

Notification Type * Instant

Email Subject Prefix * Licenses

Rate Limit 10

Recipients List * krithika.leelaraman@gigamon.com

Enter the email IDs separated by comma.

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 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, use 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 in 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 also has 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.
   - **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 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

   c. Enter the server port number in the **SNMP Port** field. The default port number is **162**.

   d. Enter the community string in the **Community** field for SNMP Version v2c. For example, public.

4. 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
- Meta data exporter in case of the Application Filtering Intelligence solution

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. On the left navigation pane, click ⚙ 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 the Fully Qualified Domain Name of GigaVUE-FM or static IP like public IP (AWS)
- **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. On the left navigation pane, click ⚙ 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.
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

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 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 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.

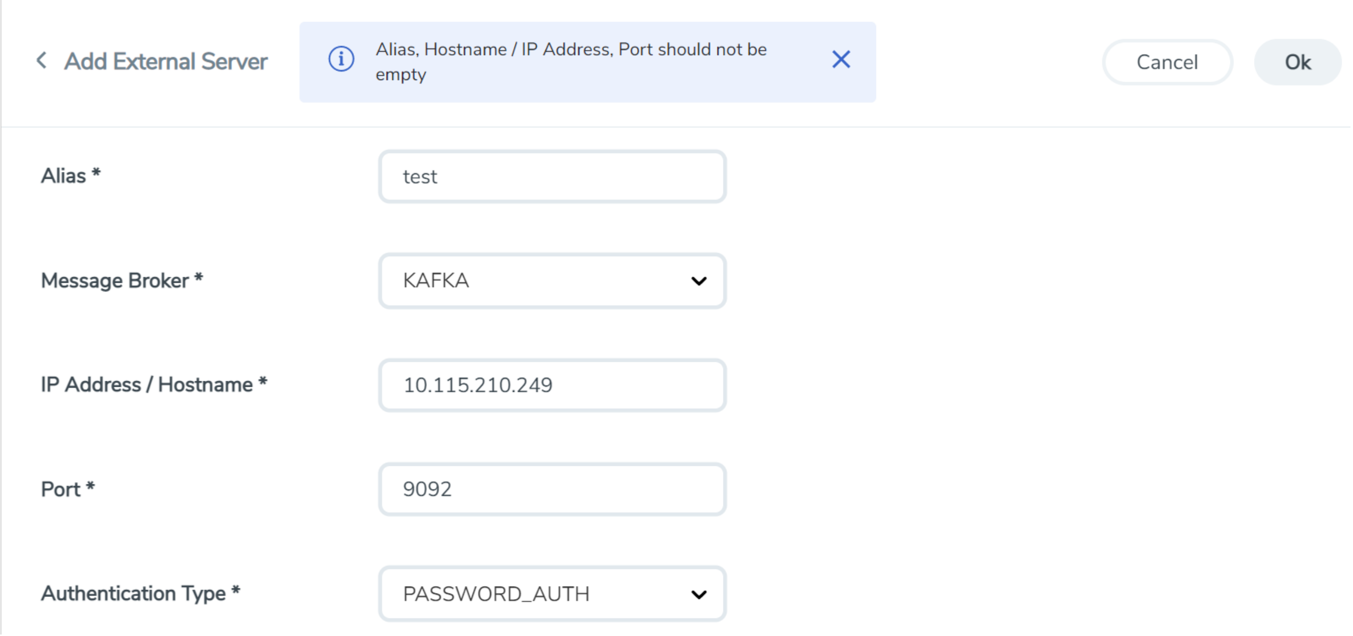
Configure External Data Server

Pre-requisite: The port that is configured must be open in the external data server.

To configure an external data server:

1. On the left navigation pane, click ⚙ and select **System > External Data Server.**

2. Click **Add**.



Alias, Hostname / IP Address, Port should not be empty

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 3.2.0[1]. ● 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.

[1] Use 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: *Successfully sent the test message to the selected Kafka server* • Upon failure of validation, the following message pops-up: *Unable to send message via the configured Kafka broker*
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.

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.

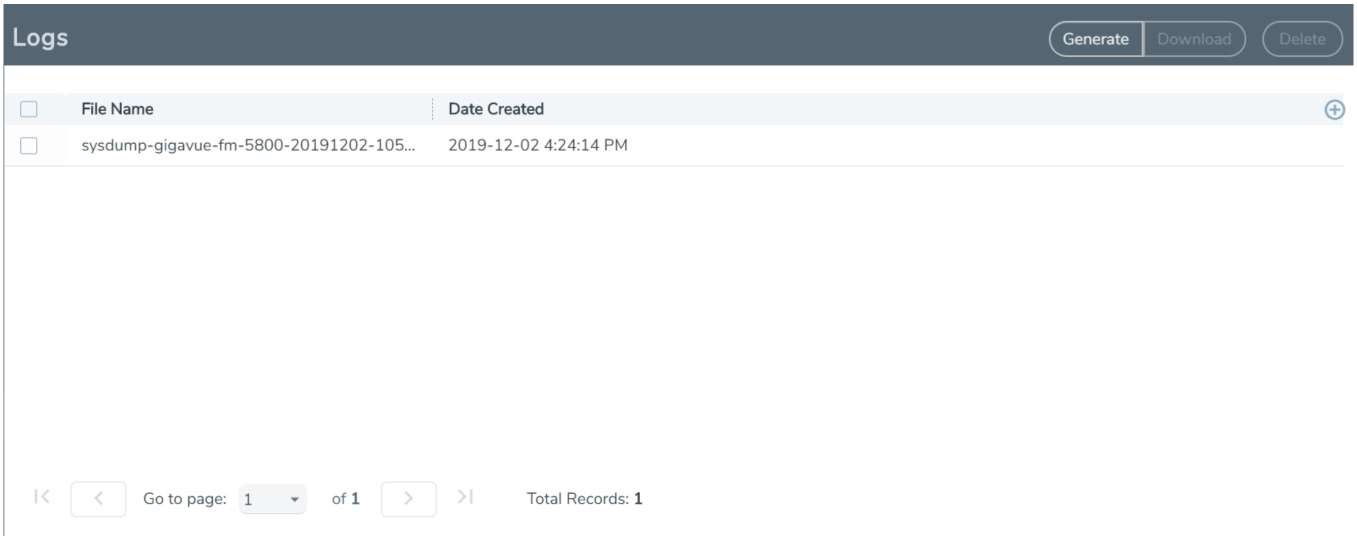
- On the left navigation pane, click ⚙ and select **System > Logs** , to access Logs.
- Click the **Download** button to download the compressed files.

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.



☐	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 22 *Logs Page*

2. Click **Generate**.

   The system generates a new log file and displays an event message.

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:

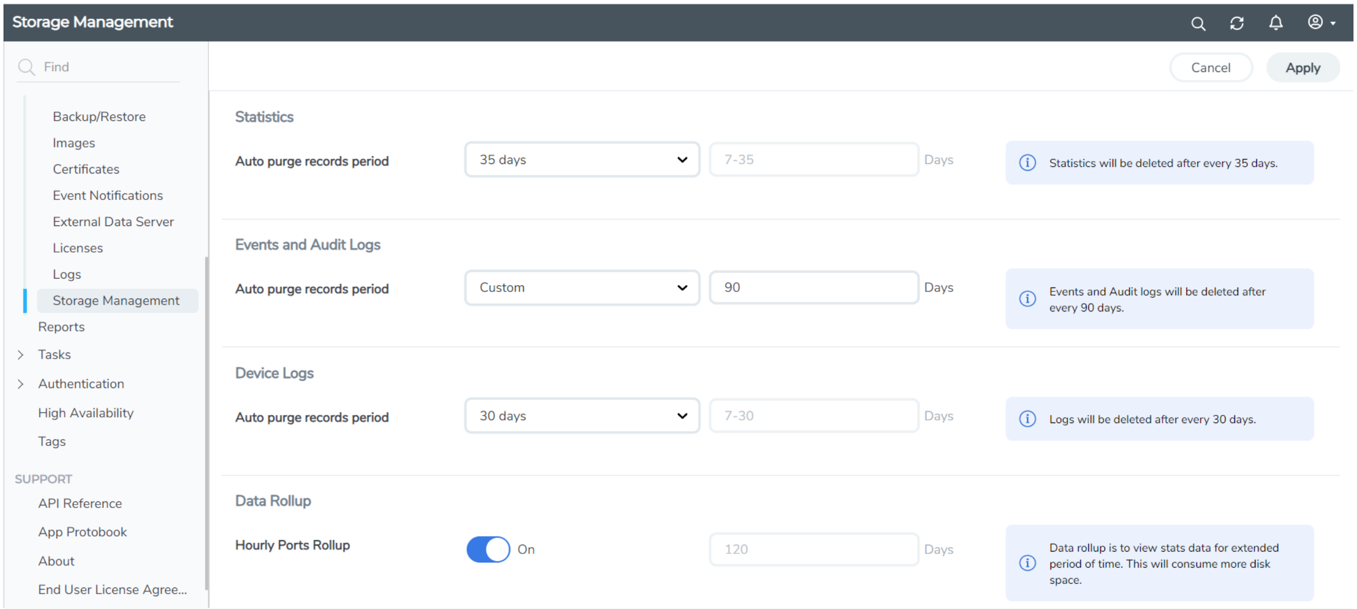
1. Select **System** > **Logs**.

   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.

On the left navigation pane, click ⚙ to access Storage Management and select **System > Storage Management**.



Statistics

Auto purge records period: 35 days | 7-35 Days | Statistics will be deleted after every 35 days.

Events and Audit Logs

Auto purge records period: Custom | 90 Days | Events and Audit logs will be deleted after every 90 days.

Device Logs

Auto purge records period: 30 days | 7-30 Days | Logs will be deleted after every 30 days.

Data Rollup

Hourly Ports Rollup: On | 120 Days | Data rollup is to view stats data for extended period of time. This will consume more disk space.

To free the used storage older than specified period:

1. On the left navigation pane, click ⚙ and navigate to **System > Storage Management**. The Storage Management page is displayed.
2. Specify the Storage Management settings for each type of record using the drop-down.
3. Click **Apply** to apply the settings.

Setting		Description
Statistics		
	Delete stats older than	Select the purge period, which is the number of days after which the records will be for deleted. Options are • 7 days • 35 days

Setting		Description
		• custom (between 7 and 35 days) 35 days is the default. **Important**: The records will be immediately and 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		
	Automatically delete 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. When you click **OK**, the records older than the specified duration will get deleted immediately. 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		
	Automatically delete 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. When you click **OK**, the records older than the specified duration will get deleted immediately. 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 Logs page for the node.
Rollup - Hourly Ports Rollup		
	Allows you to browse and evaluate the performance of Port Statistics for a duration of up to 120 days.	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.

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.

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

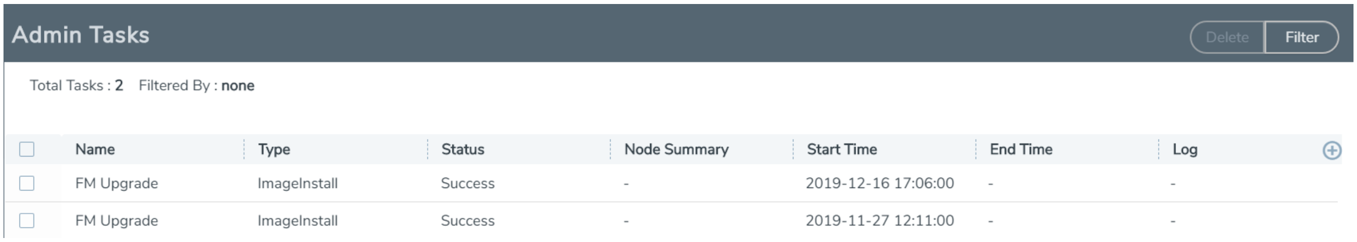
This section covers the following topics:

- 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.

On the left navigation pane, click ⚙ , to view the **Admin Tasks** and click **Tasks**.



Admin Tasks

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 Admin Tasks.

> **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. On the left navigation pane, click ⚙ select **Tasks**.
2. In the Admin Tasks page, click the Detail link in the Node Summary column. Refer to Admin Tasks.
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. On the left navigation pane, click ⚙ 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.

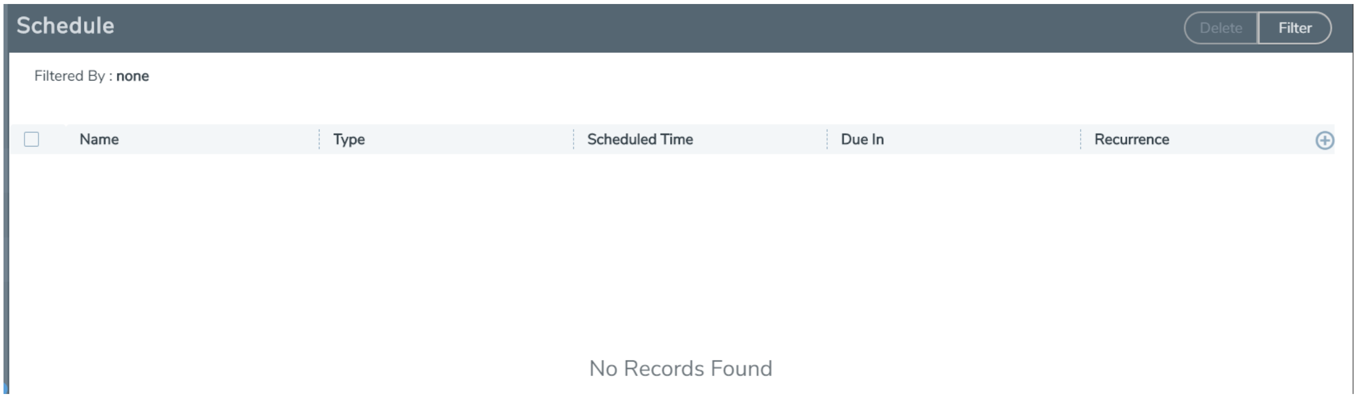


Figure 24 *Scheduled Tasks Page*

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:

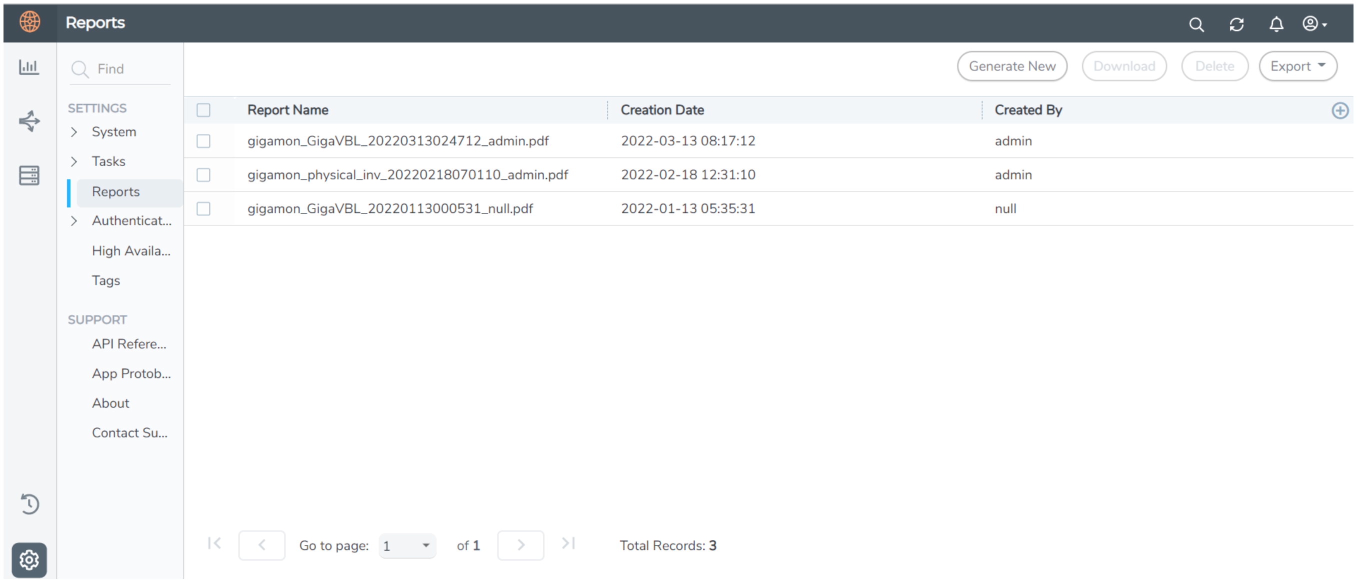
1. On the left navigation pane, click ⚙ select **Tasks > Scheduled Task**.
2. Select a task from the list.

   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.



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

Refer to the following sections for details:

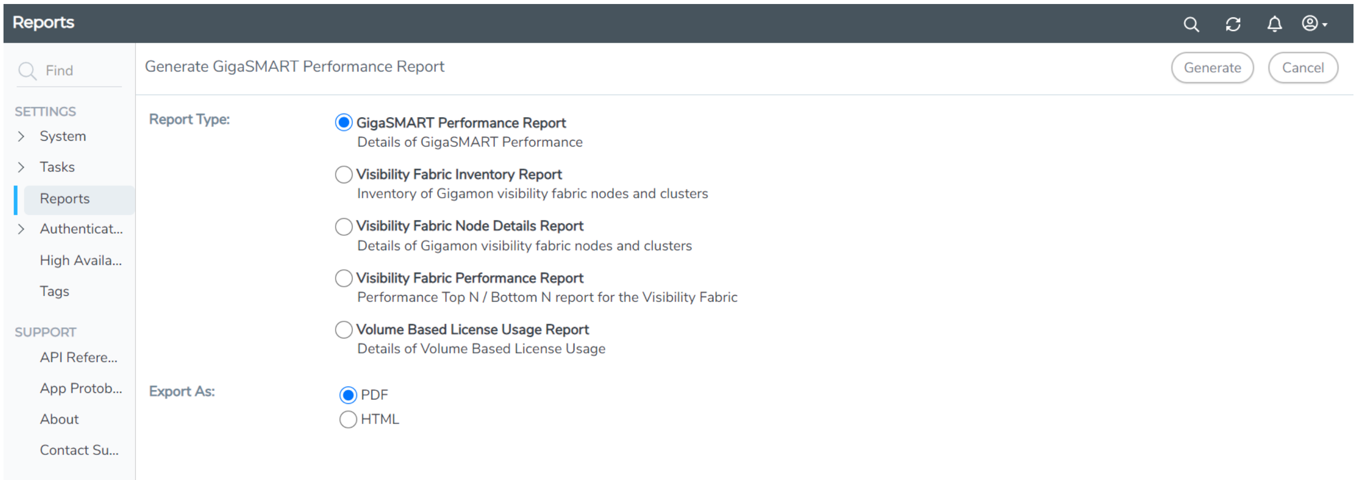
- Overview of Reports
- Generate Reports
- NetFlow Format Support on Exporters

Generate Reports

To generate reports:

1. On the left navigation pane, click 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.



Generate GigaSMART Performance Report

Report Type:

● GigaSMART Performance Report
Details of GigaSMART Performance

○ Visibility Fabric Inventory Report
Inventory of Gigamon visibility fabric nodes and clusters

○ Visibility Fabric Node Details Report
Details of Gigamon visibility fabric nodes and clusters

○ Visibility Fabric Performance Report
Performance Top N / Bottom N report for the Visibility Fabric

○ Volume Based License Usage Report
Details of Volume Based License Usage

Export As:

● PDF
○ HTML

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.

Overview of Reports

The Reports page allows you to create the following types of reports:

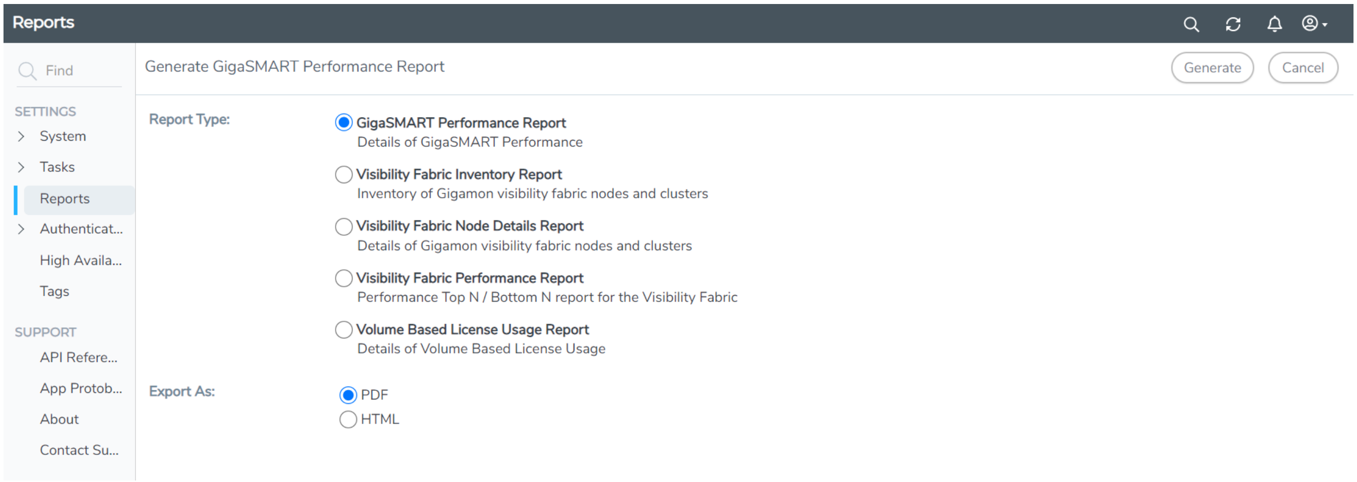
- GigaSMART Performance Report provides a summary of GigaSMART performance for all HC Series nodes with GigaSMART functionality.
- Visibility Fabric Inventory Report provides a summary of all physical inventory (includes HC Series and TA Series) that is visible on GigaVUE-FM.
- Visibility Fabric Node Details Report provides specific details relating to the physical nodes (includes HC Series, 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. On the left navigation pane, click ⚙ 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.



Generate GigaSMART Performance Report

Report Type:

- ● GigaSMART Performance Report
  Details of GigaSMART Performance
- ○ Visibility Fabric Inventory Report
  Inventory of Gigamon visibility fabric nodes and clusters
- ○ Visibility Fabric Node Details Report
  Details of Gigamon visibility fabric nodes and clusters
- ○ Visibility Fabric Performance Report
  Performance Top N / Bottom N report for the Visibility Fabric
- ○ Volume Based License Usage Report
  Details of Volume Based License Usage

Export As:

- ● PDF
- ○ HTML

Figure 26 *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.

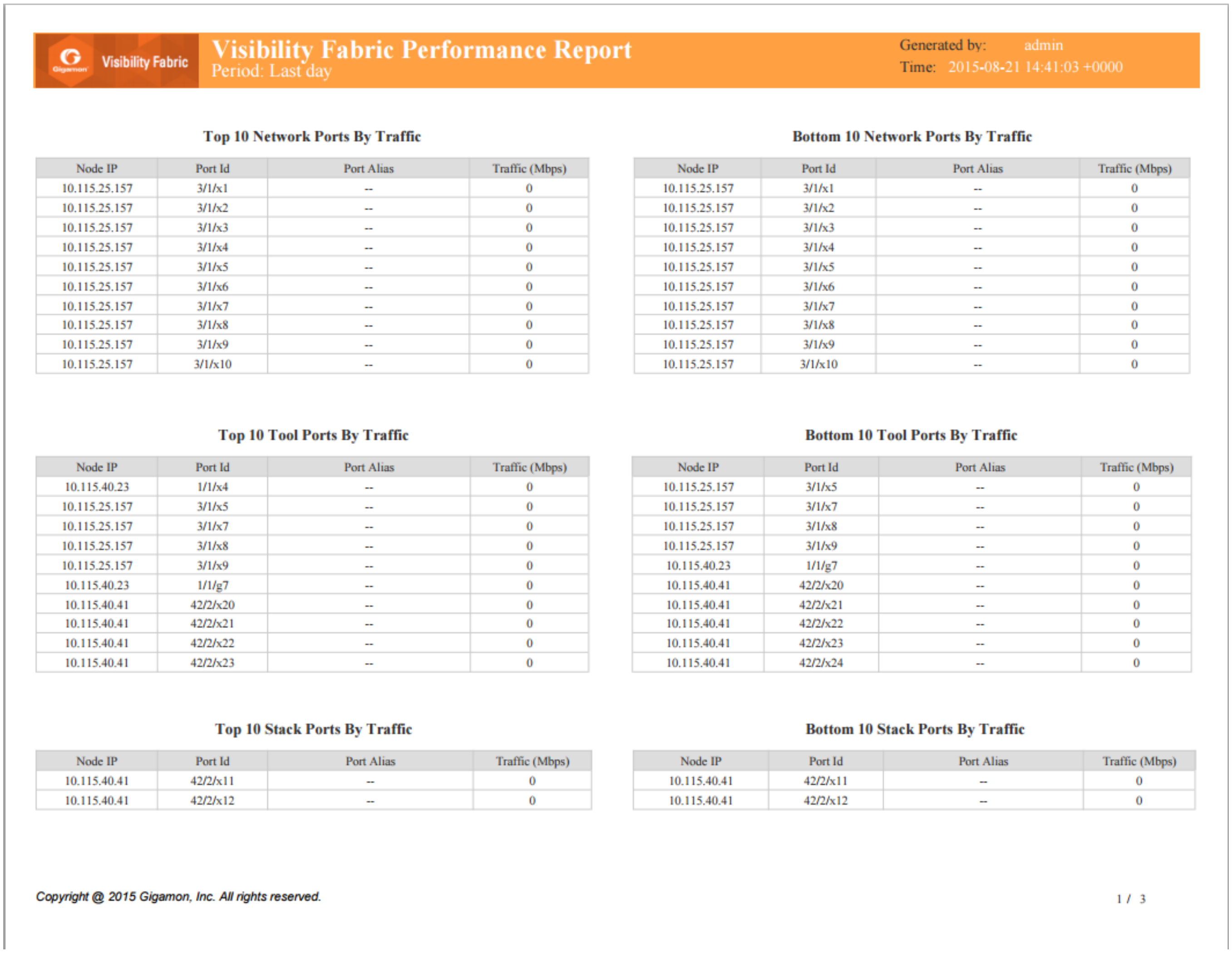
To view the reports directly from the GigaVUE-FM settings, ensure that the pop-up blocker settings on your browser is disabled. This allows you to view the reports without downloading. The reports will be available on a separate page.

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 27Visibility Fabric Performance Report shows an example of a report for Visibility Fabric Performance.



Visibility Fabric

Visibility Fabric Performance Report
Period: Last day

Generated by: admin
Time: 2015-08-21 14:41:03 +0000

Top 10 Network Ports By Traffic

Node IP	Port Id	Port Alias	Traffic (Mbps)
10.115.25.157	3/1/x1	--	0
10.115.25.157	3/1/x2	--	0
10.115.25.157	3/1/x3	--	0
10.115.25.157	3/1/x4	--	0
10.115.25.157	3/1/x5	--	0
10.115.25.157	3/1/x6	--	0
10.115.25.157	3/1/x7	--	0
10.115.25.157	3/1/x8	--	0
10.115.25.157	3/1/x9	--	0
10.115.25.157	3/1/x10	--	0

Bottom 10 Network Ports By Traffic

Node IP	Port Id	Port Alias	Traffic (Mbps)
10.115.25.157	3/1/x1	--	0
10.115.25.157	3/1/x2	--	0
10.115.25.157	3/1/x3	--	0
10.115.25.157	3/1/x4	--	0
10.115.25.157	3/1/x5	--	0
10.115.25.157	3/1/x6	--	0
10.115.25.157	3/1/x7	--	0
10.115.25.157	3/1/x8	--	0
10.115.25.157	3/1/x9	--	0
10.115.25.157	3/1/x10	--	0

Top 10 Tool Ports By Traffic

Node IP	Port Id	Port Alias	Traffic (Mbps)
10.115.40.23	1/1/x4	--	0
10.115.25.157	3/1/x5	--	0
10.115.25.157	3/1/x7	--	0
10.115.25.157	3/1/x8	--	0
10.115.25.157	3/1/x9	--	0
10.115.40.23	1/1/g7	--	0
10.115.40.41	42/2/x20	--	0
10.115.40.41	42/2/x21	--	0
10.115.40.41	42/2/x22	--	0
10.115.40.41	42/2/x23	--	0

Bottom 10 Tool Ports By Traffic

Node IP	Port Id	Port Alias	Traffic (Mbps)
10.115.25.157	3/1/x5	--	0
10.115.25.157	3/1/x7	--	0
10.115.25.157	3/1/x8	--	0
10.115.25.157	3/1/x9	--	0
10.115.40.23	1/1/g7	--	0
10.115.40.41	42/2/x20	--	0
10.115.40.41	42/2/x21	--	0
10.115.40.41	42/2/x22	--	0
10.115.40.41	42/2/x23	--	0
10.115.40.41	42/2/x24	--	0

Top 10 Stack Ports By Traffic

Node IP	Port Id	Port Alias	Traffic (Mbps)
10.115.40.41	42/2/x11	--	0
10.115.40.41	42/2/x12	--	0

Bottom 10 Stack Ports By Traffic

Node IP	Port Id	Port Alias	Traffic (Mbps)
10.115.40.41	42/2/x11	--	0
10.115.40.41	42/2/x12	--	0

Copyright @ 2015 Gigamon, Inc. All rights reserved.

1 / 3

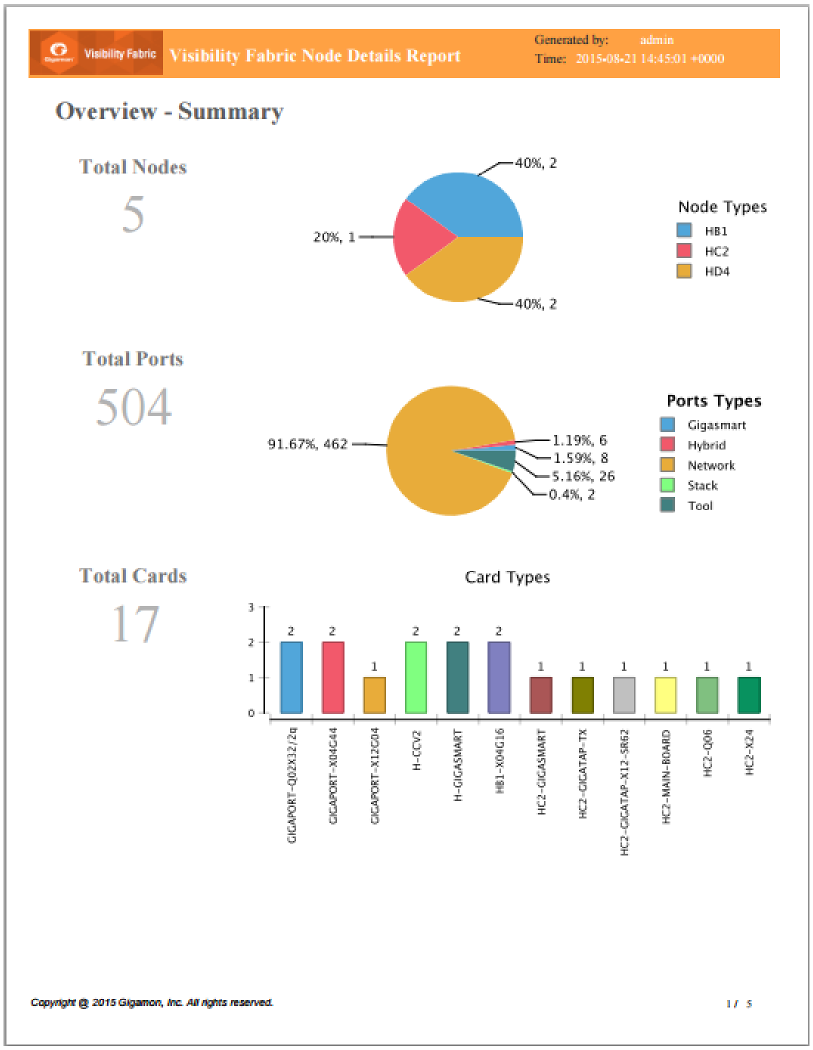
Figure 27 *Visibility Fabric Performance Report*

Visibility Fabric Node Details Report

This multi-page report provides you with printable format for specific details relating to the Physical Nodes (includes H Series, G Series and 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 FM
- Detailed report similar to as shown on Chassis Page including clustered nodes

Figure 28Inventory Details Report shows an example of a report for Visibility Fabric Node Details.



Visibility Fabric Node Details Report

Generated by: admin
Time: 2015-08-21 14:45:01 +0000

Overview - Summary

Total Nodes
5

Total Ports
504

Total Cards
17

Copyright @ 2015 Gigamon, Inc. All rights reserved.

1 / 5

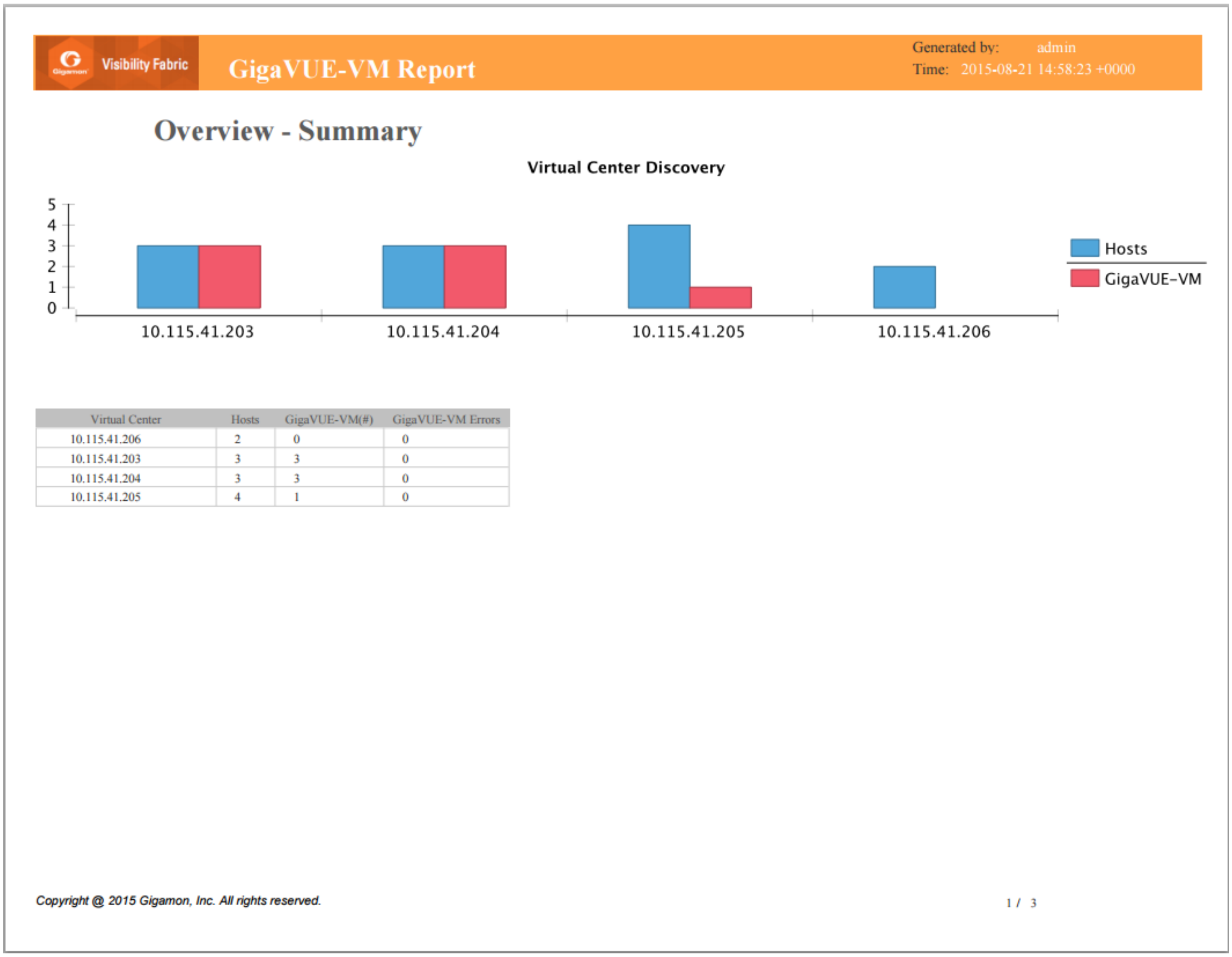
Figure 28 *Inventory Details Report*

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 29Report Pages Available for GigaVUE-VM show an example of a report for GigaVUE-VM.



Visibility Fabric **GigaVUE-VM Report**

Generated by: admin
Time: 2015-08-21 14:58:23 +0000

Overview - Summary

Virtual Center Discovery

Virtual Center	Hosts	GigaVUE-VM(#)	GigaVUE-VM Errors
10.115.41.206	2	0	0
10.115.41.203	3	3	0
10.115.41.204	3	3	0
10.115.41.205	4	1	0

Copyright @ 2015 Gigamon, Inc. All rights reserved.

1 / 3

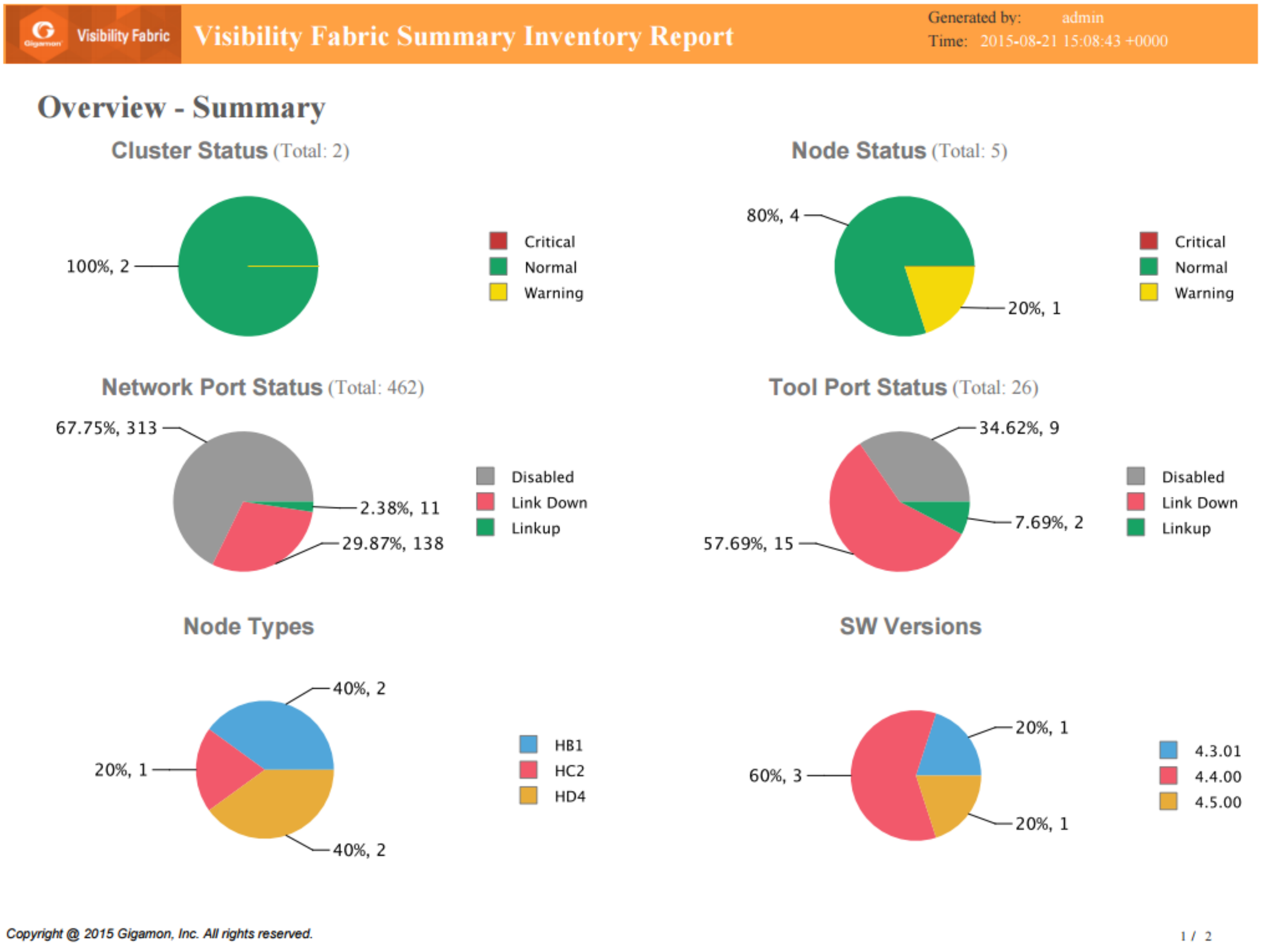
Figure 29 *Report Pages Available for GigaVUE-VM*

Visibility Fabric Inventory Report

This multi-page report provides you with printable format of summary on all your Physical inventory (includes H Series, G Series and 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 30Inventory Summary Report show an example of a report for Visibility Fabric Inventory.


Visibility Fabric Summary Inventory Report

Generated by: admin
Time: 2015-08-21 15:08:43 +0000

Overview - Summary

Copyright @ 2015 Gigamon, Inc. All rights reserved.

1 / 2

Figure 30 *Inventory Summary Report*

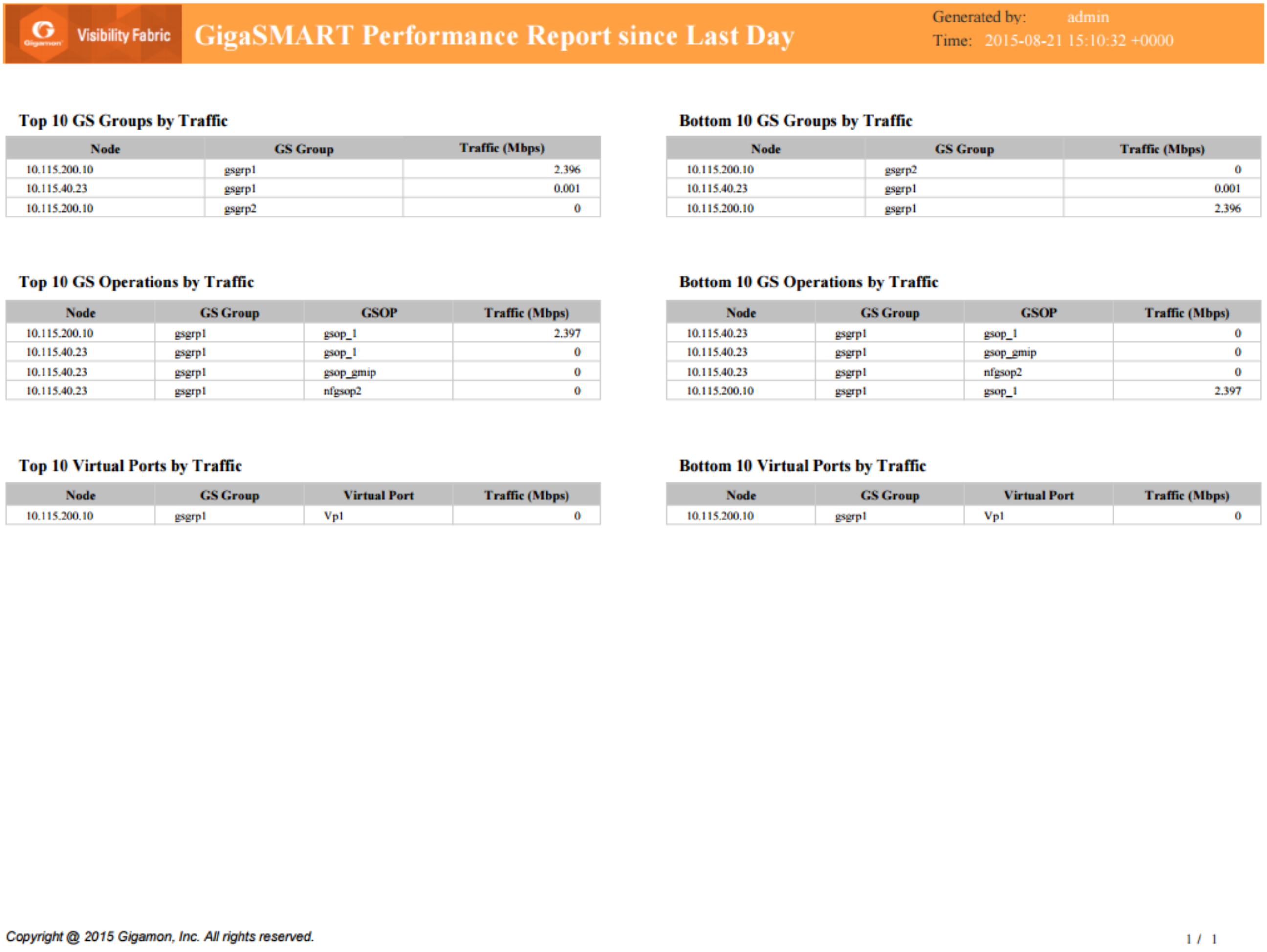
GigaSMART Performance Report

This report provides you with printable format of summary on GigaSMART performance for all H 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 31Report for GigaSMART Performance Indicators show an example of a report for GigaSMART Performance.



Visibility Fabric GigaSMART Performance Report since Last Day

Generated by: admin
Time: 2015-08-21 15:10:32 +0000

Top 10 GS Groups by Traffic

Node	GS Group	Traffic (Mbps)
10.115.200.10	gsgrp1	2.396
10.115.40.23	gsgrp1	0.001
10.115.200.10	gsgrp2	0

Bottom 10 GS Groups by Traffic

Node	GS Group	Traffic (Mbps)
10.115.200.10	gsgrp2	0
10.115.40.23	gsgrp1	0.001
10.115.200.10	gsgrp1	2.396

Top 10 GS Operations by Traffic

Node	GS Group	GSOP	Traffic (Mbps)
10.115.200.10	gsgrp1	gsop_1	2.397
10.115.40.23	gsgrp1	gsop_1	0
10.115.40.23	gsgrp1	gsop_gmip	0
10.115.40.23	gsgrp1	nfgsop2	0

Bottom 10 GS Operations by Traffic

Node	GS Group	GSOP	Traffic (Mbps)
10.115.40.23	gsgrp1	gsop_1	0
10.115.40.23	gsgrp1	gsop_gmip	0
10.115.40.23	gsgrp1	nfgsop2	0
10.115.200.10	gsgrp1	gsop_1	2.397

Top 10 Virtual Ports by Traffic

Node	GS Group	Virtual Port	Traffic (Mbps)
10.115.200.10	gsgrp1	Vp1	0

Bottom 10 Virtual Ports by Traffic

Node	GS Group	Virtual Port	Traffic (Mbps)
10.115.200.10	gsgrp1	Vp1	0

Copyright @ 2015 Gigamon, Inc. All rights reserved.

1 / 1

Figure 31 *Report for GigaSMART Performance Indicators*

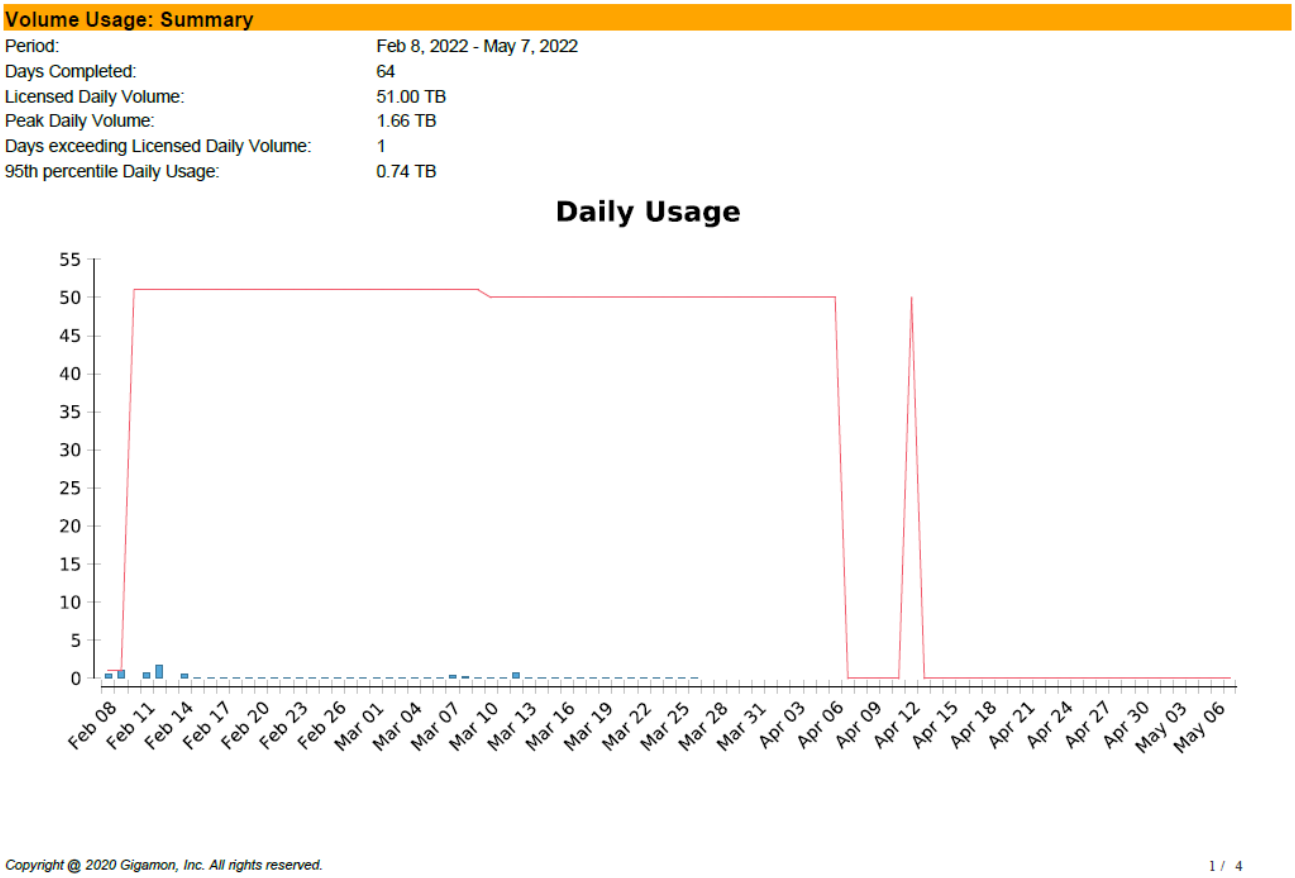
Volume Based License Usage Reports

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.

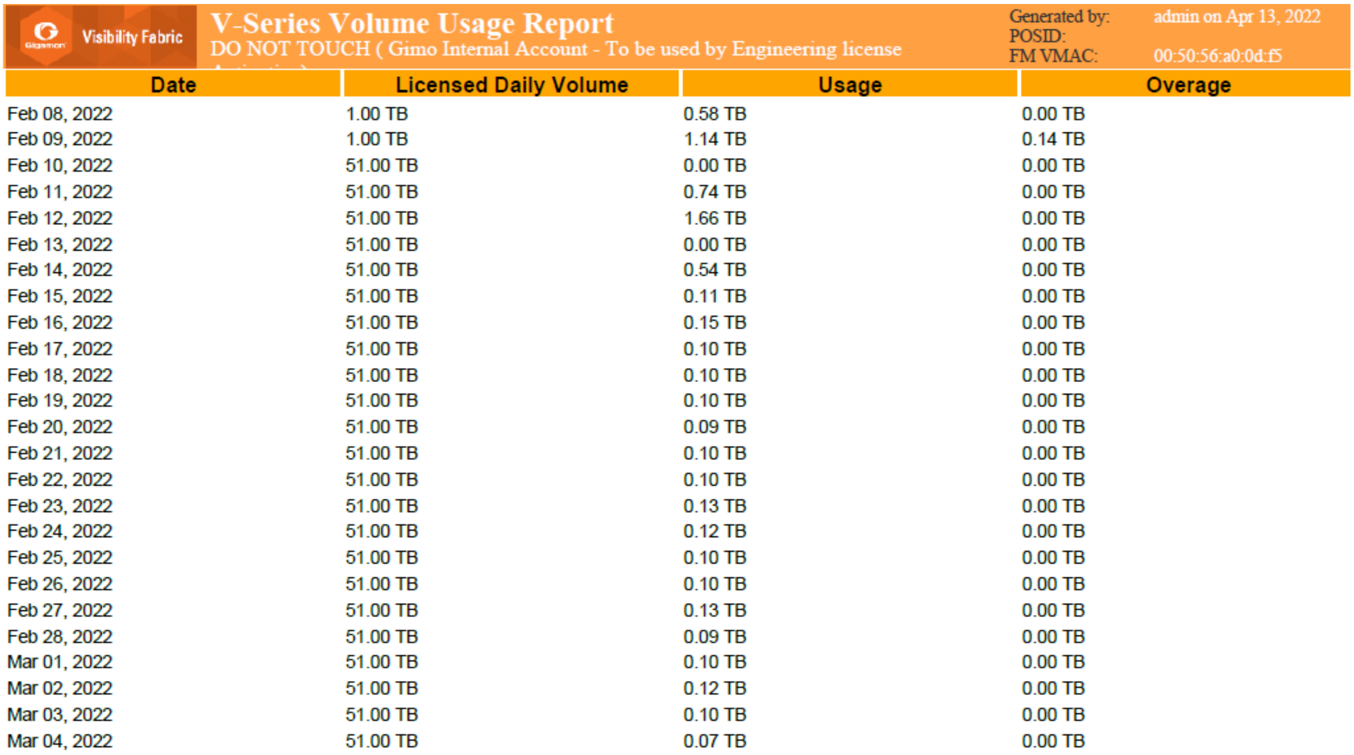


Volume Usage: Summary

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

1 / 4



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 anextension 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 standardkeys, 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=3137303130363030303030305a
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=2f433d55532f4f3d4469676943657274420496e632f4f553d7777772e64
69676963
6572742e636f6d2f434e3d446967694365727420534841322048696768204173737572616e636
52053657276 6572204341 GigamonMdataSslCertSubCommonName=*.stickyadstv.com
GigamonMdataSslSub=2f433d55532f53543d4e657720596f726b2f4c3d4e657720596f726b2f4f3
d4672656
```

5776865656c204d6564696120496e632f4f553d4672656576865656c2f434e3d2a2e737469636b7961647
37 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	Authentication Type
Default Ports	Open Ports in GigaVUE-FM in the GigaVUE-FM User's Guide
FIPS 140-2 Compliance	FIPS 140-2 Compliance in GigaVUE-FM

FIPS 140-2 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 is compliant with FIPS 140-2 Level 1 and was validated by the National Institute of Standards and Technology (NIST). The certificate number is 4066.

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.

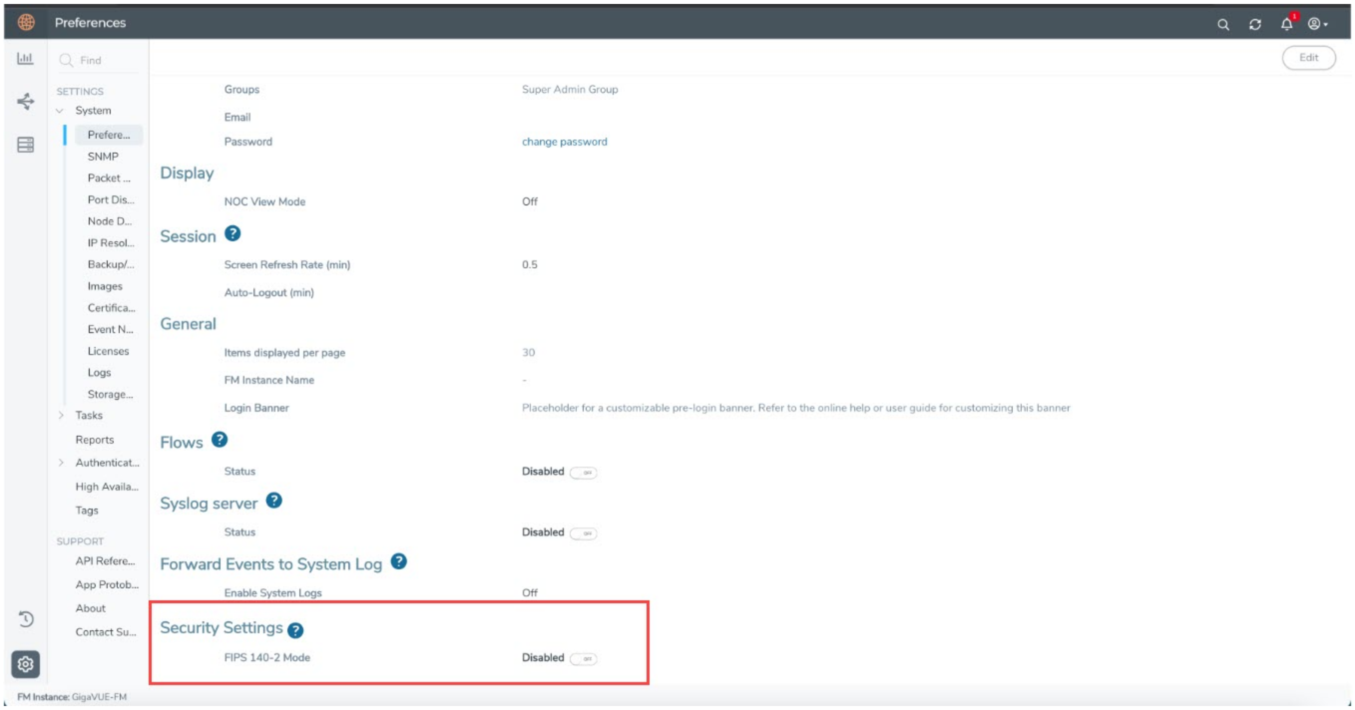
Refer to the Frequently Asked Questions section for further details.

Configure FIPS in GigaVUE-FM

To configure FIPS in GigaVUE-FM:

1. On the left navigation pane, click ⚙ and go to **System** > **Preferences**.
2. Click **Edit**.
3. Under **Security Settings**, the **FIPS 140-2 Mode** option is available. Use the toggle button to enable FIPS.
4. GigaVUE-FM reboots after switching to FIPS mode. Clear the browser cache and cookies so that GigaVUE-FM IDP URL loads without any issues.

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



Groups: Super Admin Group

Email

Password: change password

Display

NOC View Mode: Off

Session

Screen Refresh Rate (min): 0.5

Auto-Logout (min)

General

Items displayed per page: 30

FM Instance Name: -

Login Banner: Placeholder for a customizable pre-login banner. Refer to the online help or user guide for customizing this banner

Flows

Status: Disabled

Syslog server

Status: Disabled

Forward Events to System Log

Enable System Logs: Off

Security Settings

FIPS 140-2 Mode: Disabled

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.

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?

The following software versions are validated for FIPS:

- 5.12.00.01
- 5.16.00, 6.0.00, 6.1.00, 6.2.00, 6.3.00

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.

View Information About GigaVUE-FM

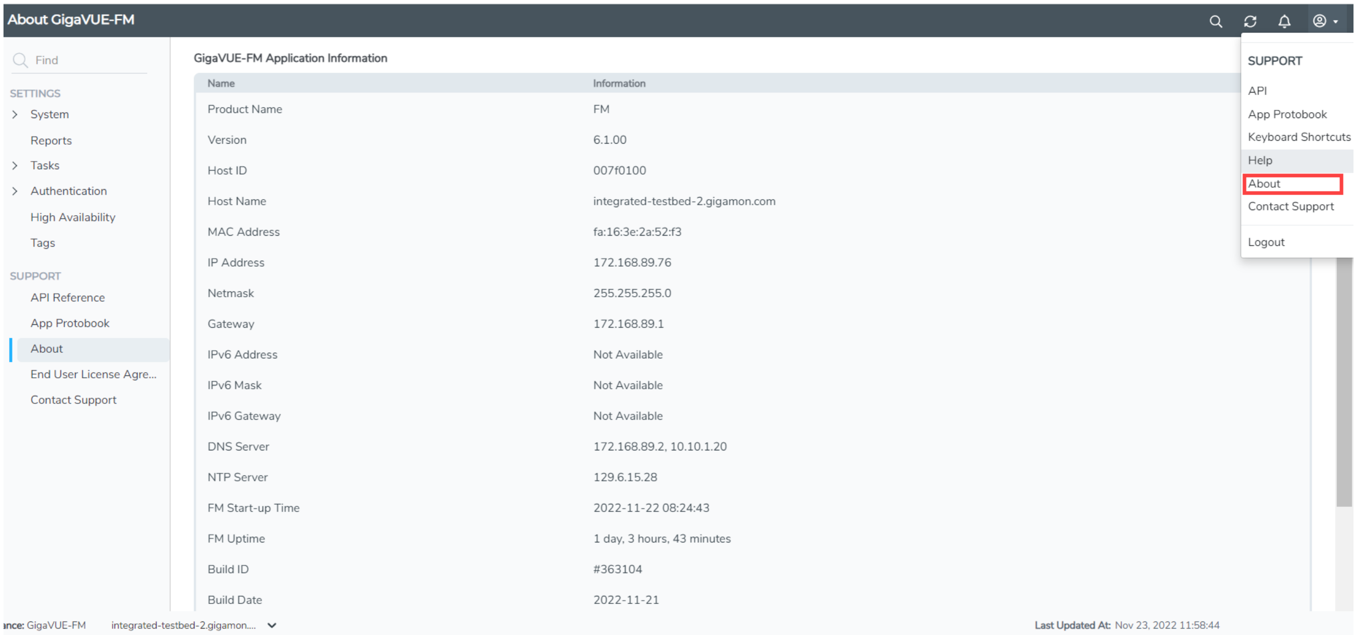
The About page provides product and version information of GigaVUE-FM that you can use when contacting customer support.

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 Adress
- 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



GigaVUE-FM Application Information

Name	Information
Product Name	FM
Version	6.1.00
Host ID	007f0100
Host Name	integrated-testbed-2.gigamon.com
MAC Address	fa:16:3e:2a:52:f3
IP Address	172.168.89.76
Netmask	255.255.255.0
Gateway	172.168.89.1
IPv6 Address	Not Available
IPv6 Mask	Not Available
IPv6 Gateway	Not Available
DNS Server	172.168.89.2, 10.10.1.20
NTP Server	129.6.15.28
FM Start-up Time	2022-11-22 08:24:43
FM Uptime	1 day, 3 hours, 43 minutes
Build ID	#363104
Build Date	2022-11-21

Figure 32 *About Page*

GigaVUE-FM High Availability

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:

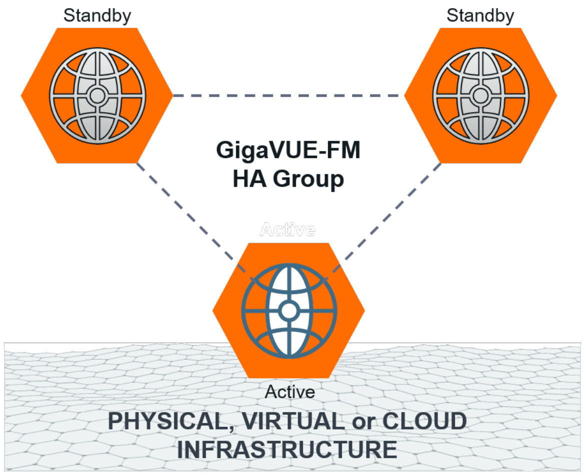
- About GigaVUE-FM High Availability
- Rules, Notes, and Limitations
- Dynamic Addition of GigaVUE-FM Instances to HA Group
- Create and Add GigaVUE-FM Instances to HA Group
- GigaVUE-FM Load Balancer Functionality
- Failover Mechanism
- Troubleshoot GigaVUE-FM High Availability Issues
- Orchestrated 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 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 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.

Supported Platforms

The GigaVUE-FM HA feature is supported on the following platforms:

- VMWare vSphere
- GigaVUE-FM Hardware Appliance
- OpenStack
- VMWare NSX-T Manager

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.
- 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).

- 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.

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 to achieve 3000 nodes. As the HA group is limited to only three GigaVUE-FM instances, there is 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 Elastic Search for features such as Fabric Health Analytics (FHA), 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

[1] GigaVUE-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.

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:

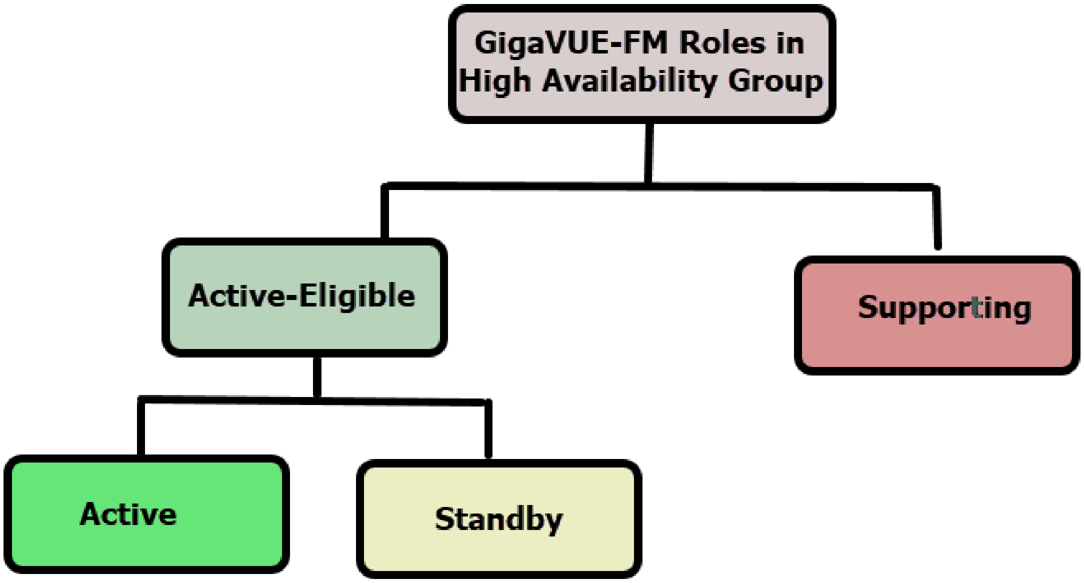
Supporting instances are GigaVUE-FMs that run minimal services, thereby providing more resources to elastic search services. Supporting instances:

- 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.



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:

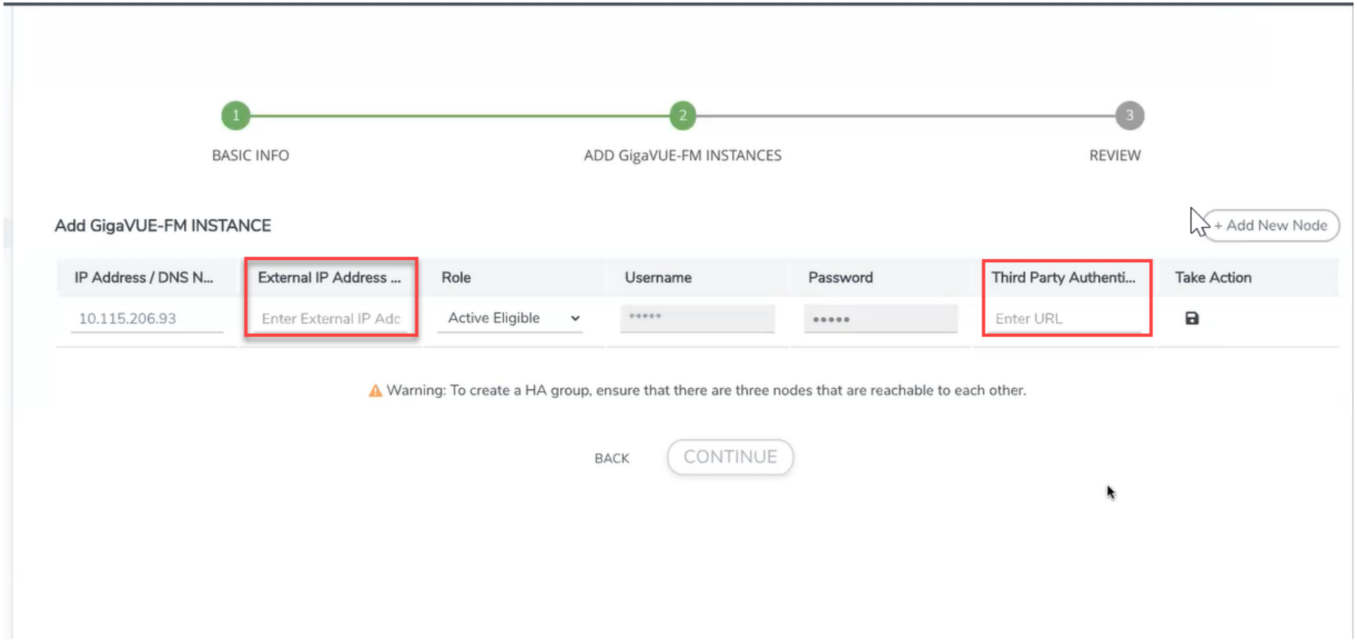
	GigaVUE-FM less than or equal to 5.13.00	GigaVUE-FM 5.14.00
Number of GigaVUE-FM Instances that can be configured in the HA group	Only three GigaVUE-FM instances can be added.	Minimum three. Additional GigaVUE-FM instances can be configured as supporting instances or active-eligible instances.
Status 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 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. 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 of 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. On the left navigation pane, click ⚙ and select **High Availability**.
2. Click **Create**. The High Availability wizard appears.
3. In the **Group Name** field, enter a unique name for the HA group, and then click **Continue**.
4. In the Add GigaVUE-FM Instance page, the details of the GigaVUE-FM instance from which the HA group is created is fetched automatically.

5. Enter the External IP Address and Third-Party Authentication details, if required. Click the **save** icon to save the configuration.



Add GigaVUE-FM INSTANCE

IP Address / DNS N...	External IP Address ...	Role	Username	Password	Third Party Authenti...	Take Action
10.115.206.93	Enter External IP Adc	Active Eligible	*****	•••••	Enter URL	

⚠ Warning: To create a HA group, ensure that there are three nodes that are reachable to each other.

6. Click **Add New Node** to add the second and third GigaVUE-FM instances. Enter the following details.

Field	Description
Status	Status of the GigaVUE-FM instance. Can be Active or Standby.
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) **NOTE:** It is always recommended to use the DNS name while creating the GigaVUE-FM High Availability group.
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 instances**: provides scalability and performance
Username	GigaVUE-FM User Name
Password	GigaVUE-FM GUI password
Third Party Authentication	Third-party authentication URL

7. Click the **Save Node** icon to validate the details entered for the instances.

   Once the first three instances are added to the HA group, the **Continue** button is enabled.

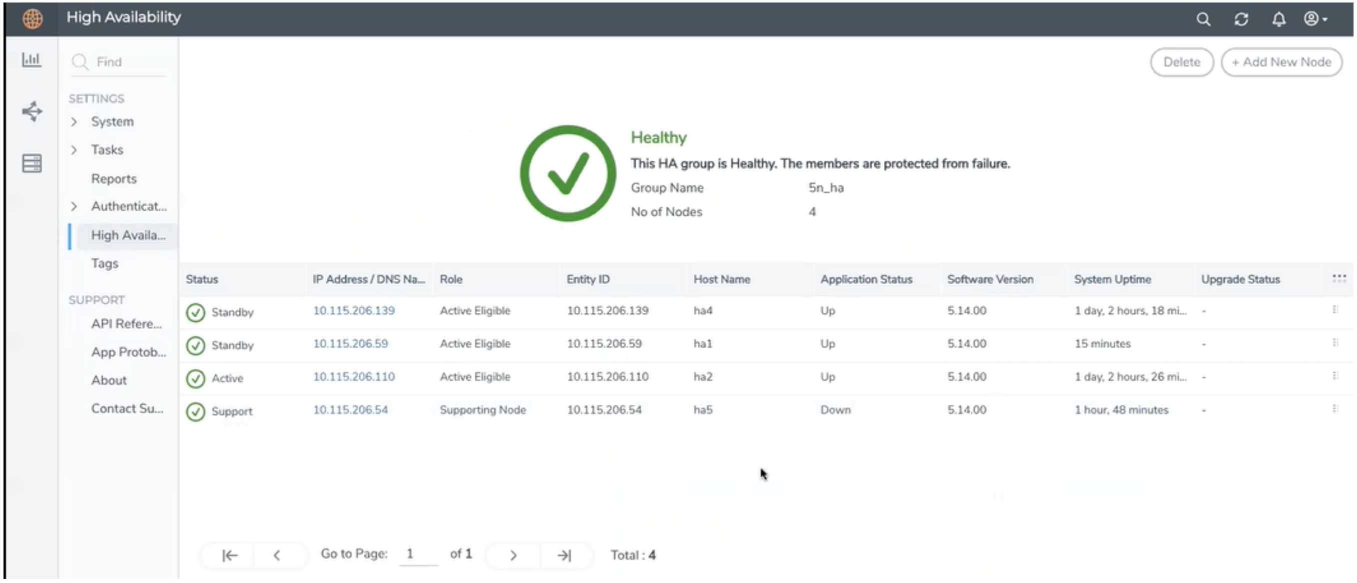
NOTE: When creating a HA group, all the existing data on the first configured GigaVUE-FM instance will be preserved, allowing the system to continue using the data after it is fully set up. However, the data on the subsequent nodes will be lost during the setup.

8. 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 instances

9. Review the details of the GigaVUE-FM instances. Use the **Back** button to go back and change the details.
10. 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:



Healthy

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

Group Name 5n_ha

No of Nodes 4

Status	IP Address / DNS Na...	Role	Entity ID	Host Name	Application Status	Software Version	System Uptime	Upgrade Status
✓ Standby	10.115.206.139	Active Eligible	10.115.206.139	ha4	Up	5.14.00	1 day, 2 hours, 18 mi...	-
✓ Standby	10.115.206.59	Active Eligible	10.115.206.59	ha1	Up	5.14.00	15 minutes	-
✓ Active	10.115.206.110	Active Eligible	10.115.206.110	ha2	Up	5.14.00	1 day, 2 hours, 26 mi...	-
✓ Support	10.115.206.54	Supporting Node	10.115.206.54	ha5	Down	5.14.00	1 hour, 48 minutes	-

Click the ellipses on a GigaVUE-FM instance to perform the following tasks:

- **Edit**: Edit the instance details**.**
- **Reboot**:Reboot a GigaVUE-FMinstance.
- **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 instances**: 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 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 quorum[1] number of instances.

[1] Quorum 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 restore.
	Few active-eligible instances are up (Quorum number of instances are up)	Backup will happen in active instance. 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 would be upgraded first followed by the active-eligible instances.
	All instances are up and running	Upgrade will be initiated in 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	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

	few Supporting instances	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 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 Elastic Search 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 upgrade and once 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 in to MongoDB as the Application Service is down by default (scheduler populates the system information every minute in to 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)

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 GigaVUE-FM GUI footer 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 footer:

- FM Health
- IP Resolver

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 Fabric Manager 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 GetDistribution 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 check up.
- 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 -" :

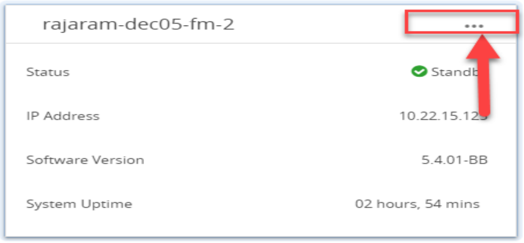
```
curl -XPOST "localhost:4466/fmcs/updateLoadBalancer?pretty"
Response :
{"operation":"success"}
```

> **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 these steps:

1. Login to any GigaVUE-FM instance.
2. On the left navigation pane, click ⚙ and select **High Availability**.
3. Select the standby GigaVUE-FM instance that you want to remove from the HA group.
4. Click the ellipsis on the GigaVUE-FM instance widget in the High Availability page as shown in Figure 33Disabling GigaVUE-FM Instance.



rajaram-dec05-fm-2 ...

Status Standb
IP Address 10.22.15.12
Software Version 5.4.01-BB
System Uptime 02 hours, 54 mins

Figure 33 *Disabling GigaVUE-FM Instance*

5. 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**.

Disassemble GigaVUE-FM High Availability Group

To completely disassemble the GigaVUE-FM HA group:

1. Login to the active GigaVUE-FM instance.

   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. On the left navigation pane, click ⚙ and select **High Availability**.
3. Click the ellipsis on the GigaVUE-FM instance widget in the High Availability page.
4. 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 the do not backup the 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 with in 3 days (72 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.

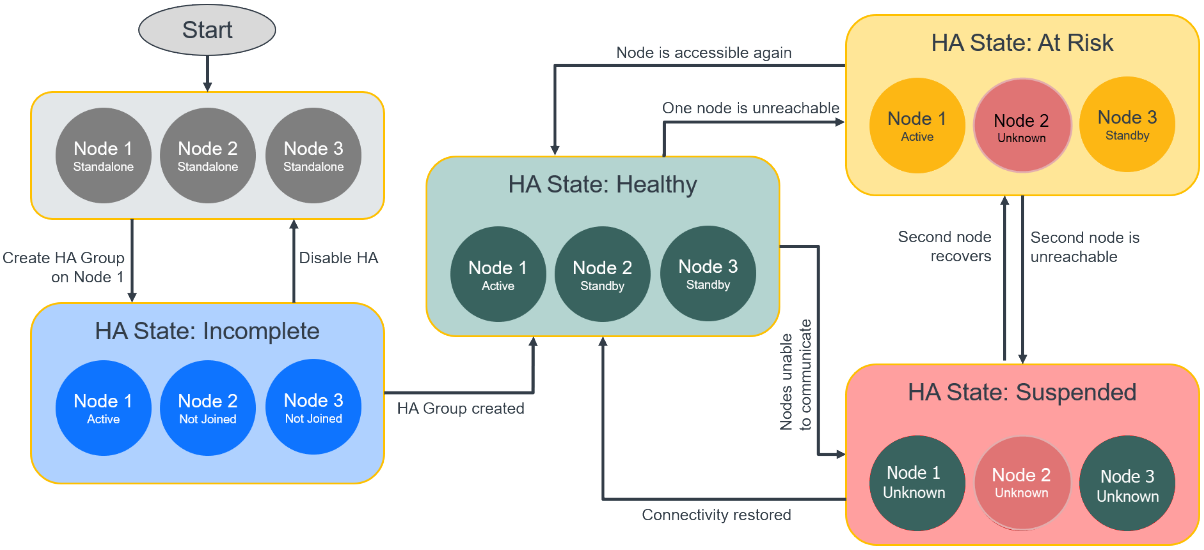


Figure 34 *High Availability States*

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:

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 (On the left navigation pane, click ⚙ and select **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.
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	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
license	
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 section in the *GigaVUE-FM Installation and Upgrade Guide* for more details.

> **NOTE:** Orchestrated Upgrade of GigaVUE-FM instances in a HA group is supported from software version 5.10.01. For GigaVUE-FM software version 5.10.00 and above, it is recommended only to use the orchestrated upgrade procedure to upgrade the GigaVUE-FM instances in a HA group.

Prerequisites

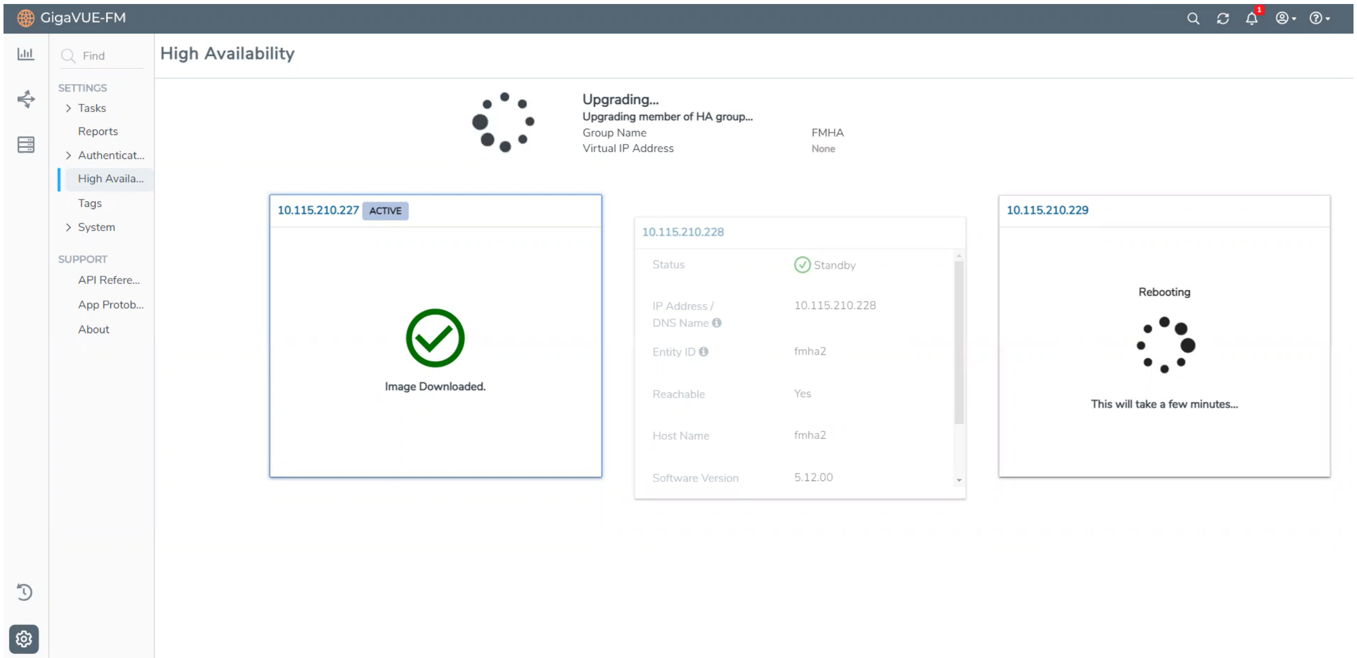
Before upgrading the GigaVUE-FM instances in a High Availability group, ensure the following:

- 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.

Steps

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.



High Availability

Upgrading...
Upgrading member of HA group...
Group Name FMHA
Virtual IP Address None

10.115.210.227 ACTIVE
Image Downloaded.

10.115.210.228
Status: Standby
IP Address / DNS Name: 10.115.210.228
Entity ID: fmha2
Reachable: Yes
Host Name: fmha2
Software Version: 5.12.00

10.115.210.229
Rebooting
This will take a few minutes...

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 f 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.

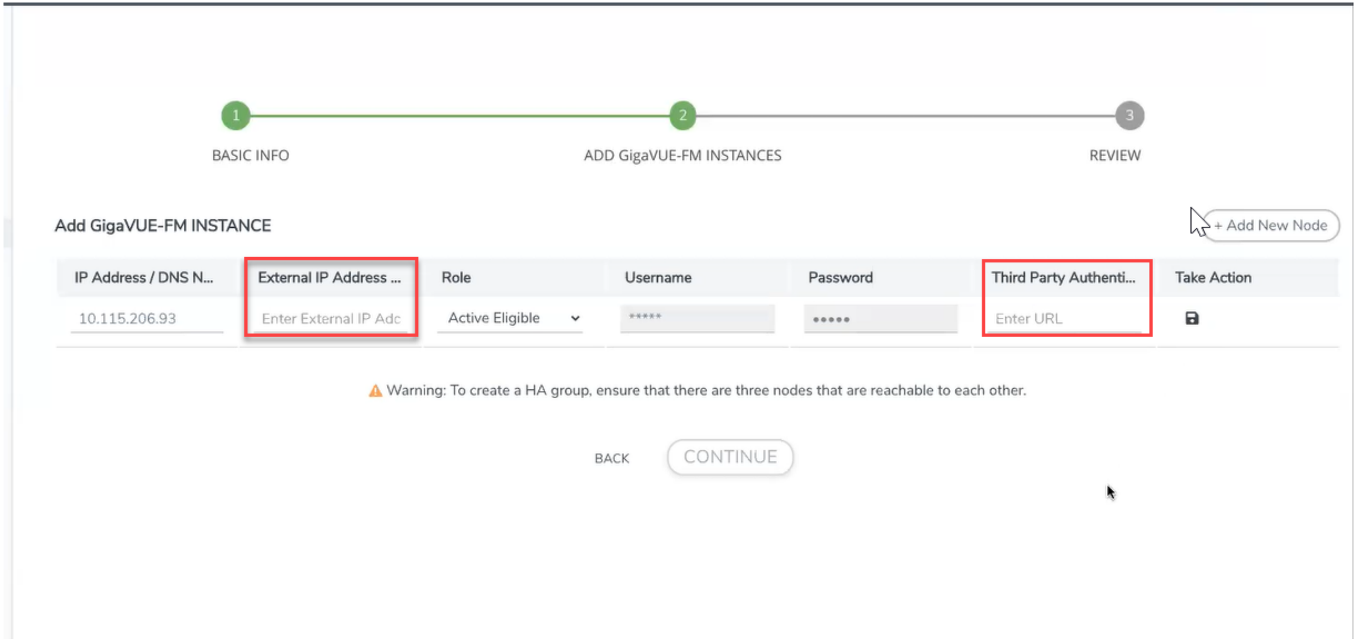
This ensures that the GigaVUE-FM High Availability group is always accessible.

Create and Add GigaVUE-FM Instances to HA Group

To add instances and to configure the HA group:

1. On the left navigation pane, click ⚙ and select **High Availability**.
2. Click **Create**. The High Availability wizard appears.
3. In the **Group Name** field, enter a unique name for the HA group, and then click **Continue**.
4. In the Add GigaVUE-FM Instance page, the details of the GigaVUE-FM instance from which the HA group is created is fetched automatically.

5. Enter the External IP Address and Third-Party Authentication details, if required. Click the **save** icon to save the configuration.



Add GigaVUE-FM INSTANCE

IP Address / DNS N...	External IP Address ...	Role	Username	Password	Third Party Authenti...	Take Action
10.115.206.93	Enter External IP Adc	Active Eligible	*****	•••••	Enter URL	

⚠ Warning: To create a HA group, ensure that there are three nodes that are reachable to each other.

6. Click **Add New Node** to add the second and third GigaVUE-FM instances. Enter the following details.

Field	Description
Status	Status of the GigaVUE-FM instance. Can be Active or Standby.
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) **NOTE:** It is always recommended to use the DNS name while creating the GigaVUE-FM High Availability group.
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 instances**: provides scalability and performance
Username	GigaVUE-FM User Name
Password	GigaVUE-FM GUI password
Third Party Authentication	Third-party authentication URL

7. Click the **Save Node** icon to validate the details entered for the instances.

   Once the first three instances are added to the HA group, the **Continue** button is enabled.

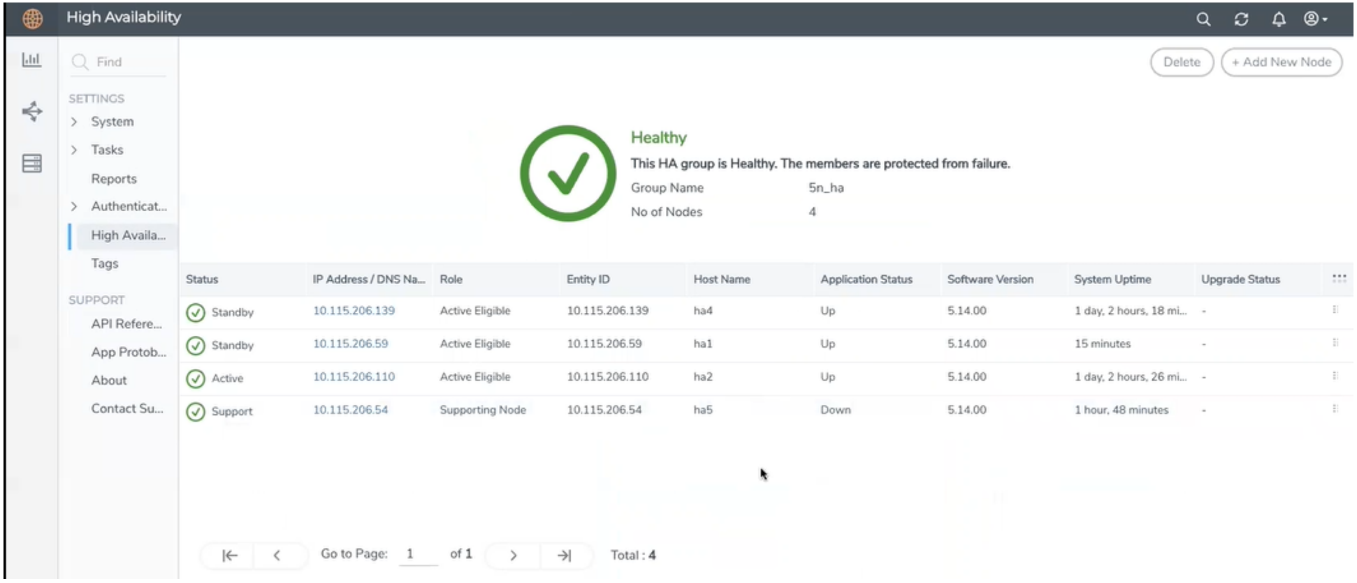
> **NOTE:** When creating a HA group, all the existing data on the first configured GigaVUE-FM instance will be preserved, allowing the system to continue using the data after it is fully set up. However, the data on the subsequent nodes will be lost during the setup.

8. 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 instances

9. Review the details of the GigaVUE-FM instances. Use the **Back** button to go back and change the details.
10. 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:



Healthy

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

Group Name 5n_ha

No of Nodes 4

Status	IP Address / DNS Na...	Role	Entity ID	Host Name	Application Status	Software Version	System Uptime	Upgrade Status
✓ Standby	10.115.206.139	Active Eligible	10.115.206.139	ha4	Up	5.14.00	1 day, 2 hours, 18 mi...	-
✓ Standby	10.115.206.59	Active Eligible	10.115.206.59	ha1	Up	5.14.00	15 minutes	-
✓ Active	10.115.206.110	Active Eligible	10.115.206.110	ha2	Up	5.14.00	1 day, 2 hours, 26 mi...	-
✓ Support	10.115.206.54	Supporting Node	10.115.206.54	ha5	Down	5.14.00	1 hour, 48 minutes	-

Click the ellipses on a GigaVUE-FM instance to perform the following tasks:

- **Edit**: Edit the instance details**.**
- **Reboot**:Reboot a GigaVUE-FMinstance.
- **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 instances**: 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 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 quorum[1] number of instances.

[1] Quorum 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 restore.
	Few active-eligible instances are up (Quorum number of instances are up)	Backup will happen in active instance. 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 would be upgraded first followed by the active-eligible instances.
	All instances are up and running	Upgrade will be initiated in 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	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

	few Supporting instances	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 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 Elastic Search 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 upgrade and once 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 in to MongoDB as the Application Service is down by default (scheduler populates the system information every minute in to 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)

Configure GigaVUE-FM High Availability in 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. Refer to the Gigamon Containerized Broker Guidefor details on how to deploy GigaVUE-FM in Gigamon Containerized Broker.

Configure GigaVUE-FM High Availability in OpenStack Environment

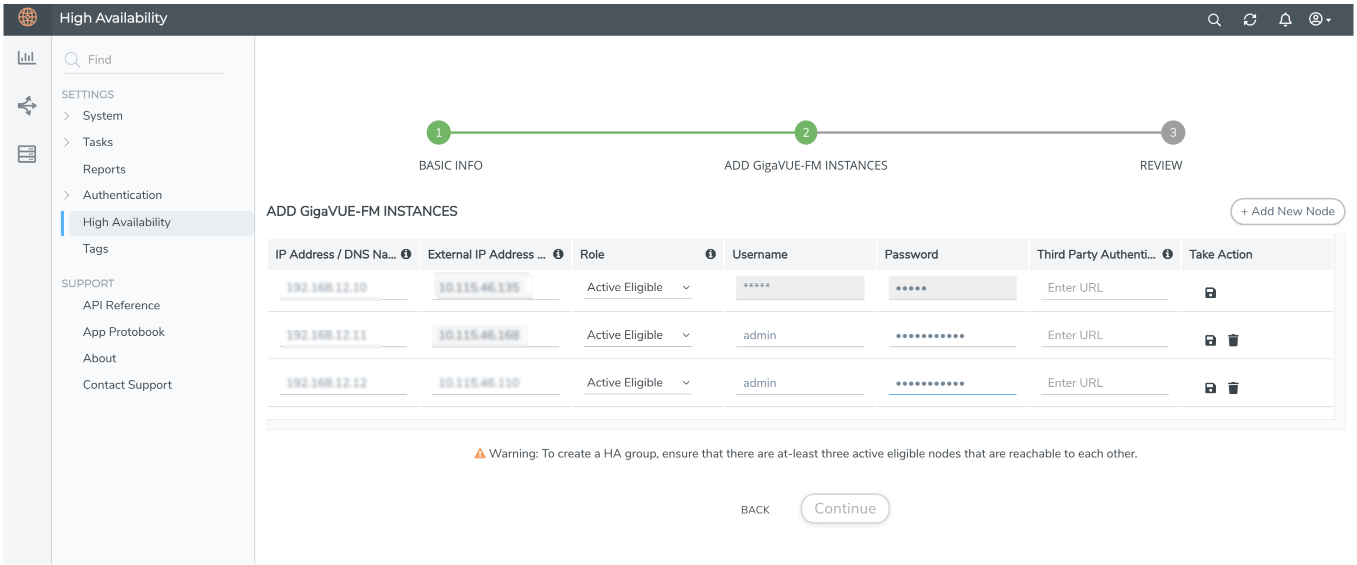
GigaVUE-FM High Availability group can be configured in an OpenStack Environment in which the three GigaVUE-FM instances are launched and deployed in the OpenStack environment. Refer to the *GigaVUE Cloud Suite for OpenStack guide* for details on how to deploy GigaVUE-FM in OpenStack.

Before configuring HA in OpenStack, you must ensure the following:

- The three GigaVUE-FM instances must be in the same OpenStack environment and must be reachable to each other.
- The internal and external IP addresses of GigaVUE-FM must be assigned at the time of configuring GigaVUE-FM in OpenStack:
    - Internal IP Address (Private/Local IP): Reachable only within the private Network.
    - External IP Address (Public/Floating IP): Reachable from user network.

The process of configuring a High Availability group in OpenStack environment is similar to the existing configuration steps described in GigaVUE-FM High Availability. When configuring FM HA group in OpenStack:

- Use the internal IP address for communication between the GigaVUE-FMs and to configure the HA.
- Use the external IP address for accessing the GigaVUE-FM HA from outside the internal network.



ADD GigaVUE-FM INSTANCES

IP Address / DNS Na...	External IP Address ...	Role	Username	Password	Third Party Authenti...	Take Action
[redacted]	[redacted]	Active Eligible	*****	•••••	Enter URL	
[redacted]	[redacted]	Active Eligible	admin	•••••••••••	Enter URL	
[redacted]	[redacted]	Active Eligible	admin	•••••••••••	Enter URL	

⚠ Warning: To create a HA group, ensure that there are at-least three active eligible nodes that are reachable to each other.

NOTE: Use of Virtual IP address is not supported in GigaVUE-FM HA in OpenStack.

Disassemble GigaVUE-FM Instances in OpenStack Environment

To disassemble the GigaVUE-FM instances in a High Availability group, refer to the Disassemble GigaVUE-FM High Availability Group section for details.

After the GigaVUE-FM instances in the High Availability group are disassembled, the GigaVUE-FM instances will be restored to the default configuration. However, you must ensure to delete the fabric nodes on the monitoring domains launched by GigaVUE-FM on the respective tenants.

Configure GigaVUE-FM High Availability in VMware NSX-T Manager

GigaVUE-FM High Availability group can be configured in VMware NSX-T Manager in which a minimum of three GigaVUE-FM instances are launched and deployed in the VMware ESXi and managed by VMware NSX-T Manager. Refer to the *GigaVUE Cloud Suite for VMware—GigaVUE V Series Guide* for details on how to deploy GigaVUE-FM in VMware NSX-T.

Before configuring HA in VMware NSX-T Manager, you must ensure the following:

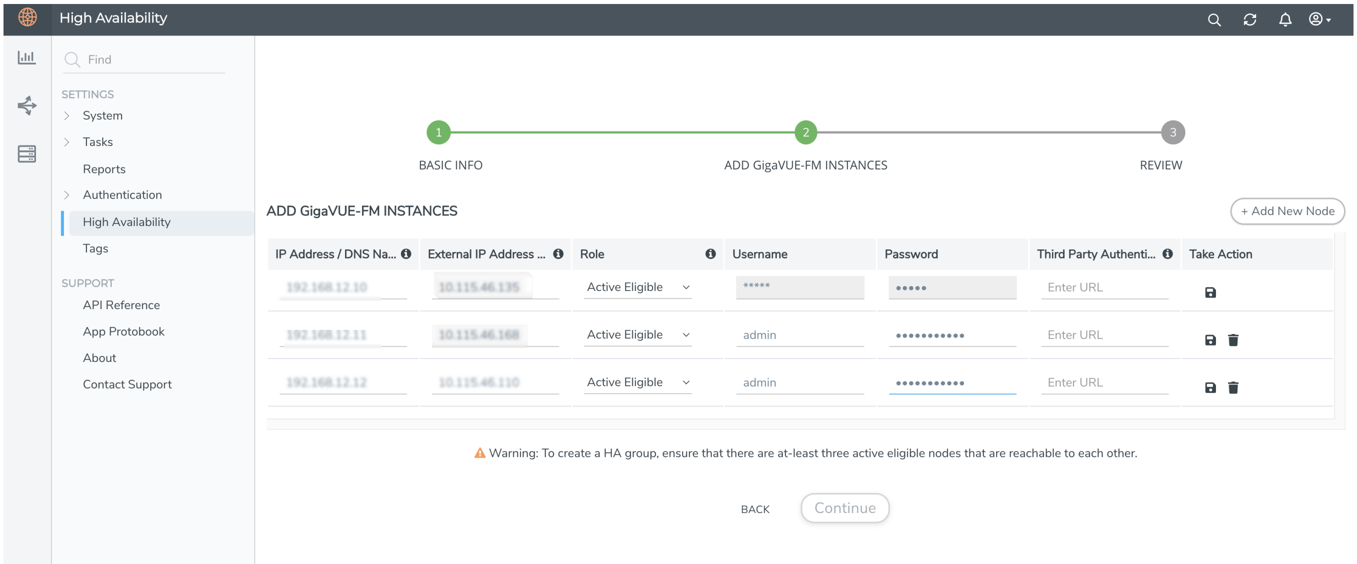
- The three GigaVUE-FM instances must be in the same VMware NSX-T Manager and must be reachable to each other.

- GigaVUE-FM has two interfaces, one is for VMware ESXi and the other one is for VMware NSX-T. The internal address of GigaVUE-FM must be assigned at the time of configuring GigaVUE-FM in VMware NSX-T Manager and the external address of GigaVUE-FM must be assigned at the time of configuring GigaVUE-FM in VMware ESXi platform:
  - Internal IP Address (Private/Local IP): Reachable only within the private Network.
  - External IP Address (Public/Floating IP): Reachable from user network.

> **NOTE:** External IP address is optional. If the internal IP address is accessible from the user network, then you can exclude the external IP address.

The process of configuring a High Availability group in VMware NSX-T Manager is similar to the existing configuration steps described in GigaVUE-FM High Availability. When configuring FM HA group in VMware NSX-T Manager:

- Use the internal IP address for communication between the GigaVUE-FMs and to configure the HA.
- Use the external IP address for accessing the GigaVUE-FM HA from outside the internal network.



ADD GigaVUE-FM INSTANCES

IP Address / DNS Na...	External IP Address ...	Role	Username	Password	Third Party Authenti...	Take Action
192.168.12.10	10.115.46.135	Active Eligible	*****	•••••	Enter URL	
192.168.12.11	10.115.46.168	Active Eligible	admin	•••••••••••	Enter URL	
192.168.12.12	10.115.46.110	Active Eligible	admin	•••••••••••	Enter URL	

⚠ Warning: To create a HA group, ensure that there are at-least three active eligible nodes that are reachable to each other.

> **NOTE:** Use of Virtual IP address and IPv6 address is not supported in GigaVUE-FM HA in VMware NSX-T Manager.

Disassemble GigaVUE-FM Instances in VMware NSX-T Manager

To disassemble the GigaVUE-FM instances in a High Availability group, refer to the Disassemble GigaVUE-FM High Availability Group section for details.

After the GigaVUE-FM instances in the High Availability group are disassembled, the GigaVUE-FM instances will be restored to the default configuration. However, you must ensure to delete the fabric nodes on the monitoring domains launched by GigaVUE-FM on the respective tenants.

Administer GigaVUE Nodes

Featured topics:

- Introducing the GigaVUE Nodes
- Access Nodes From GigaVUE-FM
- Get Started with GigaVUE Nodes
- Configure Security Options
- License GigaVUE TA Series
- Chassis
- Manage Roles and Users—GigaVUE-OS
- Reboot and Upgrade Options
- Backup and Restore
- Use SNMP
- Monitor Utilization

Introducing the GigaVUE Nodes

This chapter introduces the GigaVUE HC Series and the GigaVUE TA Series Visibility Platform nodes, describes their features and functions, and provides an orientation to the physical layout of the models. Refer to the following sections for details:

- About the GigaVUE HC Series and TA Series
- GigaVUE HC Series Features and Benefits

About the GigaVUE HC Series and TA Series

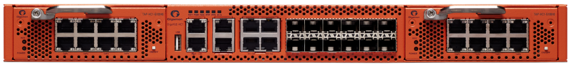
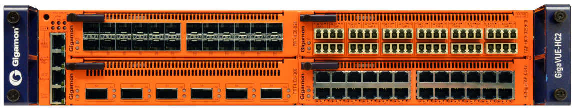
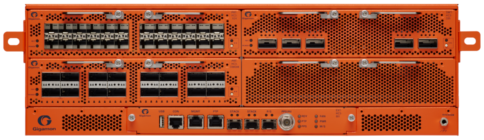
The GigaVUE HC Series delivers performance and intelligence in each of its Traffic Visibility Platform nodes, with port density and speeds that scale to your needs, from 1Gb to 100Gb. With an intuitive web-based interface (GigaVUE-FM) and a powerful GigaVUE-OS, the Visibility Platform is able to replicate, filter, and selectively forward network traffic to monitoring, management, and security tools.

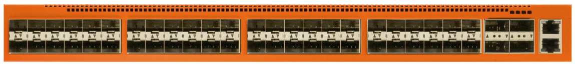
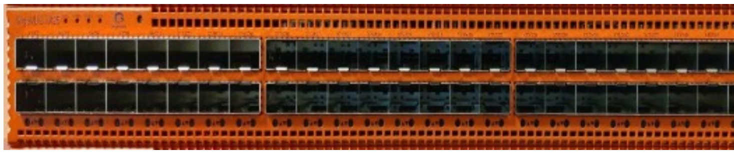
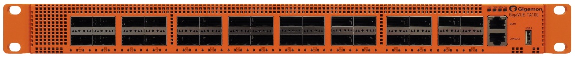
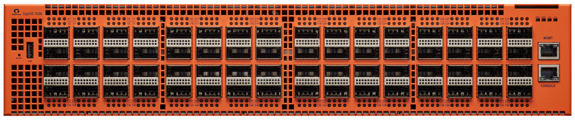
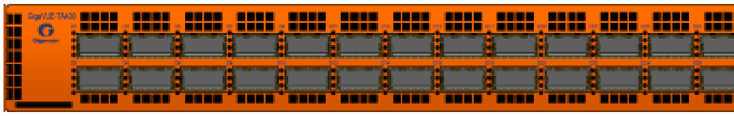
The GigaVUE HC Series and TA Series include the following models that run GigaVUE-OS:

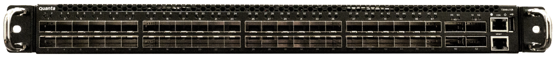
- GigaVUE-HC1
- GigaVUE-HC2
- GigaVUE-HC3
- GigaVUE-TA10

- GigaVUE-TA25
- GigaVUE-TA40
- GigaVUE-TA100
- GigaVUE-TA100-CXP
- GigaVUE-TA200
- GigaVUE-TA400
- Certified Traffic Aggregation White Box

> **NOTE:** This document describes how to configure and operate the GigaVUE-OS for GigaVUE HC Series and TA Series nodes.

GigaVUE-HC1	▪ **1RU Footprint** ▪ **Built-in GigaSMART functionality** ▪ **Standard GigaVUE-OS CLI and GigaVUE-FM GUI** ▪ **Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes**	
GigaVUE-HC2	▪ **2RU Footprint** ▪ **Four front-facing bays for port, TAP, BPS, and GigaSMART front modules** ▪ **One rear bay for a GigaSMART rear module** ▪ **Standard GigaVUE-OS CLI and GigaVUE-FM GUI** ▪ **Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes**	
GigaVUE-HC3	▪ **3RU Footprint** ▪ **Four Module Slots (Bays)** ▪ **Internal Control Card** ▪ **Extension Board** ▪ **Dedicated Cluster Management Port** ▪ **Standard GigaVUE-OS CLI and GigaVUE-FM GUI** ▪ **Supports all GigaVUE-HC3 Modules** ▪ **Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes**	
GigaVUE-TA10	▪ **1RU Footprint** ▪ **Flexible 10Gb/40Gb Modes for**	

	40Gb Ports ▪ Standard GigaVUE-OS CLI and GigaVUE-FM GUI ▪ Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes	
GigaVUE-TA25	▪ 1 RU Footprint ▪ 48 25Gb/10Gb/1Gb ports and 8 100Gb/40Gb ports ▪ Standard GigaVUE-OS CLI and GigaVUE-FM GUI ▪ Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes	
GigaVUE-TA40	▪ 1RU Footprint ▪ Flexible 10Gb/40Gb Modes for 40Gb Ports ▪ Standard GigaVUE-OS CLI and GigaVUE-FM GUI ▪ Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes	
GigaVUE-TA100	▪ 1RU Footprint ▪ 32 x 100Gb/40Gb Ports ▪ Standard GigaVUE-OS CLI and GigaVUE-FM GUI ▪ Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes	
GigaVUE-TA100 CXP	▪ 1RU Footprint ▪ 20 100Gb CXP Ports, 8 100Gb QSFP28 Ports ▪ Standard GigaVUE-OS CLI and GigaVUE-FM GUI	
GigaVUE-TA200	▪ 2RU Footprint ▪ 64x 100Gb/40Gb Ports ▪ Standard GigaVUE-OS CLI and GigaVUE-FM GUI ▪ Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes	
GigaVUE-TA400	▪ 1RU Footprint ▪ 32 400Gb/ 100Gb/40Gb QSFP-DD/ QSFP28/QSFP+ ports ▪ Standard GigaVUE-OS CLI and GigaVUE-FM GUI	

	▪ Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes	
Certified Traffic Aggregation White Box	▪ 1RU Footprint ▪ 10Gb/40Gb Ports ▪ Standard GigaVUE-OS CLI and GigaVUE-FM GUI ▪ Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes	

Notes on TA Series Nodes

- A twenty-four (24) port GigaVUE-TA10 version, called the GigaVUE-TA10A is available with only the first 24 1Gb/10Gb ports enabled. A license is needed to expand a GigaVUE-TA10A to include all 48 1Gb/10Gb ports as well as the four (4) 40Gb ports.
- On the GigaVUE-TA100, only the first 16 out of 32 100Gb ports are enabled. Two port licenses are available to enable an additional 8 or 16 ports to expand from 16 ports to 24 ports or from 16 ports to 24 ports and then to 32 ports.
- On the GigaVUE-TA200, only the first 32 out of 64 100Gb ports are enabled. A port license is available to enable an additional 32 ports.
- The ports on the GigaVUE-TA100 can be used as network, tool, or hybrid ports.
- For more information about the TA Series nodes, refer to the *GigaVUE TA Series Hardware Installation Guide*.

GigaVUE HC Series Features and Benefits

Capable of port-to-port full line rate performance with minimal packet latency, the GigaVUE HC Series uses patented Flow Mapping® techniques to aggregate, replicate, and direct traffic flows, providing dynamic connectivity for 400Gb, 200Gb, 100Gb, 40Gb, 10Gb, or 1Gb monitor, compliance, and archival tools, including:

- Intrusion Detection Systems
- Protocol Analyzers
- VoIP Analyzers
- Application Performance Monitors
- Stream-to-Disk Data Recorders

Any Packet, Any Destination

The GigaVUE HC Series nodes provide a powerful graphical user interface that lets you unobtrusively acquire and map traffic from multiple data sources to multiple tools, including the following common scenarios:

Mapping(Any-to-Any)	Direct traffic from any network port to any tool port. Use map rules to send different types of traffic to different tool ports.
Aggregation(Many-to-Any)	Aggregate traffic from multiple links to deliver a network-wide view to any tool. Merge Tx and Rx traffic into a single tool interface.
Multicasting(Any-to-Many)	Multicast filtered or unfiltered, singular or aggregated traffic to multiple tools.

The Gigamon Visibility Platform

GigaVUE Visibility Platform nodes and management software form the Gigamon Visibility Platform, providing passive monitoring of mission critical networks. The Visibility Platform solves access problems, improves network performance and uptime, and saves capital, operation and maintenance costs.

The Visibility Platform addresses many common network management issues, including security, compliance, forensics review, application performance, and VoIP QoS, among others. Once data is acquired from multiple SPAN ports or TAPs, it can be multicast to multiple tools, aggregated to a few consolidated tools, and filtered or divided across many instances of the same tools.

You can think of the Visibility Platform as a data socket that provides immediate access for ad hoc tool deployment without impact to the production network. Gigamon’s Visibility Platform nodes accommodate the growing number of network monitoring tools and network security tools. Figure 1The Gigamon Visibility Platform summarizes these features.

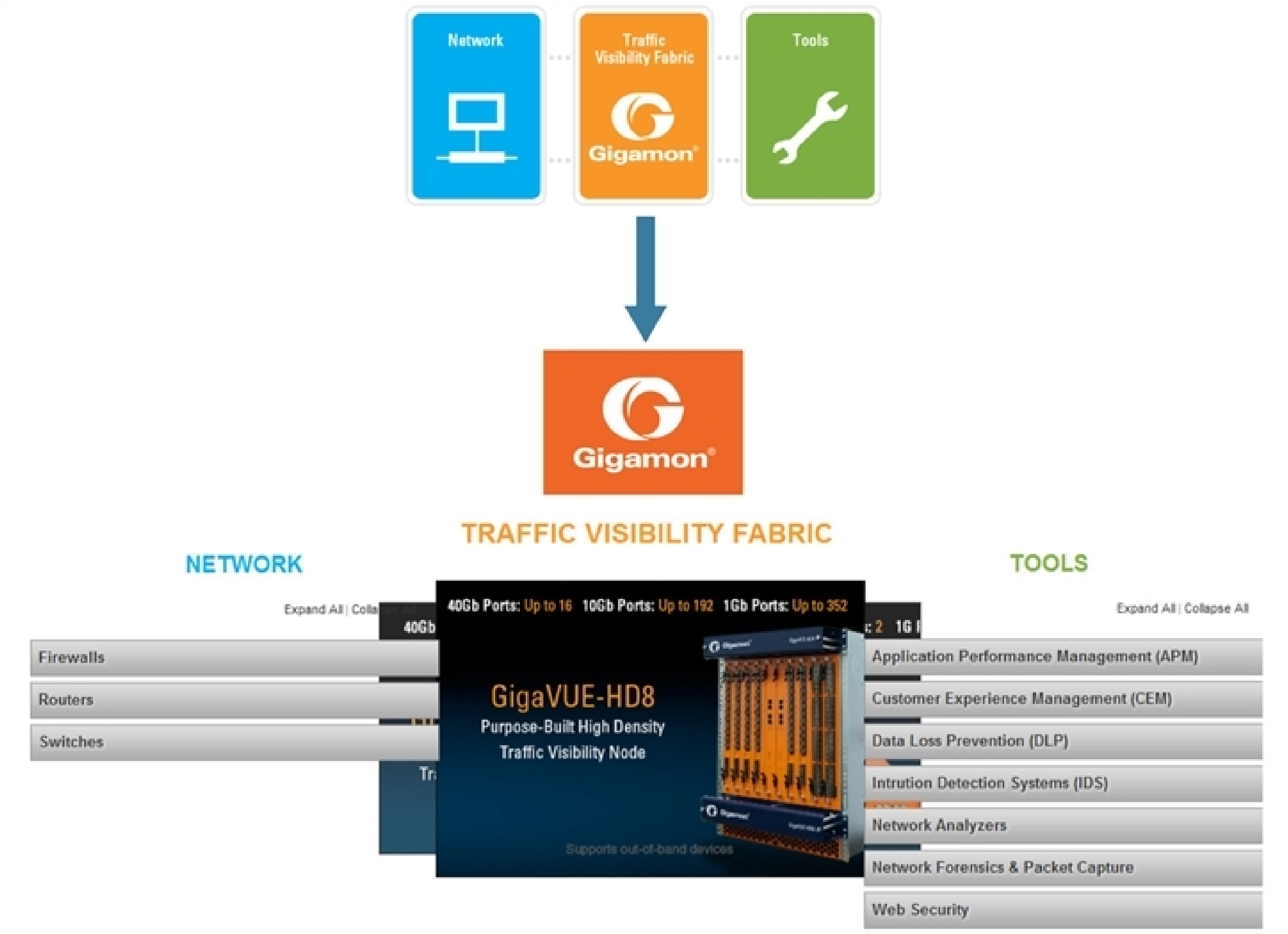

Network
Traffic Visibility Fabric
Gigamon
Tools
Gigamon
TRAFFIC VISIBILITY FABRIC
NETWORK
TOOLS
Expand All | Colla
40Gb Ports: Up to 16 10Gb Ports: Up to 192 1Gb Ports: Up to 352
Firewalls
Routers
Switches
GigaVUE-HD8
Purpose-Built High Density Traffic Visibility Node
Supports out-of-band devices
Expand All | Collapse All
Application Performance Management (APM)
Customer Experience Management (CEM)
Data Loss Prevention (DLP)
Intrution Detection Systems (IDS)
Network Analyzers
Network Forensics & Packet Capture
Web Security

Figure 1 *The Gigamon Visibility Platform*

Features and Benefits

The following table lists the major features and benefits of the GigaVUE HC Series:

Benefit	Descriptions
CLI Management	Configure the operations of the GigaVUE HC Series node using a command-line interface, the GigaVUE-OS: ● Local access over the serial **console** port on control card. ● Remote network access using SSH2 over the 10/100/1000 Ethernet **Mgmt** port on control card. ● Secure access to the CLI, either through local authentication or optional RADIUS/TACACS+/LDAP support.
Scalable Port Density	Use the line cards that best suit your port density needs. Depending on the line cards installed in the node, you can have as many as 256 10Gb ports (a node fully populated with PRT-H00-Q02X32 line cards). In addition, the GigaVUE HC Series node evolves with network speeds, including line cards with 40Gb and 100Gb support for data centers and service providers.

Benefit	Descriptions
Cluster Support	Connect multiple GigaVUE HC Series nodes in a self-healing, intelligent cluster. When you create a cluster of GigaVUE HC Series nodes, available ports appear as a unified fabric, with ingress ports able to send packets to any egress port, regardless of its physical chassis. Nodes are connected through stack links consisting of one or more 10Gb, 40Gb, or 100Gb ports. Cluster management traffic can be carried out-of-band on its own network or inband on stack links.
Share SPAN Ports	Connect a SPAN port to a network port on the GigaVUE HC Series node and multicast that traffic to multiple different tool ports, giving multiple different tools access to the same data. Use flow mapping to send specific traffic to different tool ports, ensuring that each tool sees the data that best suits its individual strengths. You can move, add, and reconfigure tools at will without affecting production networks.
Aggregate Links	Send the data from multiple different network ports to one or more tool ports, allowing you to combine traffic from multiple access points into a single stream for analysis.
Flow Mapping®	The GigaVUE HC Series Flow Mapping® feature lets you direct traffic arriving on network ports to one or more tool ports based on different packet criteria, including VLAN IDs, IP addresses, port ranges, protocols, bit patterns, and so on. You can drop some traffic intentionally using drop rules and also create a shared-collector destination for any packets not matching the maps configured on a shared set of network ports.
GigaVUE-FM Support	Deploy Gigamon's umbrella fabric management system, GigaVUE-FM to manage all of your GigaVUE HC Series, GigaVUE TA Series, and G Series nodes. The GigaVUE HC Series is fully compatible with GigaVUE-FM, allowing you to centralize deployment of images, configuration backups, and alert management.
Role-Based Access	Role-based access makes it easy to share the Gigamon Visibility Platform between different groups of users with different needs. Administrators can assign egress ports to different groups of users. Users can then select the traffic they need to see from shared ingress ports. Administrators adjust map priority to ensure that each packet is delivered to the correct destination.
Cisco-Style CLI	The GigaVUE HC Series node's CLI offers a similar style to the familiar Cisco interface, minimizing relearning for IT professionals.
Command Abbreviation	Type only as many letters of a command as are needed to positively differentiate from other available commands. For example, you only need to type **co t** to enter Configure mode, not the full **configure terminal** command (although that works, too!).
SNMP Support	Rely on secure SNMP v3 access to the onboard SNMP agent as well as v1/v2 SNMP traps.

Benefit	Descriptions
Email Notifications	Use email alerts for proactive notification of a wide variety of GigaVUE events, helping you keep tabs on system status in real time.
Modularized Design	Hot-pluggable line cards, power supplies, and fan trays allow for flexibility and future growth. For GigaVUE-HC1, GigaVUE-HC2, and GigaVUE-HC3, the modules are interchangeable between the front bays of each chassis type, but not with each other, due to form and factor.
Flexible 10Gb/1Gb Support	All 10Gb ports in GigaVUE HC Series line cards can be used with 1Gb Ethernet media by inserting a copper or optical SX/LX SFP instead of an SFP+. Interoperability and support are ensured by purchasing SFPs from Gigamon – transceivers purchased from other vendors are not supported.

Access Nodes From GigaVUE-FM

You can access Gigamon nodes that have been added to GigaVUE-FM from the GigaVUE-FM interface.

To access a node from the GigaVUE-FM interface:

1. On the left navigation pane, click 🗄 under **Physical** select **Nodes**. This displays the list of Devices/Cluster Nodes managed by this instance of GigaVUE-FM.
2. Click the Cluster ID of any node to open the node.

   Once you are in the node, you will be able to access the **System** menu in the left navigation pane and perform the administration tasks in the node.

Refer to the following topics for detailed information:

- Chassis for a detailed snapshot of a selected GigaVUE nodes.
- Manage Roles and Users—GigaVUE-OS to manage roles and users in GigaVUE-FM and to assign access permissions.
- Reboot and Upgrade Options to upload and upgrade images on the GigaVUE node.
- Backup and Restore to learn how to back up and restore the configuration of the GigaVUE node.
- Use SNMP to learn how to use the SNMP features on the GigaVUE node.

Get Started with GigaVUE Nodes

This chapter describes the following configuration tasks that you can complete when you access the nodes from GigaVUE-FM:

- Initial User Account Configuration (Optional)
- Configure the Host Name
- Configure Time Options
- Configure Logging

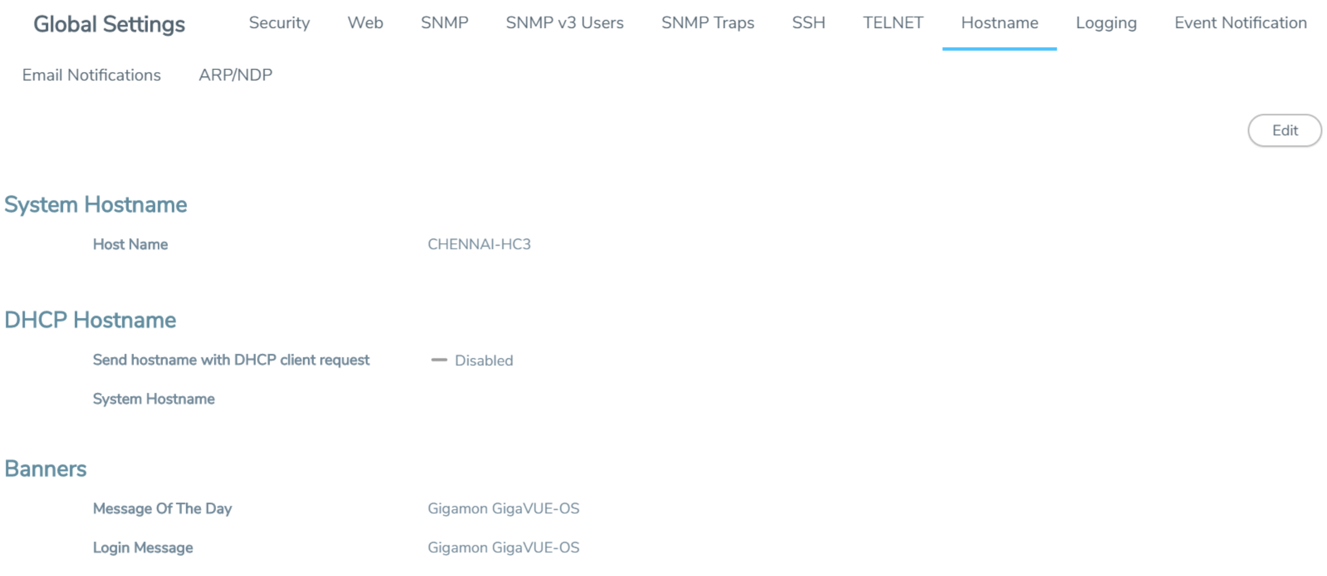
- Configure Automatic Email Notifications
- Use a Custom Banner
- View Information About the Node
- Cluster Safe and Limited Modes
- Supported Browsers

Configure the Host Name

It is generally a good idea to configure the GigaVUE-OS node’s name, date, and time as part of your initial configuration. For information on setting options related to time and date, refer to Configure Time Options. The Hostname is shown on the Hostname page, which is shown in Figure 2Hostname Page.

To set the host name, do the following:

1. On the left navigation pane, click , and then select **Physical>Nodes**. Select the required node or cluster.
2. Select **Settings > Global Settings > Host Name**.
3. Click **Edit**.
4. Enter a name in the **Hostname** field.
5. Click **Save**.



System Hostname

Host Name CHENNAI-HC3

DHCP Hostname

Send hostname with DHCP client request — Disabled

System Hostname

Banners

Message Of The Day Gigamon GigaVUE-OS

Login Message Gigamon GigaVUE-OS

Figure 2 *Hostname Page*

Configure Time Options

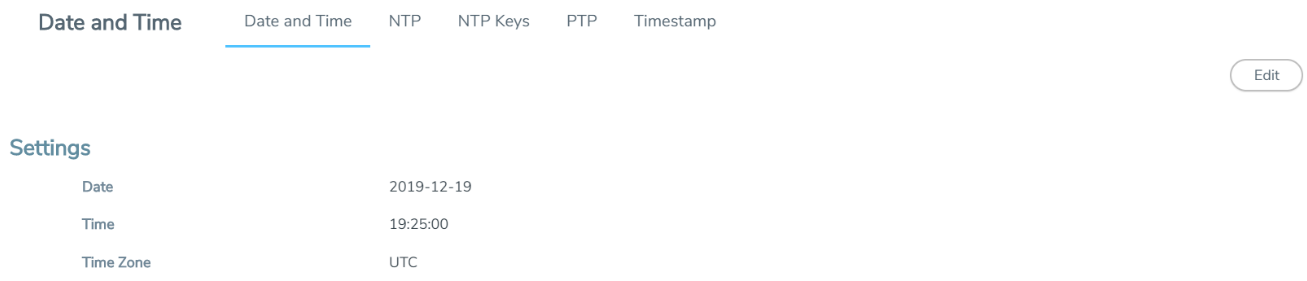
The GigaVUE-OS nodes include a variety of features for setting the time. By default, the GigaVUE HC Series node is configured to use its local clock, as configured with the Date and Time page by selecting **Settings > Date and Time**. The following table provides references to information about the various methods available for setting the time.

Method	For more information:
System Clock	*Setting Time Manually* on page 59
One-Time NTP Synchronization	*Performing One-Time NTP Server Synchronization* on page 60
Persistent NTP Synchronization	*Using NTP Time Server for Clock Synchronization* on page 60
PTP Synchronization	*Refer to the GigaVUE-OS CLI Reference Guide*

> **NOTE:** Keep in mind that PTP and NTP are mutually exclusive – enabling one disables the other.

Set Time Manually

The easiest way to set the GigaVUE-OS node's time is manually from the Date and Time page, which is shown in the following figure.



Date 2019-12-19
Time 19:25:00
Time Zone UTC

To set the time manually, do the following:

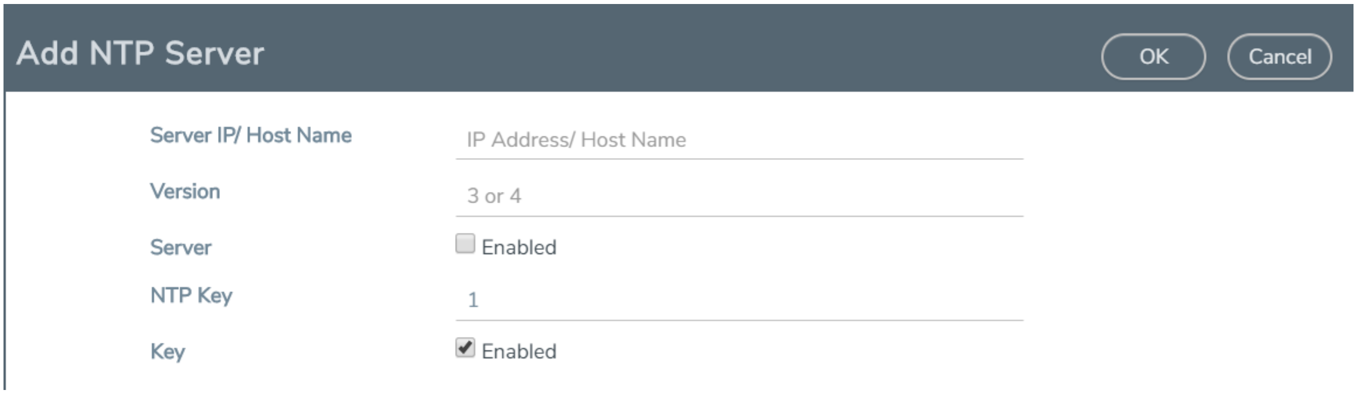
> **NOTE:** Even if you are using NTP, configure time manually as well. The GigaVUE node will automatically fall back to the manual time setting if it is unable to synchronize with the specified time server.

1. Select **Settings > Date and Time > Date And Time**.
2. Click **Edit**.
3. On the Date and Time Edit page, enter the current **Date**, **Time**, and select the **Time Zone** for your location.
4. Click **OK** to update the date and time settings.

Use NTP Time Server for Clock Synchronization

The GigaVUE node can optionally use one or more NTP servers for its time setting. Use the following procedure to add an NTP server to the GigaVUE node's list and enable the use of NTP.

1. Select **Settings > Date and Time > NTP**.
2. Click **Add**. The Add NTP Server page appears.



Add NTP Server

Server IP/ Host Name	IP Address/ Host Name
Version	3 or 4
Server	□ Enabled
NTP Key	1
Key	☑ Enabled

3. Specify the address of the time server in the Server IP/Host Name field.

   You can specify an IPv4, IPv6, or hostname. To use IPv6 addresses, IPv6 must be enabled through the CLI. For more information, refer to the *GigaVUE-OS CLI Reference Guide*.

   > **NOTE:** There are many public NTP servers available on the Internet.

4. Select the NTP version in the **Version** field.
5. Select **Enable** to enable the server.
6. Click **Save**.

   The GigaVUE node connects to the specified NTP server and synchronizes to its time. Also, NTP reports times in UTC. Because of this, it is a good idea to specify the GigaVUE H Series node's timezone so that UTC can be converted to the local timezone.

Perform One-Time NTP Server Synchronization

You can perform a one-time synchronization with an NTP server by doing the following:

1. Select **Settings > Date and Time > NTP**.
2. Clicking **Settings** to open the Edit NTP Settings page.
3. On the Edit NTP Settings page, select **Enabled**.
4. Click **Save**.

Role-Based Access: Rules and Notes

This section provides rules and notes for role-based access related to the following:

- User Management
- Role Management
- Port Ownership

User Management

The following role-based access rules and notes apply to user management:

- There must always be at least one user with the administrator role assigned. The system prevents deletion of the last configured administrator to prevent an accidental lockout situation.
- Only administrators can add, edit, or delete users.
- Non-admin users must have at least one role assigned. If you remove all of a user’s custom roles, the Default role is automatically assigned to the user, even if it was previously removed.
- Users can only be deleted by administrators if they do not have any lock or lock-share privileges in place. Deleted users are automatically removed from all assigned roles.

Role Management

The following role-based access rules and notes apply to role management:

- A role cannot be deleted if ports are still assigned to it.
- Only administrators can add, edit, or delete roles.
- The built-in **admin** and **Default** roles cannot be deleted.
- Only administrators can assign or remove user roles.
- Administrators are prevented from changing a user’s assignment to a port locked by the user.

> **NOTE:** The admin must first unlock the port before changing a user’s assignment.

Port Ownership

The following role-based access rules and notes apply to port ownership:

- Only administrators can assign or remove roles from ports.
- To remove a user's lock from a port, refer to Remove a Lock from a User's Port.
- To remove a user's lock-share, refer to Remove a User's Lock-Share.
- Administrators can also lock a port for a user. Refer to Lock a Port for a User.
- The admin role automatically has Level 4 permissions to all ports. The admin role cannot be assigned to any port.

Configure Logging

GigaVUE HC Series nodes provide comprehensive logging capabilities to keep track of system events. Logging is particularly useful for troubleshooting system issues, as well as maintaining an audit trail. You can specify what types of events are logged, view logged events by priority, date, or name, and upload log files to a remote host for troubleshooting.

Logged events are always written to the local log file (syslog.log). You can optionally specify an external syslog server as a destination for the GigaVUE HC Series node's logging output. When an external syslog server is specified, the GigaVUE HC Series node will send logged events through UDP, TCP, or SSH to the specified destination.

To configure a syslog server as destination for logging in GigaVUE-FM, do the following:

1. Select **Settings > Global Settings > Logging**.
2. Click **Add**.
3. Select the logging protocol: **UDP**, **TCP**, or **SSH**.

   For UDP, do the following:

   a. Enter the external server's IP address in the **IP Address** field.

   b. Select the logging level from the **Log Level** list. For a description of the logging levels, refer to Table 1: Logging Levels.

   For TCP, do the following:

   a. Enter the external server's IP address in the **IP Address** field.

      IPv6 addresses are supported; for example, 2001:db8:a0b:12f0::82. Also, hostnames are supported; for example, syslog.ipv6.

      Note: IPv6 must be enabled before you can configure an IPv6 syslog server. To enable the IPv6, use the CLI command `enable ipv6`.

   b. Select the logging level from the **Log Level** list. For a description of the logging levels, refer to Table 1: Logging Levels.

   c. Enter the port number in the TCP Port field.

   For SSH, do the following:

   a. Enter the external server's IP address in the **IP Address** field.

b. Select the logging level from the **Log Level** list. For a description of the logging levels, refer to Table 1: Logging Levels.

c. Enter the port number in the TCP Port field.

d. Enter the user name for logging in to the SSH server in the **Username** field.

Table 1: Logging Levels

Log-Level	Description
emergency	Emergency – the system is unusable. The severity level with the least logging – only emergency level events/commands are logged.
alert	Action must be taken immediately.
critical	Critical conditions.
error	Error conditions.
warning	Warning conditions.
notice	Normal but significant condition.
info	Informational messages.
debug	Debug-level messages. Authorized for factory use only.

> **NOTE:** Syslog servers configured through device CLI do not get reflected in the GigaVUE-FM GUI. Click the Sync button for GigaVUE-FM to sync with the device and retrieve the syslog servers. GigaVUE-FM prompts a message after the syslog server retrieval is completed and the syslog servers added through the CLI get reflected in the GUI.

External Syslog Servers and Clustered Nodes

When working with clustered nodes, set up logging individually for each clustered node.

Events sent to external syslog servers are sent over the Mgmt port of the node logging the event and not over the cluster’s leader/VIP address.

Delete an External Syslog Server

Remove a logging server by doing the following:

1. Select **Settings > Global Settings > Logging**.
2. Select the external server on the Logging page as shown in Delete an External Syslog Server
3. Click **Delete**.
4. Delete message shown in the following figure displays. Click **OK** to delete the server.

Packet Format for Syslog Output

Syslog packets sent by the GigaVUE H Series node to an external syslog server conform to the format recommended by RFC 3164 (but are not facility numerical code compatible).

Keep in mind the following about this packet format:

- Severity indications in the packet's PRI field are derived from corresponding event levels on the GigaVUE H Series node.
- Timestamps are provided in **Mmm dd hh:mm:ss** format, where Mmm is the standard English language abbreviation of the month (for example, Jan, Feb, Mar).
- Syslog packets include the IP address of the Mgmt port.

Configure Automatic Email Notifications

The GigaVUE-OS node provides powerful email notification capabilities, automatically sending emails to specified addresses when any of a wide variety of events take place on the node. Gigamon strongly recommends that you configure this feature so you have immediate visibility of events affecting node health.

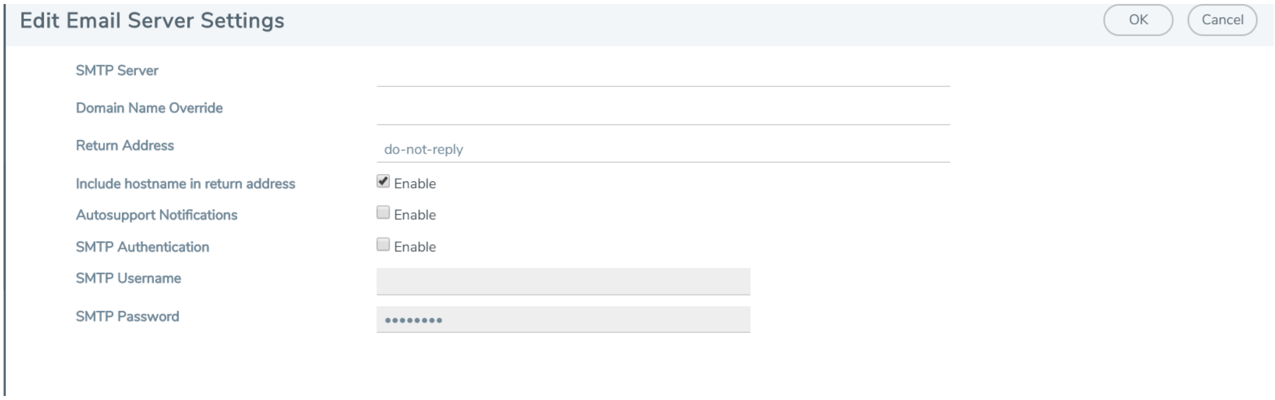
To configure automatic email notification, you will need to specify the email server settings, the events about which to be notified, and the recipient or recipients for the notifications.

Configure the Email Server Settings

To configure the server settings for automatic email notifications for the GigaVUE node, do the following:

1. On the left navigation pane, click ▤, and then select **Physical>Nodes**. Select the required node or cluster.
2. Select **Settings > Global Settings > Email Notifications.**

   The Email Notifications page shows the current server settings, the events enabled for notification, and the recipients for the notifications.
3. Click **Server Settings**. The Edit Email Server Settings page displays.



Edit Email Server Settings

SMTP Server

Domain Name Override

Return Address: do-not-reply

Include hostname in return address ☑ Enable

Autosupport Notifications □ Enable

SMTP Authentication □ Enable

SMTP Username

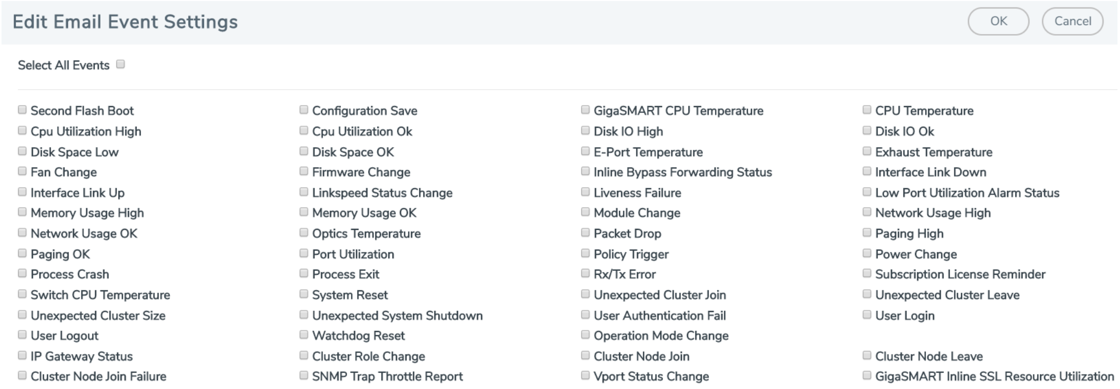
SMTP Password ••••••••

4. Enter the information about the email server on the settings page.
5. Click **OK**.
6. Select the events for notification. For the configuration steps, refer to the next section Configure the Event Settings.

Configure the Event Settings

To configure the event settings for automatic email notifications for the GigaVUE node, do the following:

1. On the left navigation pane, click , and then select **Physical>Nodes**. Select the required node or cluster.
2. Select **Settings > Global Settings > Email Notifications**
3. Click **Event Settings**. The Edit Email Event Settings page displays, which provides a list of events that you can select for email notifications.



Edit Email Event Settings

Select All Events □

□ Second Flash Boot
□ Cpu Utilization High
□ Disk Space Low
□ Fan Change
□ Interface Link Up
□ Memory Usage High
□ Network Usage OK
□ Paging OK
□ Process Crash
□ Switch CPU Temperature
□ Unexpected Cluster Size
□ User Logout
□ IP Gateway Status
□ Cluster Node Join Failure

□ Configuration Save
□ Cpu Utilization Ok
□ Disk Space OK
□ Firmware Change
□ Linkspeed Status Change
□ Memory Usage OK
□ Optics Temperature
□ Port Utilization
□ Process Exit
□ System Reset
□ Unexpected System Shutdown
□ Watchdog Reset
□ Cluster Role Change
□ SNMP Trap Throttle Report

□ GigaSMART CPU Temperature
□ Disk IO High
□ E-Port Temperature
□ Inline Bypass Forwarding Status
□ Liveness Failure
□ Module Change
□ Packet Drop
□ Policy Trigger
□ Rx/Tx Error
□ Unexpected Cluster Join
□ User Authentication Fail
□ Operation Mode Change
□ Cluster Node Join
□ Vport Status Change

□ CPU Temperature
□ Disk IO Ok
□ Exhaust Temperature
□ Interface Link Down
□ Low Port Utilization Alarm Status
□ Network Usage High
□ Paging High
□ Power Change
□ Subscription License Reminder
□ Unexpected Cluster Leave
□ User Login
□ Cluster Node Leave
□ GigaSMART Inline SSL Resource Utilization

4. Select the event or events about which the email recipient should be notified.
5. Click **OK**.
6. Add a recipient for the notifications. For the steps to add a recipient, refer to the next section Add Email Notification Recipients.

Add Email Notification Recipients

To add an email notification recipient for the GigaVUE node, do the following:

1. On the left navigation pane, click , and then select **Physical>Nodes**. Select the required node or cluster.
2. Select **Settings > Global Settings > Email Notifications,** and then click **Add**.
3. Enter the recipient’s email address in the **Email Address** field. You can add more than one email address, separating each address with a comma.
4. Set the level of notification to be sent to the recipient by selecting one or more of the following:
   - **Send Detail Notification** — send a detailed description about the event. Use detail notification to specify whether summarized of detailed output should be included in the email. Not that not all events have both summary and detail formats
   - **Send info Notification** — send information about the event, but without detail.
   - **Send Failure Notification** — send only notification about failure events. No email is sent when failure notification is enabled and an information event is generated.
5. Click **OK**.

Use a Custom Banner

The GigaVUE node can display a customizable text banner at node startup before a user logs in. This way, users connecting to the node see the banner before they log in, giving them an idea of which node they are logging in to. The banner also appears after a user logs outs.

To set the custom banner:

1. Select **Settings > Global Settings > Host Name**.
2. Click **Edit**. The Edit Hostname page displays.
3. Enter the custom banner in the Login Message field.
4. Click **OK**.

Acknowledge the Custom Banner

The 'enable' GigaVUE-OS CLI option is available when configuring the GigaVUE-OS UI acknowledgment banner. This allows customer to enable or disable the banner acknowledgment; which is the requirement for users to acknowledge the banner. If this is disabled, the banner will appear but will not require the user to acknowledge it.

View Information About the Node

GigaVUE-FM includes pages that provide specific information about the node.

- The Interface page provides information about current settings for the interface.
- The DNS page lists the IP addresses for Domain Name Services.
- The Protocol Configuration page allows you to configure the discovery protocols or gratuitous ARP on the management interface of the device.

Interface

The Interface page shows status information about the various interfaces.

To access the interface page:

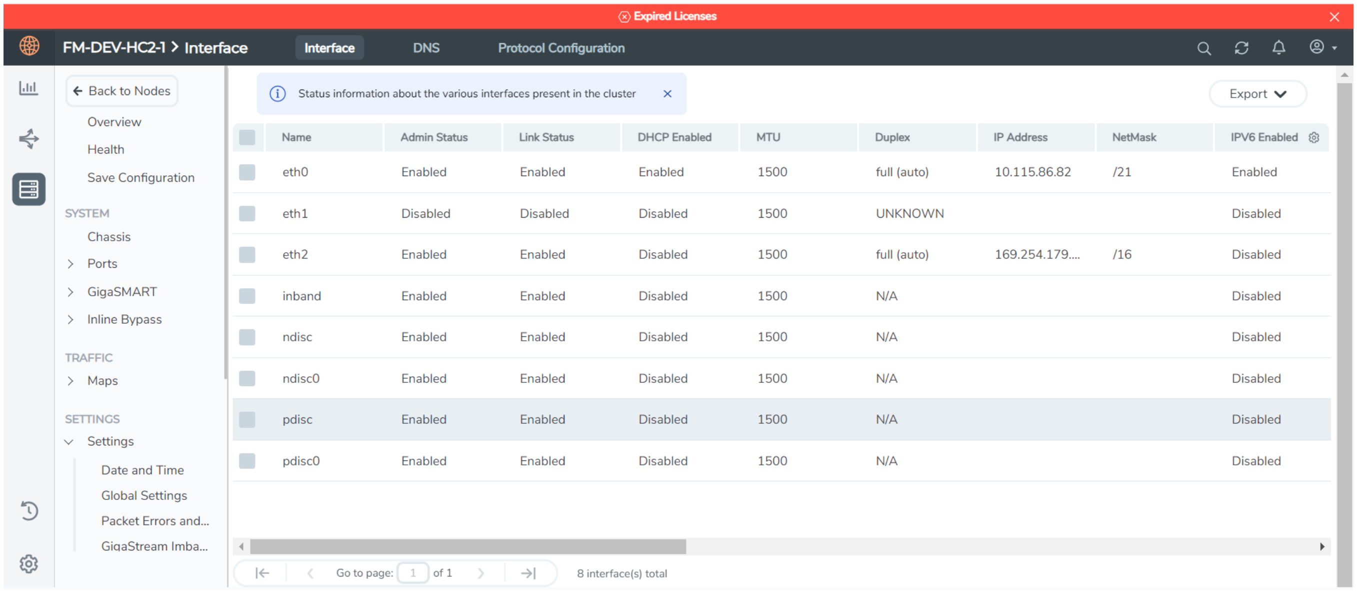
1. On the left navigation pane, click on 🗄 and select **Nodes**.
2. Click on a node for which you want to set the interface settings.
3. Select **Settings > Interface > Interface**. The page provides the following information:

> **NOTE:** Some settings can only be enabled through the CLI, such as IPv6 addressing.

- **Ethernet status information** (eth0, eth1, eth2). The number of interfaces depends on the model of the node. The following information is provided about the interface:
  - Name
  - Admin Status
  - Link Status
  - DHCP enabled
  - MTU
  - Duplex
  - IP address
  - Netmask
  - IPv6 Enabled
  - Autconf enabled
  - Autoconf route
  - Auoconf privacy
  - DHCPv6 running
  - Speed
  - Type
  - ifindex
  - ifsource
  - HW addr
  - Cluster Name
  - Description
  - IPv6 addresses
  - IPv6 address
- **Interface inband status** provides information when the node is configured for inband clustering: The following information is provided about the inband interface:

  - Admin Status
  - Link Status
  - Duplex
  - MTU
  - HW addr
  - ifSource
  - Autoconf enabled
  - Autoconf privacy
  - IPv6 addresses
  - Dhcp enabled
  - Speed
  - IP address
  - Netmask
  - Type
  - ifindex
  - IPv6 enabled
  - Autoconf route
  - DHCPv6 running
  - IPv6 address
- **Interface NDisc** status provides status information about the internal interfaces for neighbor discovery. Depending on how the node is configured, there can be more than one NDisc (NDisc, NDisc0, NDisc1, and so on). The following information is provided about NDisc:
  - Admin Status
  - Link Status
  - Duplex
  - MTU
  - HW addr
  - ifSource
  - Autoconf enabled
  - Autoconf privacy
  - IPv6 addresses
  - Dhcp enabled
  - Speed
  - IP address
  - Netmask
  - Type
  - ifindex
  - IPv6 enabled
  - Autoconf route
  - DHCPv6 running

- IPv6 address



Status information about the various interfaces present in the cluster

Name	Admin Status	Link Status	DHCP Enabled	MTU	Duplex	IP Address	NetMask	IPV6 Enabled
eth0	Enabled	Enabled	Enabled	1500	full (auto)	10.115.86.82	/21	Enabled
eth1	Disabled	Disabled	Disabled	1500	UNKNOWN			Disabled
eth2	Enabled	Enabled	Disabled	1500	full (auto)	169.254.179....	/16	Disabled
inband	Enabled	Enabled	Disabled	1500	N/A			Disabled
ndisc	Enabled	Enabled	Disabled	1500	N/A			Disabled
ndisc0	Enabled	Enabled	Disabled	1500	N/A			Disabled
pdisc	Enabled	Enabled	Disabled	1500	N/A			Disabled
pdisc0	Enabled	Enabled	Disabled	1500	N/A			Disabled

8 interface(s) total

Figure 3 *Interface Page*

DNS

To view Domain Name Servers (DNS) information for the node, select **Settings > Interface > DNS**. The DNS page displays the following information:

- Primary DNS IP Address
- Secondary DNS IP Address
- Tertiary DNS IP Address

Cluster Safe and Limited Modes

Safe and limited modes in cluster safeguard critical provisioning errors for both standalone nodes and nodes in a cluster.

During provisioning operations such as configuring a map, in rare occasions there can be unrecoverable system errors that can potentially put the cluster or the clustered nodes or standalone nodes into unsafe or unstable states. Once in such a state, additional operations or configuration changes can cause the node to crash, the cluster to deform, or the data traffic to be impacted. For example, due to a node attempting to rejoin a cluster, a chassis can end up in a reboot loop. In previous software versions, there was no way to prevent entering the loop.

These modes provide notification, stop further operations from being performed, and give you time to troubleshoot and plan the recovery of the cluster or of any node in the cluster or standalone node.

Two modes are supported. The first is called safe mode and is triggered when the node detects unrecoverable errors, but the existing flow maps are not impacted. The second is called limited mode and is triggered when the node detects continuous system reboots. In this mode, the node will become standalone and only basic configuration will be allowed.

When a node enters safe mode it displays the following message when you attempt to make a change to the configuration that is not available in safe mode:

```
The system has restricted provisioning in safe mode. Contact Gigamon Support on
how to troubleshoot and recover from safe mode.
```

Safe Mode

A node enters safe mode when there are unrecoverable errors. Any node in a cluster can enter this mode. The purpose of this mode is to detect system configuration failures early and avoid future failures, such as system crashes.

Examples of unrecoverable errors are when there are inconsistencies between the system and the running configuration or when the cluster configuration did not merge properly with the existing configuration.

As part of merge error recovery, nodes joining a cluster are automatically restarted so the merge error can be fixed. If the restart cannot correct the merge error, the node will enter safe mode.

Another example is that a TA Series node could enter safe mode when unlicensed cluster ports are used in an offline configured map. (It is recommended to use only licensed ports in map configurations.)

A node will automatically enter safe mode.

When a node is in safe mode:

- The node displays a banner indicating it is in safe mode. (Refer to Cluster Safe and Limited Modes.)
- An SNMP trap is sent to notify the user when the mode changes.
- Configured traffic continues to be forwarded.
- Traffic provisioning is not allowed on the affected node. Any other configuration remains as is.
- If the standby node in the cluster is in safe mode, it can still become the leader if the current leader fails or switches over, but the database on the standby node may not be in sync, so it is not recommended to continue in that state. Instead, take immediate action to recover the node.
- In safe mode, the member nodes in the cluster do not process any incoming traffic configuration from the cluster leader.

- SSH is not supported in safe mode if Enhanced Cryptography is enabled. This is a requirement of FIPS. If you are working in an Enhanced Cryptography environment and the node enters in to SAFE mode, you will get a 'connection refused' error. Restart the device to recover the node from SAFE mode. SSH will work again.

When a node is in safe mode and you try do any operations that are not allowed in safe mode, the UI displays the message shown in Cluster Safe and Limited Modes.

When safe mode has been detected, collect information and report it to Gigamon Technical Support. Refer to Collect Information for Technical Support. To recover from safe mode, reload the node.

Limited Mode

A node automatically enters limited mode when it detects repeated system crashes. The node also becomes a standalone node when a it enters limited mode.

When a node is in limited mode:

- The node displays a banner indicating that it is in limited mode.
- An SNMP trap is sent to notify the user when the mode changes.
- All traffic forwarding halts; no traffic flows.
- The node will become standalone (clustering will be disabled).
- Only basic system provisioning is allowed. Traffic provisioning is not allowed. Only commands that are related to image download, installation, next boot, and reboot are allowed, as well as reset factory.

Limited mode is triggered when there are three (3) failures/system crashes within 15 minutes. In limited mode, the cluster configuration is ignored. No cluster configuration or GigaVUE-OS configuration is accepted when the node is in limited mode.

When limited mode has been detected, collect information and report it to Gigamon Technical Support. Refer to Collect Information for Technical Support.

Enable SNMP Trap for Safe Mode and Limited Mode

Use the following steps to configure a notification that will be sent to all configured destinations when a node in the cluster changes from operational mode to safe mode or from operational mode to limited mode.

The safe mode and limited mode capabilities are enabled through the SNMP trap event Operational Mode Change. To enable the trap on a node, do the following:

1. Select **Settings > Global Settings > SNMP Traps**.
2. Click **Trap Settings**.
3. On the Edit SNMP Traps Settings page, select **Operational Mode Change**.

4. Click **Save**.

When the cluster leader enters safe mode, the SNMP trap will be sent and the leader will be identified as the local node in the trap.

When a node in a cluster (normal or standby) enters safe mode, the SNMP trap will be sent and the node will be identified as the local node in the trap. In addition, a notification will be sent to the cluster leader in the form of a CLI console message. The node that entered safe mode will be identified by its box ID in the notification to the leader. The following is an example of the CLI console message:

```
hc2 [default-cluster:leader] (config) # ! Box-ID 4: System has entered into safe mode!!hc2
[default-cluster:leader] (config) #
```

Log messages also provide information. The following is a sample log:

```
Jun 8 13:46:27 GC-TA10-N6 mgmtd[2400]: [mgmtd.INFO]: SAFE mode: Merge error detected !!
Triggering SAFE mode ...
```

Collect Information for Technical Support

Collecting the following information can help Technical Support:

- Sysdumps/debug dumps for all nodes in the cluster
- Sysdumps for nodes that observed a crash entering safe or limited mode
- Debug dumps for nodes that did not observe a crash
- Console logs
- CLI histories
- CLI or GigaVUE-FM screen captures
- SNMP captures

To generate a system dump file, refer to Generate Sysdump or Debug Dump File.

To contact technical support, refer to Contact Technical Support.

Generate Sysdump or Debug Dump File

You can generate the system dump files for all the nodes that are part of a cluster by logging into the leader. However, to download the system dump file for a node, you must log into the respective node. For standalone nodes, log into the respective nodes to generate, view, download, or delete the system dump files.

To generate the system dump file for nodes in a cluster:

1. On the left navigation pane, click , and then select **Physical > Nodes**
2. Select a cluster ID, and then from the left navigation pane, go to **Support > Debug > Sysdump**.
3. Click **Generate**. The Generate Debug File quick access view appears.
4. Either select the **All Host Names** check box to generate the debug files for all the nodes that are part of the cluster or select the required host name from the **Host Name** drop-down list to generate the debug file for the respective node.
5. Click **Generate**.

To generate the system dump file for a standalone node:

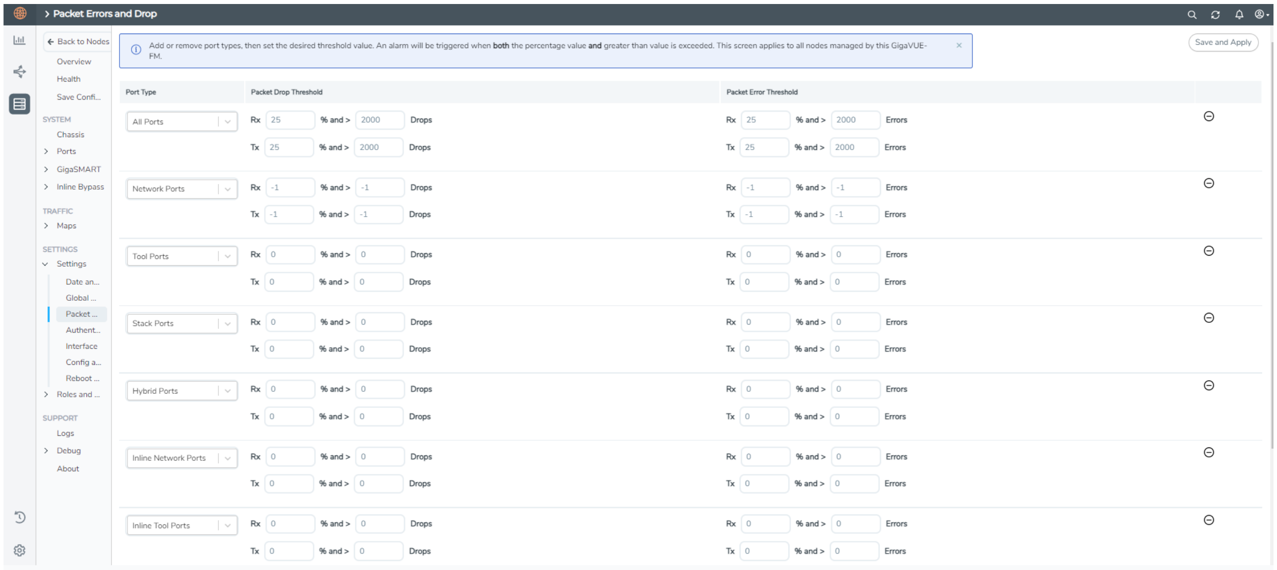
1. On the left navigation pane, click , and then select **Physical > Nodes**
2. Select a standalone node, and then from the left navigation pane, go to **Support > Debug > Sysdump**.
3. Click **Generate**.

Configure Port Packet Drop/Error in Devices

To configure port packet drop/error through the device settings page:

1. On the left navigation pane, click on and under **Physical**, select the required device or cluster.
2. Click **Settings** > **Packet Errors and Drops**. The Packet Errors and Drops page is displayed.
3. Select or enter the following values:

Field	Description
Port Type	Port type for which the threshold is to be configured. Configuration for *All Ports* will be applied to all the ports (equivalent to the global level configuration in device CLI).
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.



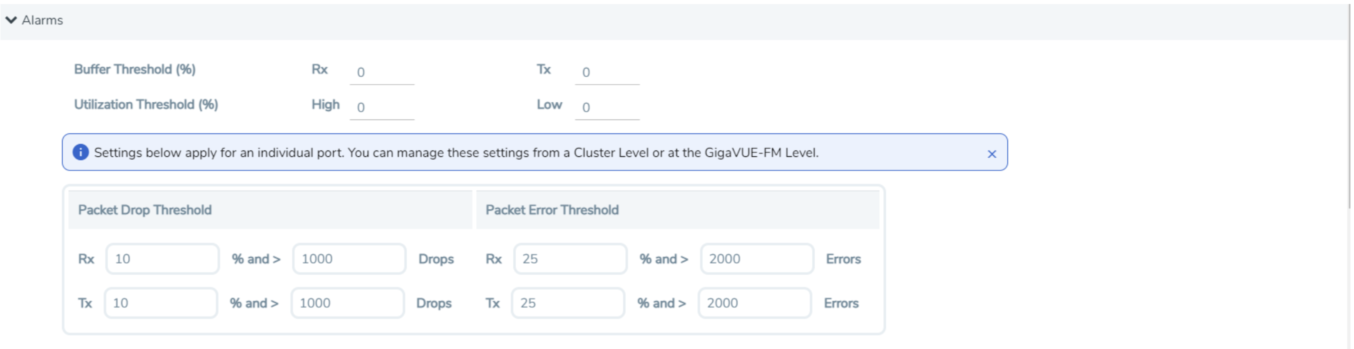
Add or remove port types, then set the desired threshold value. An alarm will be triggered when **both** the percentage value **and** greater than value is exceeded. This screen applies to all nodes managed by this GigaVUE-FM.

Port Type	Packet Drop Threshold	Packet Error Threshold
All Ports	Rx 25 % and > 2000 Drops Tx 25 % and > 2000 Drops	Rx 25 % and > 2000 Errors Tx 25 % and > 2000 Errors
Network Ports	Rx -1 % and > -1 Drops Tx -1 % and > -1 Drops	Rx -1 % and > -1 Errors Tx -1 % and > -1 Errors
Tool Ports	Rx 0 % and > 0 Drops Tx 0 % and > 0 Drops	Rx 0 % and > 0 Errors Tx 0 % and > 0 Errors
Stack Ports	Rx 0 % and > 0 Drops Tx 0 % and > 0 Drops	Rx 0 % and > 0 Errors Tx 0 % and > 0 Errors
Hybrid Ports	Rx 0 % and > 0 Drops Tx 0 % and > 0 Drops	Rx 0 % and > 0 Errors Tx 0 % and > 0 Errors
Inline Network Ports	Rx 0 % and > 0 Drops Tx 0 % and > 0 Drops	Rx 0 % and > 0 Errors Tx 0 % and > 0 Errors
Inline Tool Ports	Rx 0 % and > 0 Drops Tx 0 % and > 0 Drops	Rx 0 % and > 0 Errors Tx 0 % and > 0 Errors

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

To configure threshold values for a specific port:

1. Select **Ports > Ports > All Ports**. Select the Port ID of the port on which you want to configure the packet drop/error threshold.
2. Click **Edit** to open the port editor.
3. Under **Alarms**, configure the **Packet Drop Threshold** and **Packet Error Threshold** values in % and number for both Rx and Tx traffic.



Buffer Threshold (%)	Rx	0	Tx	0
Utilization Threshold (%)	High	0	Low	0

Settings below apply for an individual port. You can manage these settings from a Cluster Level or at the GigaVUE-FM Level.

Packet Drop Threshold	Packet Error Threshold
Rx 10 % and > 1000 Drops	Rx 25 % and > 2000 Errors
Tx 10 % and > 1000 Drops	Tx 25 % and > 2000 Errors

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

The configuration is applied to that specific port.

> **NOTE:** To configure the threshold values globally for all the devices managed by GigaVUE-FM refer to Configure Port Packet Drop/Error in GigaVUE-FM

Related topics

- Port Packet Errors and Drops
- Configure Port Packet Drop/Error in GigaVUE-FM

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:

- About Security and Access
- About Role-Based Access
- Configure Authentication and Authorization (AAA)
  - Configure AAA Authentication Options
  - Grant Roles with External Authentication Servers
  - Add AAA Servers to the Node's List
  - Configure Roles in External Authentication Servers
- Supported Clients
- Default Ports
- FIPS 140-2 Compliance
- UC APL Compliance
- Common Criteria
- GigaVUE-OS Security Hardening
- Best Practices for Security Hardening

About Security and Access

The GigaVUE HC Series nodes provide an interlocking set of options that let you create a comprehensive security strategy for the node. These options are summarized in the following table:

Security Tools	Description
Roles/Groups	**Roles** specify which users have access to a given port. The following built-in roles are provided: ● **Admin** – This role provides access to all command modes, including Standard, Enable, and Configure. Admin users also have access to all commands and all ports. They are also members of all groups. ● **Default –** This role also provides access to all command modes. Users with the Default Role has no access to unassigned ports. New users are created with the Default role automatically. However, you can remove it if you do not want to allow a user access to unassigned ports ● **Monitor** – This built-in role provides view-only access to ports and configurations Administrators create additional custom **roles** and assign them to users together with the Default role. For example, if you create a role named **Security_Team** and assign it to tool port 5/1/x2, users assigned the **Security_Team** role will be able to

Security Tools	Description
	access tool port 5/1/x2. Conversely, users without a role that gives them some access to tool port 5/1/x2 will not even be able to see it in the CLI. Users can have multiple assigned roles, allowing administrators to fine-tune access to the Visibility Platform.
Permissions	Administrators assign **Permissions** to specify what users can do with a port to which they have access. You can assign the following permission levels: ● **Level 1**: Can view the port but cannot make any changes to port settings or maps. When applied to a network port, can view maps attached to the network port. This level is used for users who only need to monitor the activities of the port. ● **Level 2**: Can use the port for maps, create tool-mirror to/from port, and change egress port filters. Can configure port-lock, lock-share, and all traffic objects except port-pair. Also includes all Level 1 permissions. ● **Level 3**: Can configure port parameters (such as administrative status of the port, speed, duplex, and autonegotiation), as well as create port pairs. Also includes all Level 2 and Level 1 permissions. ● **Level 4**: Can change the port type. Also includes all Level 3, 2, and 1 permissions. Permissions are hierarchical so that higher levels include all lower-level permissions (for example, a Level 3 user also has Level 2 permissions and can configure all traffic distribution, set locks, and share locks). Administrators can configure permissions differently on a port-by-port basis for a given role. This can be useful in situations where you want to give a group full authority to reconfigure maps and port parameters for a set of tool ports but only map creation permissions for a network port shared with other groups.
Port Locking/Sharing	Port locking lets a user with Level 2+ access to a port prevent other users from changing any settings for a locked port. This is useful in situations where a user needs undisturbed access to a port for short-term troubleshooting. When a port is locked, all users with Level 2+ access to the port will temporarily only have Level 1 access (read-only). Normal configured permissions are restored when the lock is released. Users can also share a locked port with any other specified user. Sharing a locked port provides the account with whom the port is shared the same port permissions as the account sharing the port. So, for example, if UserX has Level 2 permissions on port 12/5/x3, he can share a lock on 12/5/x3 with any other user account, providing them with Level 2 permissions regardless of their normal privileges on the port.
Authentication	The GigaVUE HC Series node can authenticate users against a **local** user database or against the database stored on an external authentication server (LDAP, RADIUS, or TACACS+). Admin users can specify the authentication methods used for logging in using **AAA Authentication.** **NOTE:** The serial **console** port always retains **local** authentication as a fallback option to prevent unintended lockouts.

Management Port Security

Management port security lets you restrict the exchange of packets through the management port by creating an access control list to restrict user and SNMP access.

Use the CLI to access and configure the Management port and Console port. For instructions, refer to the *GigaVUE-OS CLI Reference Guide*.

> **NOTE:** Exercise caution when using the following configuration example described in the *GigaVUE-OS CLI Reference Guide* so as not to interfere with communications through the backplane or within a cluster.

About Role-Based Access

GigaVUE nodes use role-based access control to manage access to the Gigamon Visibility Platform, providing different groups of users with different analysis needs full access to the packets they need for their tools. Figure 4Role-Based Access in Action shows role-based access in action, with separate sets of tool ports partitioned to different groups of users while different sets of network ports are shared.

Figure 4Role-Based Access in Actionshows an example of role-based access control in action. Different teams have been assigned roles that give them access to different sets of ports. For example, the Security Team has access to network ports N1...N2 and tool ports T1...T3. Because the Security Team is sharing N1...N2 with the Server Team, permissions are used to give each team full control of their tool ports while preventing port parameter changes to the shared network ports.

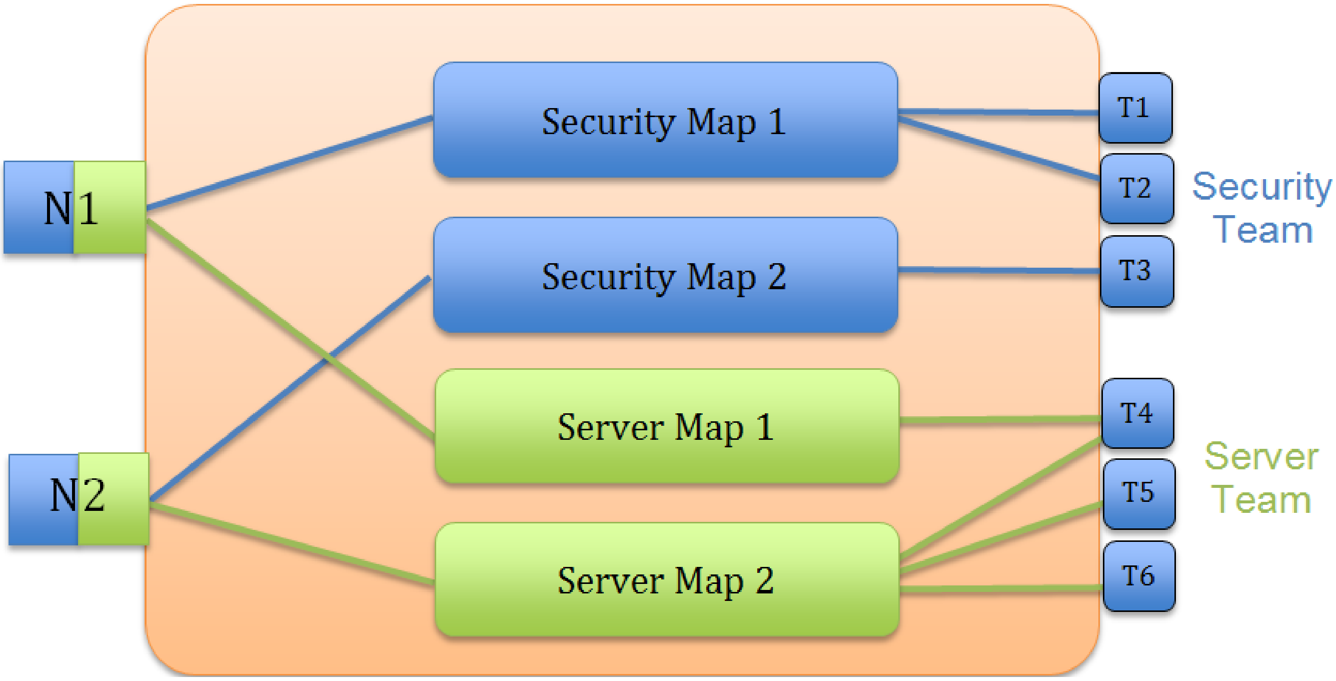


Figure 4 *Role-Based Access in Action*

Configure Role-Based Access: A Summary

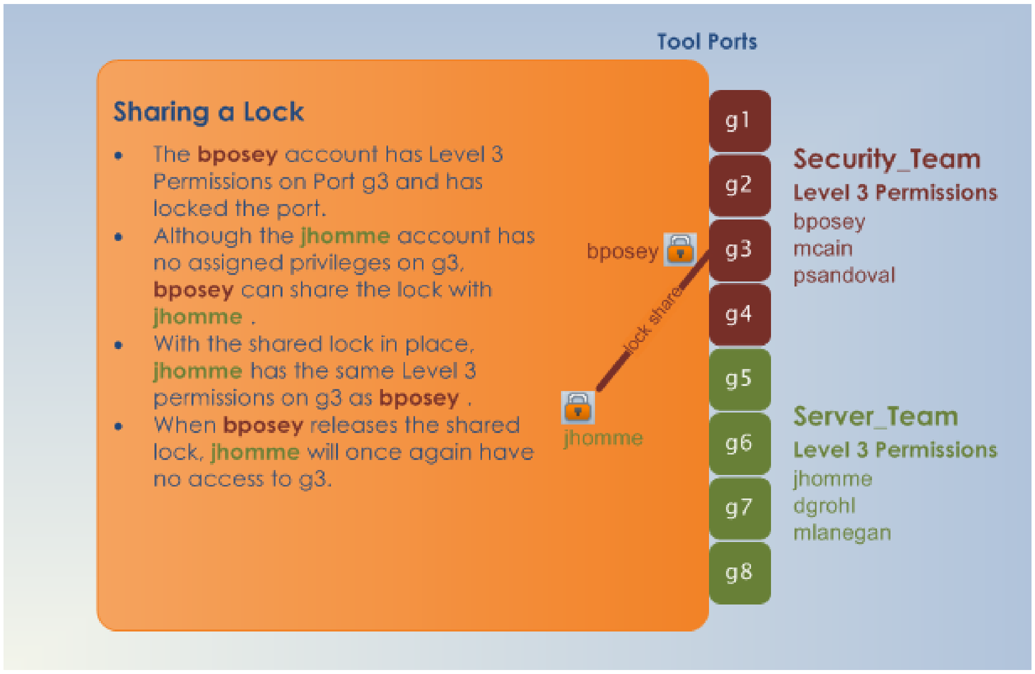
Configuring role-based access consists of the major steps listed in the following table:

Step	Description
Configure Roles	Administrators use the **Roles** page in the UI to create roles. At first, roles are empty containers. You can create as many as you need to share the Visibility Platform effectively. For example, if you have an IT organization with six different groups (Security, Desktop, Application Performance Management, Server, Archive, and so on), each with different packet needs, you may want to create separate roles for each of them and assign them to different sets of tool ports. **NOTE:** The built-in "Default" role has no access to unassigned ports.
Create Users with Roles Assigned	Once you have roles created, you can assign them to users. You can assign roles to existing users or as you create new users. Users can have multiple roles assigned, giving them access to different sets of ports. Use the User page to assign roles. Keep in mind that admin-level users automatically have access to all roles. Administrators assign roles to default-level users.
Associate Roles with Ports and Permissions	The final step is to associate roles with ports and permissions. A user with a particular role will have access to all ports assigned that role at the designated permission level. Use Assigned to Roles fields on the Ports page to associate roles with ports and permissions.
Restriction for Removing a Role	An error message is displayed if you try to remove a role when it is used in a port tool-share. Remove the port tool-share first and then the role.
Fine Tune and Evolve	The Visibility Platform evolves as your needs change. You can continue to add new roles and tweak assigned ports and permissions to achieve the sharing results needed for different groups to get the packets they need.

About Locks and Lock Sharing

Short-term analysis needs are always changing, occasionally creating situations where one user may temporarily need exclusive access to a port. Rather than create new roles and associations in situations like this, a user can lock a port to which they have Level 2+ access, preventing other users from changing settings.

Locks can also be shared with other users, allowing users to collaborate. Sharing a locked port provides the account with whom the port is shared the same port permissions as the account sharing the port. So, for example, if UserX has Level 2 permissions on port 12/5/x3, he can share a lock on 12/5/x3 with any other user account, providing them with Level 2 permissions regardless of their normal privileges on the port, if any. This is summarized in Figure 5Sharing Locks



Sharing a Lock

- The **bposey** account has Level 3 Permissions on Port g3 and has locked the port.
- Although the **jhomme** account has no assigned privileges on g3, **bposey** can share the lock with **jhomme** .
- With the shared lock in place, **jhomme** has the same Level 3 permissions on g3 as **bposey** .
- When **bposey** releases the shared lock, **jhomme** will once again have no access to g3.

Figure 5 *Sharing Locks*

Notes:

- There is no requirement that the user with whom the locked port is shared have any normal access to the port at all.
- Keep in mind that Administrators always retain access to all ports, regardless of the locks in place.

Configure Authentication and Authorization (AAA)

Use the AAA page for authentication, authorization, and accounting settings for the GigaVUE HC Series node. In general, configuring authentication consists of specifying the login methods accepted, the order in which they are tried, the local user account to map to external logins, whether to accept roles specified by the AAA server, and the configuration of the external authentication server itself.

To open the AAA page, select **Settings > Authentication > AAA**.

Refer to the following sections for details:

- Configure AAA Authentication Options
- Grant Roles with External Authentication Servers
- Add AAA Servers to the Node’s List

Overview of the AAA Page

The following sections describe the settings and options available on the AAA page.

Authentication Priority

The **Authentication Priority** section of the AAA page specifies which authentication methods should be used for logging in to the GigaVUE H series node as well as the order in which they should be used. You can specify first, second, third, and fourth priority for the login method. For each priority, you can select one of the following:

- Local
- TACACS+
- RADIUS
- LDAP

For details about setting the login methods, refer to Configure AAA Authentication Options.

User Mapping

User mapping specifies **Map Order** and the **Map Default User**. Map order specifies how externally authenticated logins (RADIUS, TACACS+, or LDAP) are mapped to local accounts. For Map Order, you can select the following:

- **Remote First**—Maps externally authenticated logins in the following order:

    a. Mapped to the matching local account name, if present.

    b. If there is no matching local account, the local user mapping attribute provided by the AAA server is used.

    c. If the local user mapping attribute is not present or does not specify a valid local user account, the account name specified by the **Map Default User**.

    This is the default.
- **Local Only**—Maps all externally authenticated logins to the user specified by **Map Default User**.
- **Remote Only**—Maps externally authenticated logins in the following order:

    a. Mapped to the matching local account name, if present.

    b. If there is no matching local account, the local user mapping attribute provided by the AAA server is used.

    c. If the local user mapping attribute is not present or does not specify a valid local user account, no further mapping is attempted.

Map Default User specifies the account to which externally authenticated logins are mapped and how externally authenticated logins (RADIUS, TACACS+, or LDAP) are mapped to local accounts when **Map Order** is set to **Remote First** (if there is no matching local account) or **Local Only**. The default user is one of the following: admin, operator, or monitor.

Password

Select **Enabled** to set the number of days before a password expires. Use the **Duration** field to set the number of days.

Lockout

Track Authentication Failures enables or disables tracking of authentication failures. The default is disabled. Tracking can be used for informational purposes or with the **Enable Lockout.**

Disabling tracking does not clear any records of past authentication failures or the locks in the database. However, it prevents any updates to this database from being made. No new failures are recorded. It also disables lockout, preventing new lockouts from being recorded and existing lockouts from being enforced.

Enable Lockout, when selected, enables or disables locking out of user accounts based on authentication failures. This suspends the enforcement of any existing lockouts and prevents any new lockouts from being recorded. If lockouts are later re-enabled, any lockouts that had been recorded previously, resume being enforced, but accounts that passed the **Maximum Failure** limit are not automatically locked at this time. They are permitted one more attempt, and then locked out. Lockouts are applied after an authentication failure, if the user has surpassed the threshold at that time.

Lockouts only work if tracking is enabled. Enabling lockouts will automatically enable tracking. Disabling tracking will automatically disable lockouts

Lock Time specifies that no logins are permitted for this number of seconds following any login failure (not counting failures caused by the lockout mechanism, or the lock-time itself). This is not based on the number of consecutive failures.

Unlock Time specifies that if a user account is locked due to authentication failures, another login attempt will be permitted if this number of seconds has elapsed since the last login failure. That does not count failures caused by the lockout mechanism itself. A user must have been permitted to attempt to login, and then failed. After this interval has elapsed, the account does not become unlocked, nor does its history reset. It simply permits one more login attempt even if the account is locked. Unlike **Maximum Failure**, this does take effect immediately for all accounts.

If both **Unlock Time** and **Lock Time** are set, the unlock time must be greater than the lock time.

Maximum Failure sets the maximum number of consecutive authentication failures (attempts) permitted for a user account before the account is locked. After this number of failures, the account is locked and subsequent attempts are not permitted.

The **Maximum Failure** setting only impacts the lockouts imposed while the setting is active. It is not retroactive to previous logins. So if **Maximum Failure** is disabled or changed, this does not immediately cause any users to be changed from locked to unlocked or vice-versa.

Selecting **Enable Admin Lockout** overrides the global settings for tracking and lockouts for the admin account. When option is not selected, it means that the admin user will never be locked out, though their authentication failure history will still be tracked if tracking is enabled overall. This option applies only to the single account with the username admin. It does not apply to any other users with administrative privileges.

Non Local User Authentication

Track Authentication Failures enables tracking of authentication failures for non-local users.

When **hashUsername** is selected, a hash function is applied to the username and the hashed result is stored.

FAQ for Logins and Passwords

This section answers frequently asked questions for logins and passwords.

Do Passwords Expire?

By default, the **Password** option is not enabled. When enabled, it is set to expire in 90 days, by default. Use **Duration** to enable password expiration.

The time when the user enables password expiration is relative to when the user account was created. For example, if **admin** creates a user named bob today, and in 15 days decides to enable password expiration with a 10-day limit, the user bob will be forced to change his password the next time he logs in.

What Happens After Unsuccessful Logins?

After 5 unsuccessful login attempts, login access is locked for 15 seconds.

Use the **Lockout** option to temporarily lock an account after every authentication failure, for a fixed period of time.

> **NOTE:** This option provides some protection from brute force attacks.

Can a User be Forced to Change Their Password?

There is not a way to force a user to change their password when they next log in.

Are Passwords Displayed?

Passwords are not displayed. Passwords are always hashed on the screen.

Who Creates Users and Passwords?

Only a user with an **admin** role can create user accounts and passwords.

Configure AAA Authentication Options

The **Authentication Priority** section of the AAA page specifies which authentication methods should be used for logging in to the GigaVUE HC series node as well as the order in which they should be used.

The valid authentication the authentication methods are:

- Local database
- External authentication servers
  - RADIUS
  - TACACS+
  - LDAP

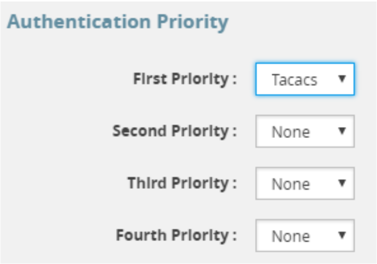
You can enable any of or all of the authentication methods ((TACACS+, RADIUS, LDAP, and local) at the same time. If you enable more than one method, the GigaVUE HC Series node uses the methods in the same order in which they are specified, falling back as necessary:

- If remote authentication is configured first followed by local, the system only falls back to local authentication method when all the remote servers are unreachable.
- If local authentication is configured first followed by remote, the system will fallback to the remote authentication method only if the user is either non-existent in the local database or the password entered does not match the local one.

Refer to the following examples.

Example 1

In this example, TACACS+ server authentication is configured as the only authentication method. Local is not included as one of the methods. Therefore, the node will be authenticated exclusively by the TACACS+ server:



Authentication Priority

First Priority : Tacacs

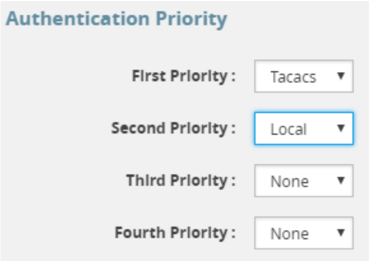
Second Priority : None

Third Priority : None

Fourth Priority : None

Example 2

In this example, TACACS+ server authentication is configured with first priority followed by Local authentication. If TACACS+ server is reachable, the local method will not be checked. If the TACACS+ server becomes unreachable, the system will fall back to local authentication method only when all the TACACS+ servers are unreachable:



Authentication Priority

First Priority : Tacacs

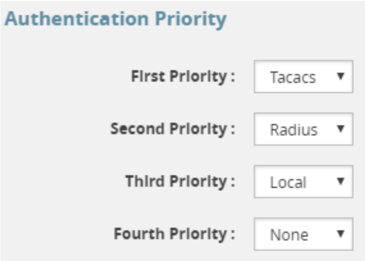
Second Priority : Local

Third Priority : None

Fourth Priority : None

Example 3

In this example, the local method will only be checked if neither the TACACS+ server or the RADIUS servers are reachable:



Authentication Priority

First Priority : Tacacs

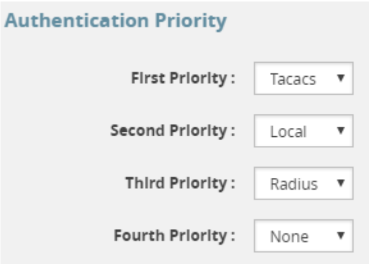
Second Priority : Radius

Third Priority : Local

Fourth Priority : None

Example 4

In this example, if the TACACS+ server is not reachable, the next method in order will be checked, which is local:



Authentication Priority

First Priority : Tacacs

Second Priority : Local

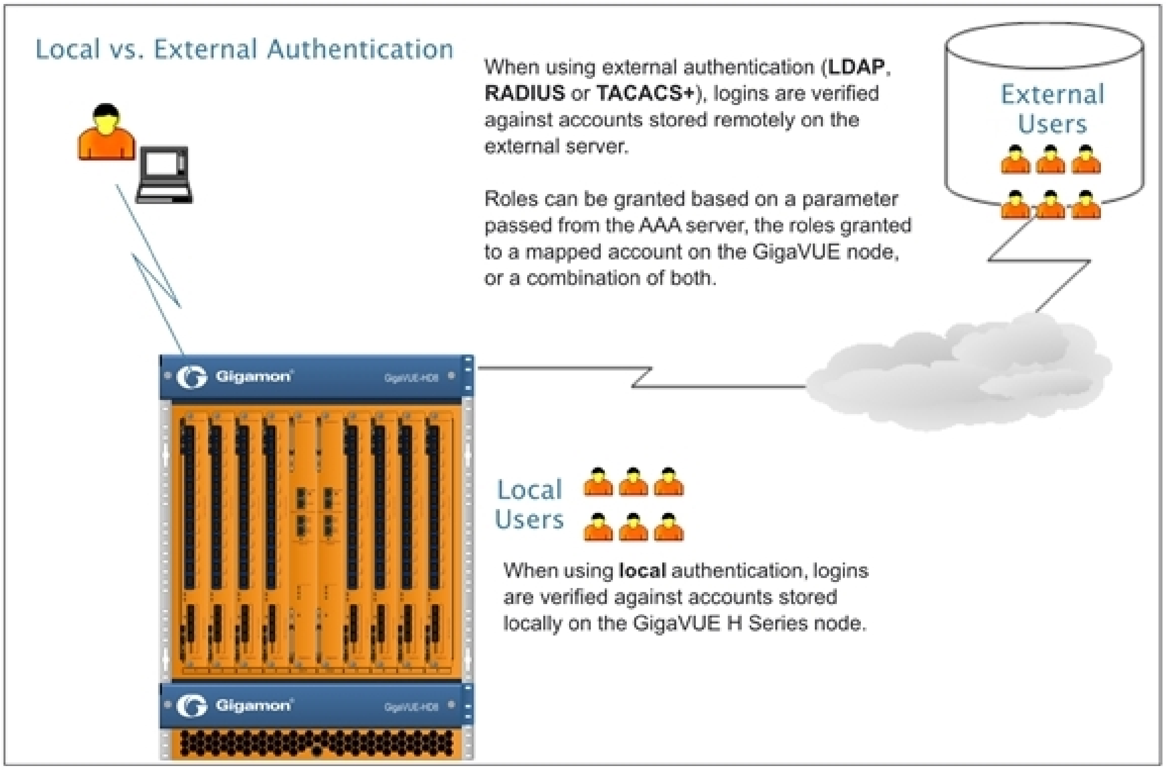
Third Priority : Radius

Fourth Priority : None

> **NOTE:** To prevent lockouts, it is recommended that you include **local** as one of the methods. However, the **local** method is optional.

For example, you could use an external authentication server as your primary authentication method with local authentication as a fallback (Figure 6Local vs. External Authentication). The fallback is used when an authentication server is unreachable.

> **NOTE:** If a server responds to a login attempt with an authentication reject, then next configured server is tried. If all the servers are unreachable, the next method is tried until either the user's login is granted or all specified methods are exhausted.



When using external authentication (**LDAP**, **RADIUS** or **TACACS+**), logins are verified against accounts stored remotely on the external server.

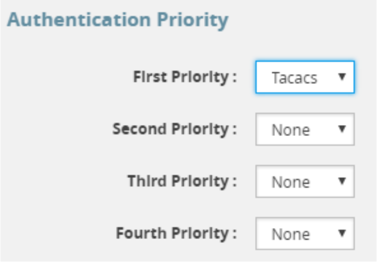
Roles can be granted based on a parameter passed from the AAA server, the roles granted to a mapped account on the GigaVUE node, or a combination of both.

When using **local** authentication, logins are verified against accounts stored locally on the GigaVUE H Series node.

Figure 6 *Local vs. External Authentication*

Remote Authentication Only

If you want to have the node authenticated exclusively by a remote server, do not include local as one of the methods in the **Authorization Priority**:



Authentication Priority

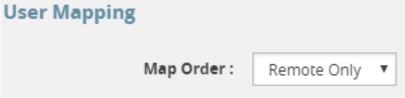
First Priority : Tacacs

Second Priority : None

Third Priority : None

Fourth Priority : None

Also, configure remote-only authorization by selecting **Remote Only** for **Map Order** under **User Mapping** on the AAA page as shown in the following figure.



User Mapping

Map Order : Remote Only

When AAA authentication is configured to a single method and authorization is configured to remote-only, there is no fallback.

When local is not in the default login order, there will be no way to access the local default users in the node’s database. If the connection to the remote server is no longer available, no further authentication will be made.

If this happens, the only option is to use a password recovery process which requires a reboot of the node. Refer to Contact Technical Support on page 345.

Authorization of User Account

If a user account exists on the remote server as well as on the local device, the remote user will be mapped to the local account, regardless of the LDAP mapping policy.

Next Steps

If you enable **RADIUS**, **TACACS+**, or **LDAP**, you must also:

- Add the RADIUS, TACACS+, or LDAP server to the GigaVUE HC Series node’s list using the corresponding **RADIUS**, **TACACS+**, or **LDAP** pages. Refer to Add AAA Servers to the Node’s List.
- Set up GigaVUE H series nodes and users within the external authentication server itself. Depending on your authorization model, you can grant privileges to externally authenticated users based on the roles assigned to a corresponding account on the local node, the roles passed from the AAA server, or a combination of both. Refer to Grant Roles with External Authentication Servers for details.

Grant Roles with External Authentication Servers

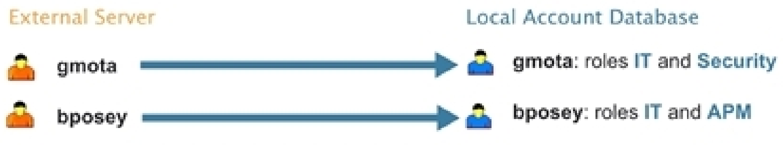
Roles are configured on the GigaVUE HC Series node itself. Roles consist of a set of ports and permission levels specifying what a user with the role assigned can do on the port.

The assignment of roles to users can be performed using any of the following techniques:

- Use Local Role Assignments
- Use AAA Server Role Assignments
- Use Combination of Local and AAA Role Assignments

Use Local Role Assignments

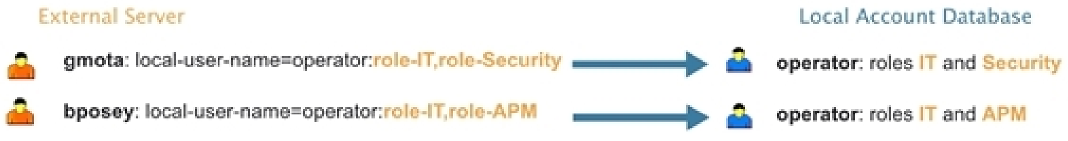
In this model, an externally authenticated user is granted the roles assigned to the account on the GigaVUE node itself. This can take place either by a matching account name (the same account name is specified both in the AAA server and the GigaVUE H Series node), or by using the **local-only** option to map all externally authenticated users to a specific account on the GigaVUE node.



In this model, matching accounts are configured both in the external server and the local account database. The AAA account automatically receives all roles assigned to the matching account on the GigaVUE node.

Use AAA Server Role Assignments

In this model, you configure the GigaVUE node to accept roles passed from the AAA server. Then, you set up a **local-user-name** attribute for the account in the AAA server to pass a reserved account name (**operator**) and one or more roles to the GigaVUE node. In this case, the roles are fully assigned in the AAA server and there are no matching accounts on the GigaVUE node.

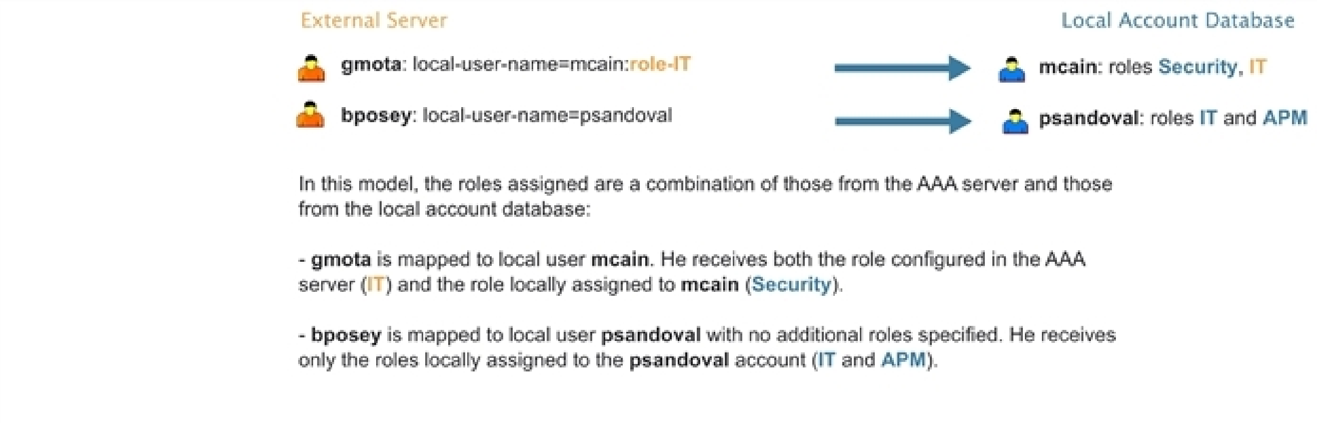

External Server
Local Account Database
gmota: local-user-name=operator:role-IT,role-Security
operator: roles IT and Security
bposey: local-user-name=operator:role-IT,role-APM
operator: roles IT and APM

In this model, there are no matching accounts configured on the GigaVUE node.
The local-user-name attribute configured in the AAA server specifies a special reserved **operator** account to be used on the GigaVUE node with the roles assigned.

Use Combination of Local and AAA Role Assignments

In this model, you configure the GigaVUE node to accept roles passed from the AAA server. Then, you set up a **local-user-name** attribute for the account in the AAA server that maps it to an existing local user account on the GigaVUE node. The **local-user-name** attribute can optional include additional roles to be assigned to the user in addition to those already assigned to the targeted local user account.

For example, in the following figure, the **gmota** account does not exist on the GigaVUE node. It has a **local-user-name** attribute that specifies the account should be mapped to the local user account **mcain**. The **Security** role is already locally assigned to **mcain**; the **IT** role comes from the AAA server with the **role-IT** argument.


External Server
Local Account Database
gmota: local-user-name=mcain:role-IT
mcain: roles Security, IT
bposey: local-user-name=psandoval
psandoval: roles IT and APM

In this model, the roles assigned are a combination of those from the AAA server and those from the local account database:

- **gmota** is mapped to local user **mcain**. He receives both the role configured in the AAA server (IT) and the role locally assigned to **mcain** (Security).

- **bposey** is mapped to local user **psandoval** with no additional roles specified. He receives only the roles locally assigned to the **psandoval** account (IT and APM).

Assign Role in AAA Servers

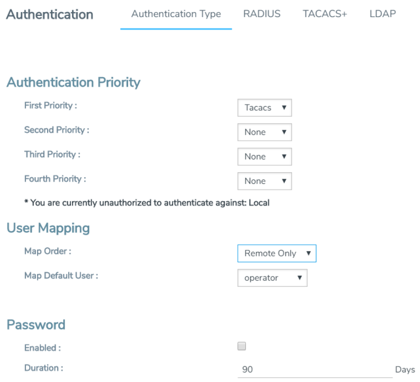
Refer to Configure Roles in External Authentication Servers for instructions on how to set up users with local-user-name attributes in RADIUS, TACACS+, and LDAP AAA servers.

Create Users for AAA and Remote Authentication Server

To create users for AAA and the remote authentication server:

1. Log in to the GigaVUE node as the administrator, externally authenticated.
2. Create a local role, for example, netops.
3. Create a local user, for example, networker.
4. Login to your authentication server as the administrator.
5. Create a user with the same name, for example, networker,
6. Create a role with the same name, for example, netops.
7. Either change the authorization rule or add a new rule for the netops group. Be careful not to lockout any users not in this group.

To display or create this configuration, select **Settings > Authentication > AAA**. The example configuration is shown in the following figure.



Authentication Priority

First Priority : Tacacs

Second Priority : None

Third Priority : None

Fourth Priority : None

* You are currently unauthorized to authenticate against: Local

User Mapping

Map Order : Remote Only

Map Default User : operator

Password

Enabled : □

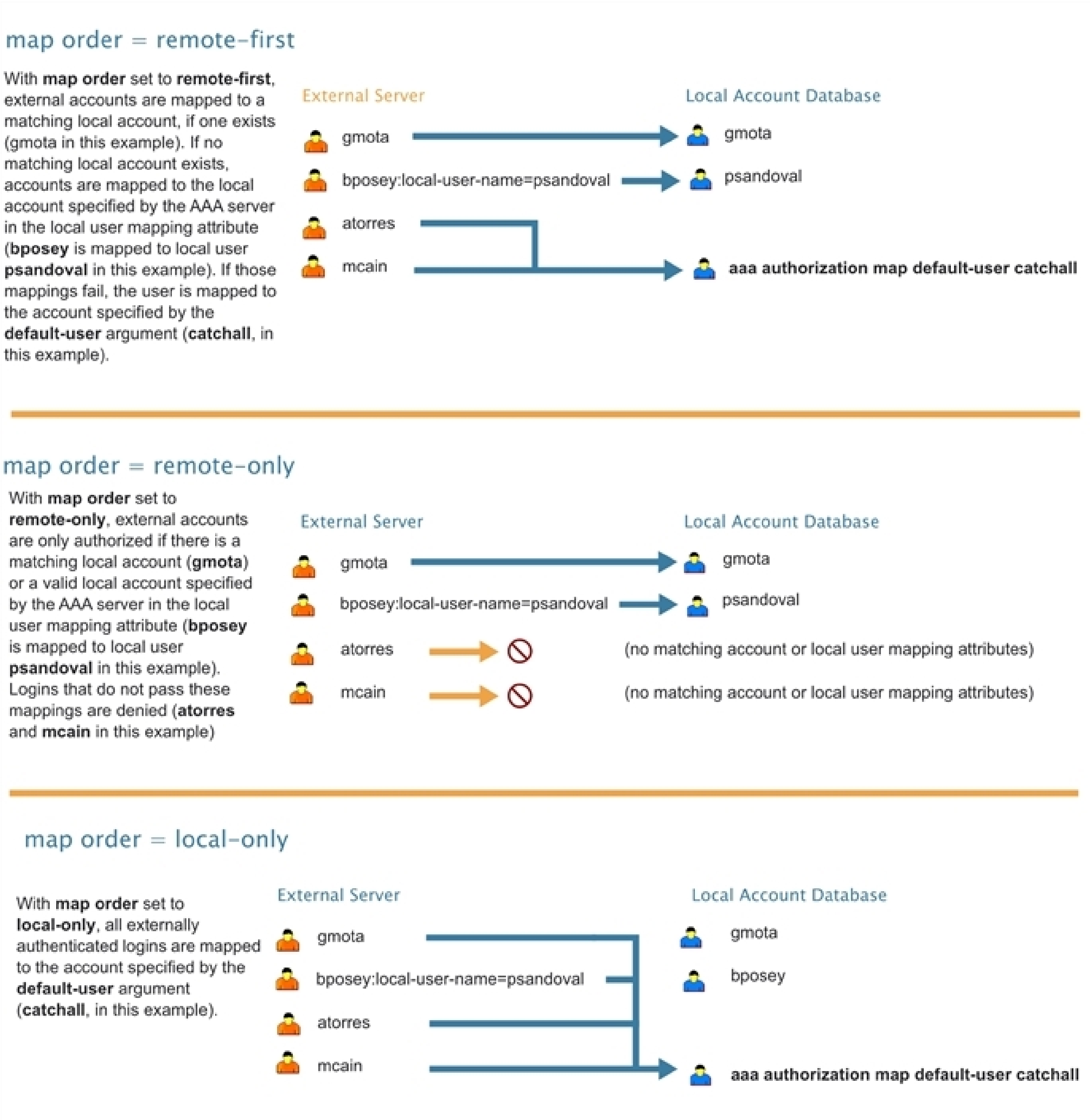
Duration : 90 Days

The settings in the example configuration are as follows:

- AAA authorization:
  - Map Order: Remote Only means the user has a local account matching the external username account.
  - Map Default User: networker is a common user member of internal netops role and TACACS+ netops group.
- Authentication method(s):
  - Tacacs means that TACACS+ is the only authentication method.

Configure AAA Authorization

For details on the AAA authorization command, refer to Overview of the AAA Page.



map order = remote-first

With **map order** set to **remote-first**, external accounts are mapped to a matching local account, if one exists (gmota in this example). If no matching local account exists, accounts are mapped to the local account specified by the AAA server in the local user mapping attribute (**bposey** is mapped to local user **psandoval** in this example). If those mappings fail, the user is mapped to the account specified by the **default-user** argument (**catchall**, in this example).

External Server
Local Account Database
gmota
bposey:local-user-name=psandoval
atorres
mcain
gmota
psandoval
aaa authorization map default-user catchall

map order = remote-only

With **map order** set to **remote-only**, external accounts are only authorized if there is a matching local account (**gmota**) or a valid local account specified by the AAA server in the local user mapping attribute (**bposey** is mapped to local user **psandoval** in this example). Logins that do not pass these mappings are denied (**atorres** and **mcain** in this example)

External Server
Local Account Database
gmota
bposey:local-user-name=psandoval
atorres
mcain
gmota
psandoval
(no matching account or local user mapping attributes)
(no matching account or local user mapping attributes)

map order = local-only

With **map order** set to **local-only**, all externally authenticated logins are mapped to the account specified by the **default-user** argument (**catchall**, in this example).

External Server
Local Account Database
gmota
bposey:local-user-name=psandoval
atorres
mcain
gmota
bposey
aaa authorization map default-user catchall

Figure 7 *How the **map order** Argument Works*

Example

The following steps demonstrate how to set up authentication using RADIUS with a fallback to local if no RADIUS server is available. Select **Settings > Authentication > AAA**.

8. On the AAA page, do the following:

   Use RADIUS authentication first, followed by local authentication.

- Set **First Priority** to **Radius**.
- Set **Second Priority** to **Local**.

If the external user also exists in the local database, use the specified local account. Otherwise, use the account specified by Map Default User.

If the external user does not exist in the local database, use the **admin** account instead. This is only done if **Map Order** is set to **Remote First** or **Local**.

- Set **Map Order** to **Remote First**.
- Set **Map Default User** to **admin**.

Click **Save** to save the configuration.

9. Add a RADIUS Server.

   These steps add a RADISU server at IPv4 address 192.168.0.62 to the GigaVUE HC Series node's list.

   a. Select **Settings > Authentication > Radius**.

   b. Click **Add**. The Add Radius Server page displays.

   c. For **Enabled** select **Yes**.

   d. In the **Server IP** field, enter 192.168.0.62

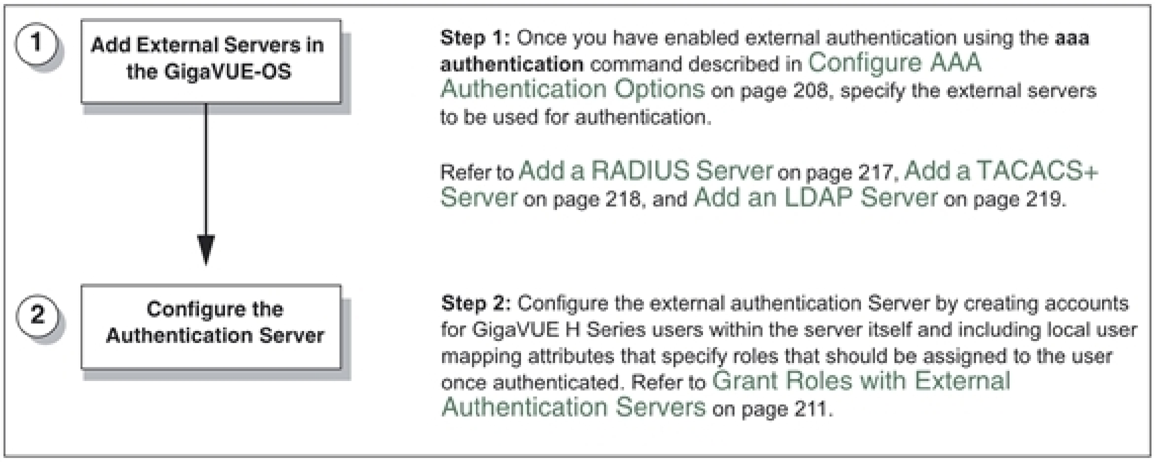
   e. In the **Key** field, enter gigamon.

   f. Click **Save**.

10. Allow the RADIUS server to include additional roles for a remotely authenticated user in the response. Refer to Grant Roles with External Authentication Servers.

Add AAA Servers to the Node's List

If you enable an external authentication option (RADIUS, TACACS+, or LDAP) with the **AAA**, you must also perform some additional configuration tasks, both within the GigaVUE node and the external server itself:


1
Add External Servers in the GigaVUE-OS
2
Configure the Authentication Server

Step 1: Once you have enabled external authentication using the **aaa authentication** command described in Configure AAA Authentication Options on page 208, specify the external servers to be used for authentication.

Refer to Add a RADIUS Server on page 217, Add a TACACS+ Server on page 218, and Add an LDAP Server on page 219.

Step 2: Configure the external authentication Server by creating accounts for GigaVUE H Series users within the server itself and including local user mapping attributes that specify roles that should be assigned to the user once authenticated. Refer to Grant Roles with External Authentication Servers on page 211.

Figure 8 *Steps to Use the Node with an External Authentication Server*

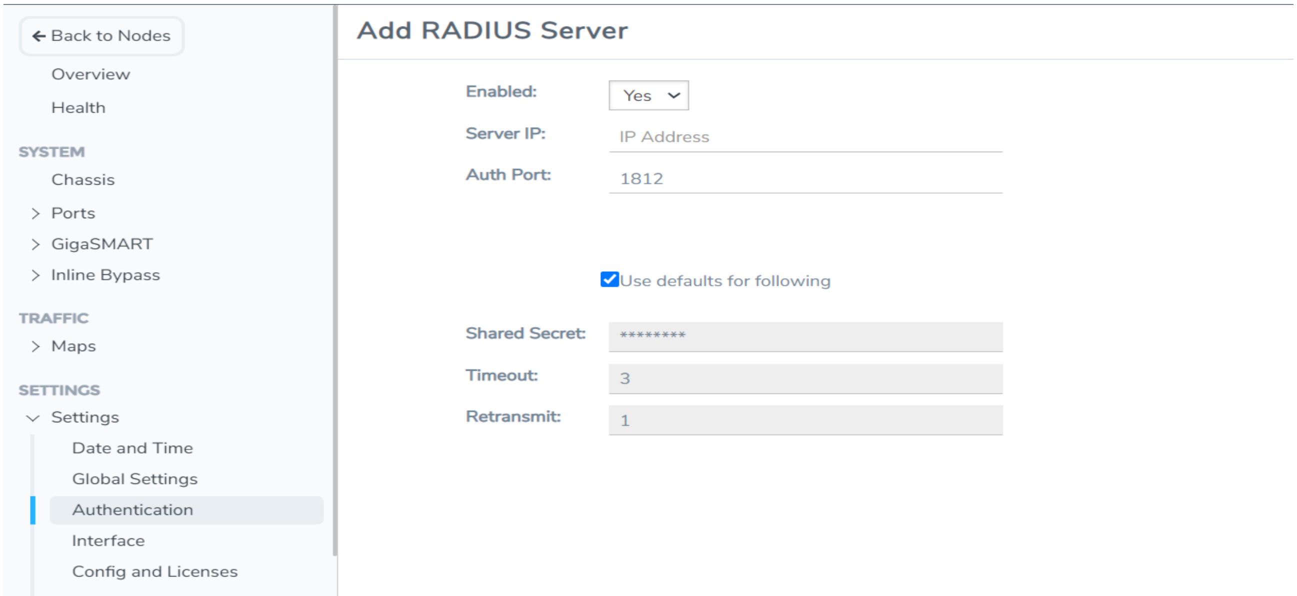
Add a RADIUS Server

Admin users use the **RADIUS** page to specify the RADIUS servers to be used for authentication. You can specify 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.

To Add a RADIUS server, do the following:

1. Select **Settings > Authentication > RADIUS**.
2. Click **Add**.
3. Enter the RADIUS information on the ADD Radius page. For an example, refer to Figure 9Adding a Radius Server.

   You can enter either an IPv4 or IPv6 address for the **Server IP**. The same IP address can be used for more than one RADIUS server if the **Auth Port** values are different.
4. Click **Save**.



Add RADIUS Server

Enabled: Yes

Server IP: IP Address

Auth Port: 1812

☑ Use defaults for following

Shared Secret: ********

Timeout: 3

Retransmit: 1

Figure 9 *Adding a Radius Server*

Delete a RADIUS Server

To delete a RADIUS server, do the following:

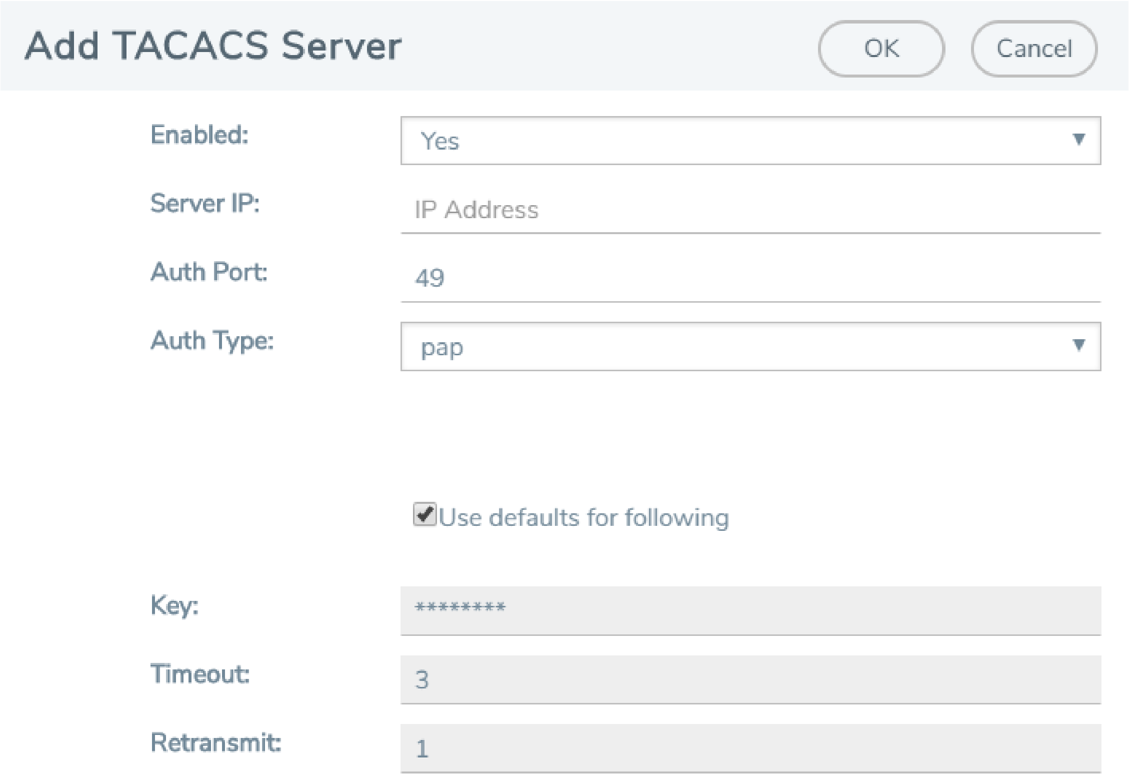
1. Select **Settings > Authentication > RADIUS**.
2. Select the RADIUS server to delete.
3. Click **Delete**.

Add a TACACS+ Server

Admin users use the TACACS+ page to specify the TACACS+ servers to be used for authentication. You can specify 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.

To Add a RADIUS server, do the following:

1. Select **Settings > Authentication > TACACS+**.
2. Click **Add**.
3. Enter the RADIUS information on the ADD TACACS Server page. For an example, refer to Figure 10Adding a TACACS Server
4. Click **Save**.



Enabled:	Yes ▾
Server IP:	IP Address
Auth Port:	49
Auth Type:	pap ▾

☑ Use defaults for following

Key:	********
Timeout:	3
Retransmit:	1

Figure 10 *Adding a TACACS Server*

Delete a TACACS+ Server

To delete a RADIUS server, do the following:

1. Select **Settings > Authentication > TACACS+**.
2. Select the TACACS+ server to delete.

3. Click **Delete**.

Configure an IPv6 Address

To configure an IPv6 address for a TACACS+ server, enter the IPv6 address in the Server IP filed on the Add TACACS Server page (select **Settings > Authentication > TACACS > Add**.)

> **NOTE:** To use IPv6 addresses, you must use the CLI to enable IPv6 through the configuration jump-start wizard. For more information, refer to the *GigaVUE-OS CLI Reference Guide*.

Add an LDAP Server

Admin users use the **LDAP** page to specify the LDAP servers to be used for authentication. You can specify 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.

To add an LDAP Server, do the following:

1. Select **Settings > Authentication > LDAP**.
2. Click **Add**.
3. Enter the IP address of the LDAP server in the **Server IP** field.
4. Enter the priority.
5. Click Save.

For Common Criteria, specify SHA password hashing when configuring the remote LDAP server. For details on Common Criteria, refer to Common Criteria.

Set the LDAP Server Default Settings

After adding an LDAP Server, do the following to specify the default settings:

1. Select **Settings > Authentication > LDAP**.
2. Select the LDAP Server, and then click **Default Settings**.
3. Enter or select the settings for the LDAP server on the **Edit LDAP Server Default Settings** page, and then click **Save**. The settings are described in Table 2: LDAP Default Settings

Table 2: LDAP Default Settings

Default Setting	Description
User Base DN	Identifies the base distinguished name (location) of the user information in the LDAP server's schema. Specify this by identifying the organizational unit (ou) in the base DN. Provide the value as a string with no spaces. For example: **ou=People,dc=mycompany,dc=com** This is a global setting. It cannot be configured on a per-host basis.
User Search Scope	Specifies the search scope for the user under the base distinguished name (dn): ● **subtree**—Searches the base dn and all of its children. This is the default. ● **one-level**—Searches only the immediate children of the base dn. This is a global setting. It cannot be configured on a per-host basis.
Login UID	Specifies the name of the LDAP attribute containing the login name. You can select ● **uid** (for User ID) ● **sAMAccountName** ● **custom attribute** and provide a string for the custom attribute name This is a global setting. It cannot be configured on a per-host basis.
Bind Password	Provides the credentials to be used for binding with the LDAP server. If **Bind DN** is undefined for anonymous login (the default), **Bind Password** should also be undefined. This is a global setting. It cannot be configured on a per-host basis.
Group Base DN	Specifies that membership in the named **Group Base DN** is required for successful login to the GigaVUE H Series node. 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 **Group Login Attr** must contain the user's distinguished name as one of the values in the LDAP server or the user will not be logged in. This is a global setting. It cannot be configured on a per-host basis.
Bind DN	Specifies the distinguished name (dn) on the LDAP server with which to bind. By default, this is left empty for anonymous login. This is a global setting. It cannot be configured on a per-host basis.
Group Login Attr	Specifies the name of the attribute to check for group membership. If you specify a value for Base **Group 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. You ca select on of the following: ▪ **custom attribute** ▪ **member** ▪ **uniqueMember** This is a global setting. It cannot be configured on a per-host basis.
LDAP Version	Specifies the version of LDAP to use. The default is version 3, which is the current standard. Some older servers still use version 2. This is a global setting. It cannot be configured on a per-host basis.
Port	Specifies 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.

Default Setting	Description
	This is a global setting. It cannot be configured on a per-host basis.
Timeout	Specifies how long the GigaVUE H Series node should wait for a response from an LDAP server to a bind request before declaring a timeout failure. The valid range is 0-60 seconds. The default is 5 seconds.
Extra Roles	When **Yes** is selected, enables the GigaVUE H Series node to accept user roles assigned in the LDAP server. The default is **No**.
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	Configures LDAP SSL port number.
SSL Cert Check	Enables LDAP SSL/TLS certificate verification. Use **Off** to disable.
SSL ca-list	Configures LDAP to use a supplemental CA list. Set to **default Ca list** to use the CA list configured with the **Enhanced Cryptography** (refer to Configure Enhanced Cryptography Mode). Set to **None** if you do not want to use a supplemental list.

Delete an LDAP Server

To delete an LDP Server, do the following:

1. Select **Settings > Authentication > LDAP**.
2. Select the LDAP server to delete on the LDAP Server page.
3. Click **Delete**.

Configure an IPv6 Address

To configure an IPv6 address for a LDAP server, enter the IPv6 address in the Server IP filed on the Add LDAP Server page (select **Settings > Authentication > LDAP > Add**.)

> **NOTE:** To use IPv6 addresses, you must use the CLI to enable IPv6 through the configuration jump-start wizard. For more information, refer to the *GigaVUE-OS CLI Reference Guide*.

Configure Roles in External Authentication Servers

This section describes how to set up RADIUS, TACACS+, and LDAP servers to work with GigaVUE nodes, including how to include a local user mapping attribute that the GigaVUE node can use to assign roles to an externally-authenticated user. Refer to the following sections for more details:

- Grant Roles with External Authentication Servers

- Configure Cisco ACS: RADIUS Authentication
- Configure Cisco ISE: RADIUS Authentication
- Configure Cisco ACS: TACACS+ Authentication
- Configure Cisco ISE: TACACS Authentication
- Configure LDAP Authentication

Configure Cisco ACS: RADIUS Authentication

Use the following steps to configure the Cisco Access Control System (ACS): RADIUS to grant extra roles to externally authenticated users on the GigaVUE H Series node.

> **NOTE:** The steps described below are based on CISCO ACS Version 5.x. The navigation path may vary depending on the CISCO ACS version that you use.

Enable Extra Roles for RADIUS on the GigaVUE Node

1. Go to **Settings > Authentication > RADIUS > Default Settings** to enable the GigaVUE H Series node to accept extra roles in response from the AAA server.

   > **NOTE:** The extra role must match a role already configured on the GigaVUE H Series node/cluster.

Example of Assigning the Class Attribute in RADIUS Authorization Profile (ACS 5.x)

In the Cisco Secure ACS screen:

1. Navigate to **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles.**
2. Click **Create** to add a new authorization profile.
3. Enter/select the following:

Parameter	Attribute
Dictionary Type	RADIUS-IETF
RADIUS Attribute	Class
Attribute Type	Default Value (string)
Attribute Value	Default Value (static)
Local user mapping and optional roles	Select the appropriate roles

4. Click **Add** to add this attribute to the authorization profile.
5. Assign this authorization profile to a group and populate it with GigaVUE users.

Configure Cisco ISE: RADIUS Authentication

To configure Cisco Identity Services Engine (ISE): RADIUS and to grant extra roles to externally authenticated users on the GigaVUE H Series node, perform the following:

> **NOTE:** The steps described below are based on CISCO ISE Version 5.x. The navigation path may vary depending on the CISCO ISE version that you use.

1. Create the following two users in the GigaVUE H Series Node and configure the remote server using the following commands:

CISCO ISE RADIUS Configuration	
Local user account configuration	
User 1 with admin auth profile	`username adminauthprofile password 7 $1$Nc/LLAfM$EwiU.qjNQHoqnWSaqQiNG0`

User 2 with read only auth profile	`no username nonadminauthprofile disable`
	`username nonadminauthprofile full-name ""`
	`username nonadminauthprofile roles replace monitor`

AAA remote server configuration	Assume the radius server host as 1.1.1.1. Add this radius-server to the GigaVUE-OS H series nodes list using the following commands:
	`# radius-server host 1.1.1.1`
	`# radius-server host 1.1.1.1 key ********`
	`# radius-server extra-user-params roles enable`

2. Create the following Users in ISE database:
   - User 1 must be mapped to the admin auth profile.
   - User 2 must be mapped to the read only auth profile.

> **NOTE:** Users can also be mapped from an Active Directory server.

3. Add Gigamon device to the ISE:
4. Enter the following:

Parameter	Attribute

Shared Secret Key	Configure the same shared secret key as what you have configured in Gigamon using the CLI command:
	`#radius server host x.x.x.x key <xxxxxx>`
	`#radius server host 1.1.1.1 key ******`

5. Create two Authorization Policies, one for admin user and one for read-only user.
6. Enter/select the Common Attribute Values in the ASA VPN. Do not enter Vendor specific radius attributes as they are not supported.

Parameter	Attribute
Name	Local user name If this is admin auth profile, then the username should be the same as configured in Gigamon, which is **adminauthprofile**. If this is the read-only auth profile, then the user name should be the same as configured in Gigamon, which is **nonadminauthprofile**.
Access type	ACCESS_ACCEPT
ASA VPN	Enabled **NOTE:** You must enable this to provide common attribute values.
Attribute Details	
Access Type	ACCESS_ACCEPT
class	local-user-name=**adminauthprofile**
Network Device profile	CISCO / TAP
local-user-name	adminauthprofile

7. Create a policy set that defines the authentication policy and the authorization policy. Policy pertains to conditions and actions.
8. Define the attributes that match the policy, for example you can define the attribute as 'Device type' and match all the devices.
9. Select the Allowed Protocols/Server Sequence as 'Default Network Access'.

10. Once the conditions are defined and the allowed protocols are configured, click the View option to configure authentication policy and map the authorization policy.
    - **For the authentication policy:** Define the conditions appropriately for the RADIUS packets to hit the authentication policy. For example, use the IP address of eth0 interface of Gigamon as condition and as per this policy the authentication would be done against the ISE local users.
    - **For the authorization policy**: Define two rules and based on these rule conditions, the authorization policy created in the previous step will be triggered.
11. If you enter the username as **adminauthprofile** while accessing the Gigamon devices via SSH/GUI, the admin auth profile is triggered. The corresponding attribute values defined in this authorization profile in the RADIUS response packet would be sent by the ISE. Based on these values, Gigamon would map this user to an user in its local database and hence the remote user gets authorized.
12. If you enter the username as **nonadminauthprofile** while accessing the Gigamon devices, as this user belongs to the monitor group in ISE, the non admin auth profile is triggered and the corresponding attribute values in the radius response packet is sent by the ISE.

Configure Cisco ACS: TACACS+ Authentication

Use the following steps to configure Cisco ACS: TACACS+ to grant extra roles to externally authenticated users on the GigaVUE H Series node.

> **NOTE:** The steps described below are based on CISCO ACS Version 5.x. The navigation path may vary depending on the CISCO ACS version that you use.

Enable Extra Roles for TACACS+ on the GigaVUE H Series Node

1. Go to **Settings > Authentication > TACACS > Default Settings** to enable the GigaVUE H Series node to accept extra roles in the response from the AAA server.

   > **NOTE:** The extra role must match a role already configured on the GigaVUE node/cluster.

Example of Assign local-user-name to Shell Profile (ACS 5.x)

2. Navigate to **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles.**
3. **C**lick **Create** to add a new shell profile.
4. Enter/select the following:

Parameter	Attribute
General	Profile Name and Description
Custom Attributes	
Attribute	local-user-name
Requirement	Default Value (Mandatory)
Attribute Value	Default Value (Static)
local user mapping and optional roles	

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

Configure Cisco ISE: TACACS Authentication

To configure Cisco ISE: TACACS and to grant extra roles to externally authenticated users on the GigaVUE H Series node, perform the following steps:

> **NOTE:** The steps described below are based on CISCO ISE Version 5.x. The navigation path may vary depending on the CISCO ISE version that you use.

1. Create the following two users in the GigaVUE H Series Node and configure the remote server using the following commands:

CISCO ISE RADIUS Configuration	
Local user account configuration	
User 1 with admin auth profile	`username adminauthprofile password 7 $1$Nc/LLAfM$EwiU.qjNQHoqnWSaqQiNG0`

User 2 with non admin auth profile (that replaces the monitor role)	`no username nonadminauthprofile disable`
	`username nonadminauthprofile full-name ""`
	`username nonadminauthprofile roles replace monitor`

AAA remote server configuration	Assume tacacs server host as 1.1.1.1 and shared key as *******.
	`tacacs-server host 1.1.1.1`
	` timeout 5 retransmit 3`
	`# tacacs-server host 1.1.1.1 key ********`
	`#tacacs-server extra-user-params roles enable`
	`# tacacs-server key ********`
	`tacacs-server retransmit 3`
	`tacacs-server service Gigamon`
	`tacacs-server timeout 5`

AAA Configuration	`aaa authentication login default tacacs+ local`
	`aaa authorization map default-user monitor`
	`aaa authorization map order remote-first`

2. Create the following users in ISE database:
   - User 1 must be mapped to Admin group
   - User 2 must be mapped to monitor group
3. Add Network devices to ISE.
4. Enter the following:

Parameter	Attribute
Shared Secret Key	Configure the same as what you have configured in Gigamon using the CLI command: `tacacs-server host 1.1.1.1 key ********`

5. Create Shell profiles for each of the users.

6. The shell profiles in TACACS is very similar to the Authorization profile in radius. Once the device is authenticated successfully, the custom attribute which is defined under the shell profile is sent to Gigamon in the TACACS response packets for the authorization to work. Similar to the RADIUS auth profile, the shell profile should have the exact username, defined as the value under Custom attributes (Attribute name: local-user-name).

   > **NOTE:** This username should match the ones you configured in the Gigamon local database)

7. Create a policy set which pairs the authentication policy and the TACACS shell policy. Similar to the policy created in RADIUS section, create one for the TACACS authentication and authorization to work.
8. Login to the device using the appropriate accounts / usernames.

Configure LDAP Authentication

Use the following steps to configure an LDAP server (for example, Apache Directory Server) to grant extra roles to externally authenticated users on the GigaVUE H Series node.

1. Enable Extra Roles for LDAP on the GigaVUE H Series.

   To enable the GigaVUE H Series node to accept extra roles in the response from the AAA server:

   a. Select **Settings > Authentication > LDAP.**

   b. Click **Default Settings**.

   c. Set the **Extra Roles** field to **Yes**.

   > **NOTE:** The extra role must match a role already configured on the GigaVUE node or cluster.

2. Assign local-user-name to Shell Profile (ACS 5.x).

   To assign a local-user-name to Shell Profile (ACS 5.x), add an **employeeType** attribute to the InetOrgPerson user object.

   The attribute format is as follows:

```
        <mapping_local_user>[:role-<mapping_local_role_1> [role-<mapping_local_role_2>
[...]]]
```

Supported Clients

The following versions of serial, SSH clients are supported:

Table 3: Tested SSH Clients

OS	Client	Version
Windows 7, Windows 10	PuTTY	0.64
Windows 7, Windows 10	Tera Term	4.87
Windows 7, Windows 10	Cygwin	1.1.6
Linux Ubuntu L4.5	Tera Term	4.87
Linux Ubuntu L4.4	LXTerminal	0.2.0
OSX 10.12 (16A323)	Term2	3.010
OSX 10.12 (16A323)	vSSH	1.11.1

Default Ports

The following default ports are normally open on GigaVUE nodes:

Table 4: Open Default Ports

Port Number	Protocol	Description	Service/Server
22	TCP	SSH	OpenSSH_8.8p1
80	TCP	HTTP	Apache httpd
161	UDP	SNMP	SNMP
443	TCP	HTTPS	Apache httpd
9090	TCP	APIs	Gigamon

Other default ports are normally closed on GigaVUE nodes, unless configured:

Table 5: Default Ports, Normally Closed

Port Number	Description
20	FTP
49	TACACS+
123	NTP
162	SNMP host
389	LDAP

Port Number	Description
514	syslog
1080	Web proxy
1812	RADIUS
2055	NetFlow Collector

The following table contains examples of other valid ports, depending on vendor:

Table 6: Other Valid Ports

Port Number	Description
53	DNS
25/465/587	SMTP
319/120	PTP
256	Route Access Protocol (RAP)
512	Binary Interchange File Format (BIFF)

FIPS 140-2 Compliance

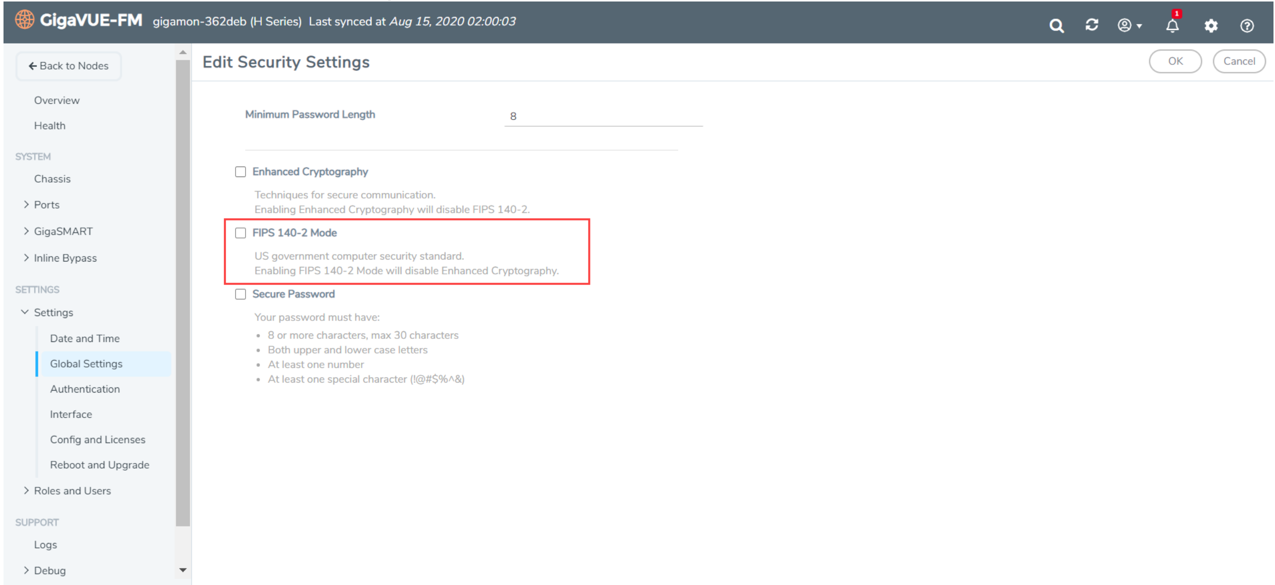
GigaVUE-OS is compliant with the Federal Information Processing Standard (FIPS), a US government standard for security requirements of cryptographic modules. The Gigamon Linux-based cryptographic module (the FIPS module) provides cryptographic functions for GigaVUE nodes and offers a high level of security for the Ethernet management interface. The FIPS module is compliant with FIPS 140-2 Level 1 and was validated by the National Institute of Standards and Technology (NIST). The certificate number is 2128.

Also, OpenSSL is integrated with the FIPS module and is updated to version 1.0.2zf.

To enable FIPS:

1. Select **Settings > Global Settings > Security**.
2. Click **Edit**.
3. On the **Edit Security Settings** page, select **FIPS 140-2 Mode**.

4. Click **OK** to save the changes.



Edit Security Settings

Minimum Password Length: 8

☐ Enhanced Cryptography

Techniques for secure communication.
Enabling Enhanced Cryptography will disable FIPS 140-2.

☐ FIPS 140-2 Mode

US government computer security standard.
Enabling FIPS 140-2 Mode will disable Enhanced Cryptography.

☐ Secure Password

Your password must have:

- 8 or more characters, max 30 characters
- Both upper and lower case letters
- At least one number
- At least one special character (!@#$%^&)

Once FIPS is enabled, the device will reload and the device configuration will be reset. All traffic, keys and certification configurations will be cleared.

For communications with the GigaVUE node, SSL or SSH clients are requested to use high strength ciphers during the session set up negotiation. A high strength cipher is one that uses a key that is equal to or greater than 128 bits.

Weak ciphers will be rejected by the GigaVUE node. For example, if a client attempts to connect to the GigaVUE Ethernet management port using blowfish, the following error message will be displayed: *No matching cipher found*.

UC APL Compliance

GigaVUE HC Series products are compliant with Unified Capabilities Approved Products List (UC APL). The products include the GigaVUE-HC2, as well as the GigaVUE-TA10 and GigaVUE-TA40.

UC APL certification ensures that the GigaVUE HC Series products comply with Internet Engineering Task Force (IETF) and Defense Information Systems Agency (DISA) standards on Internet Protocol (IP) devices. The UC APL certification verifies that the GigaVUE H Series products comply with and are configured to be consistent with the DISA Field Security Office (FSO) Security Technical Implementation Guides (STIG).

Certified equipment is listed on the US Department of Defense (DoD) UC APL list.

UC APL requires the GigaVUE HC Series products run the most current version of the Apache branch to ensure the most secure version is used. The component versions of Apache on GigaVUE HC Series products are as follows:

- httpd 2.4.54
- apr 1.6.3
- apr-util 1.6.1
- pcre 7.8

Configure UC APL

To make a system UC APL compliant, the following configuration steps are required:

- accept only HTTPS web server certificates from a DoD authorized certificate authority. Refer to Accept DoD Web Server Certificates.
- enable login failure tracking. Refer to Enable Login Failure Tracking.

Accept DoD Web Server Certificates

UC APL requires that the web server only accept certificates from a DoD authorized certificate authority. By default, this is disabled. Use the following CLI command to enable it:

```
(config) # web https require-dod-cert
```

Disable acceptance of DoD web server certificates with the following CLI command:

```
(config) # no web https require-dod-cert
```

Enable Login Failure Tracking

UC APL requires that login failure tracking be enabled. By default, this is disabled. Use the following CLI command to enable it:

```
(config) # aaa authentication attempts track enable
```

Disable login failure tracking with the following CLI command:

```
(config) # no aaa authentication attempts track enable
```

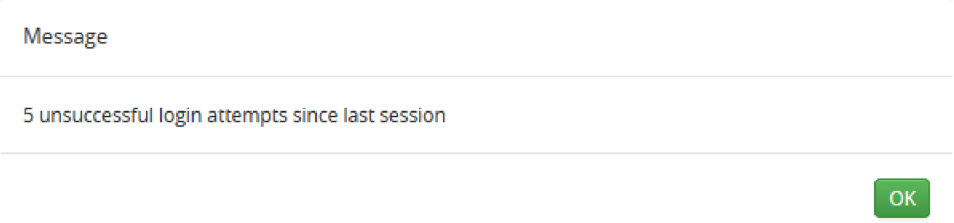
Unsuccessful login attempts are displayed on the CLI. Refer to Display Unsuccessful Login Attempts.

Display Unsuccessful Login Attempts

UC APL requires the system display the number of unsuccessful login attempts since the last successful login for a particular user when they log in. An unsuccessful login attempt includes an incorrect username or incorrect password.

After an unsuccessful login attempt, there is a delay of a few seconds before you can attempt to log in again.

If there has been an unsuccessful login attempt, a message is displayed in the UI when you successfully log in.



Message

5 unsuccessful login attempts since last session

If there have not been any unsuccessful login attempts, no message is displayed.

Common Criteria

The Common Criteria for Information Technology Security Evaluation, or Common Criteria, is an international standard (ISO/IEC 15408) for computer security certification.

Common Criteria is a framework in which computer system users can specify their security functional requirements and security assurance requirements (SFRs and SARs, respectively) through the use of Protection Profiles (PPs), vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if those claims are met.

Common Criteria provides assurance that the process of specification, implementation, and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner, at a level that is commensurate with the target environment for use.

Common Criteria is used as the basis for a Government driven certification scheme. Typically, evaluations are conducted for the use of Federal Government agencies and critical infrastructure.

Gigamon is actively keeping our products certified. Visit the NIAP CCEVS website to see the current GigaVUE-OS and models that are currently certified or check which version of the GigaVUE-OS is currently in-evaluation.

Configure Common Criteria

To make a GigaVUE node certified with Common Criteria, the following configuration steps are required:

- enable enhanced cryptography mode. Refer to Configure Enhanced Cryptography Mode.
- enable secure passwords mode and configure a password length of 15. Refer to Configure Secure Passwords Mode.
- configure syslog to send audit data securely. Refer to Encrypt Syslog Audit Data.

Configure Enhanced Cryptography Mode

A GigaVUE node can be put into enhanced cryptography mode to improve the security of the management interface. In enhanced cryptography mode, weak encryption/decryption and hashing algorithms, used for accessing data and generating keys, are disabled. The enhanced cryptography mode limits the cryptographic algorithms, hashing algorithms, and SSH transport protocols, that are available for use on a GigaVUE node.

The enhanced cryptography mode is disabled. There are two steps to enable it: configuring the mode, and then reloading either the node, if it is standalone, or the cluster, if the node is in a cluster environment.

> **NOTE:** Refer to the GigaVUE Release Notes for the latest browser support information for Secure Cryptography Mode.

Enable Enhanced Cryptography Mode

To enable enhanced cryptography mode do the following:

1. Select **Settings > Global Settings > Security**.
2. Click **Edit**.
3. On the **Edit Security Settings** page, select **Enhanced Cryptography**.
4. Click **Save**

If you enable enhanced cryptography, then FIPS mode will be disabled.

Ciphers to Use with Enhanced Cryptography Mode

Use the following ciphers with enhanced cryptography mode:

Secure Cryptography Mode
All Platforms
AES128-CBC AES256-CBC

> **NOTE:** Refer to the GigaVUE Release Notes for the latest cipher support information in Secure Cryptography Mode.

Use the following ciphers with normal (non-secure) cryptography mode:

Normal Cryptography Mode		
GVCCV2	**Other PowerPC Platforms**	**Intel Platforms**
AES128-CTR AES192-CTR AES256-CTR	AES128-CTR AES192-CTR AES256-CTR	AES128-CTR AES192-CTR AES256-CTR AES128-CBC AES256-CBC

Cryptographic Algorithms

When enhanced cryptography mode is enabled, the cryptographic algorithms are limited as follows:

SSH Host Key Algorithm	SSH Key Exchange	Encryption Algorithms	Hash-based Message Authentication Code
ECDSA	Diffie-Hellman-group14-sha1	AES128-CBC, AES256-CBC	HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-512

Status of Enhanced Cryptography Mode

If enhanced cryptography mode is configured on a GigaVUE node, once the node or cluster has been reloaded, a status is displayed when you log in.

Configure Secure Passwords Mode

Passwords that are complex and long in length provide security. To to enable the secure passwords mode:

1. Select **Settings > Global Settings > Security**. The Security page displays. Secure Passwords are disabled by default.
2. Click **Edit**.
3. On the Edit Security Settings page, select **Secure Passwords**.
4. In the **Min Password Length** field, specify the minimum password length from 8 to 64 characters.

   For Common Criteria certification, the password length should be at least 15 characters.
5. Click **Save**.

   The system displays the following notification:

Security settings updated successfully. Please reboot the device for the settings to take effect.

6. To reboot the system:
   a. Select **Settings > Reboot and Upgrade**.
   b. Click **Reboot**.

When you create a password from the User Setup page, the password must contain at least one character of each of the following:

- uppercase letters
- lowercase letters
- numbers
- special characters, for example, !, @, #, $, %, ^, &, or *

The minimum number of characters allowed is determined by the Secure Passwords setting if it is enabled.

For example, use the following steps to create and set the password for a user named myuserid user:

1. Select **Roles and Users > Users**.
2. On the User Setup page, click **Add**. The Add New User page appears.
3. Enter the account details for the user. If the password does not adhere to the rules, a message is displayed.
4. After completing the account details, click **Save**.

Encrypt Syslog Audit Data

Syslog audit data, such as messages and traps, are usually sent unencrypted between a GigaVUE node and the syslog server using UDP over port 514. The messages are sent in plain text. To allow secure transmission, starting in software version 4.4, you can send encrypted syslog audit data by using TCP and SSH options.

Sending syslogs over TCP provides a more reliable transport than UDP, with no dropped data. Tunneling using SSH provides encryption of syslog data.

On the GigaVUE node, the procedure for sending encrypted syslog audit data is as follows:

- identify the TCP port on which the syslog server is listening. (Refer to your syslog server administrator for the port number.)
- configure the TCP port of the syslog server on the GigaVUE node
- generate a public key to allow authentication between the GigaVUE node and the syslog server
- configure a secured connection

On the syslog server, integrate the key into the authorized keys.

> **NOTE:** There can be multiple logging servers. SSH is optional for each logging server.

Encryption Procedure

Use the following sample procedure to encrypt syslog audit data:

1. Generate the public key (for example, using the admin user) with the following steps.

   > **NOTE:** The SSH Server needs to be enabled before completing these steps.

   a. Select **Settings > Global Settings > SSH**.

   b. Click **Add**. The SSH Client Key page appears.

   c. In the **Username** field, enter admin and select **rsa2** for **Type**.

   d. Click Generate **Client Keys** and copy the key contents.

2. Log in to the syslog server to paste the key, and then do the following:

   a. Change the directory to .ssh.

   b. Edit the authorized_keys file, located in the .ssh directory, using any editor (such as vi), then paste the key contents.

   If the authorized_keys file does not exist, create it

   If the authorized_keys file exists but does not have write access, change the access; for example, `chmod 644 authorized_keys`

   c. Change the access on the authorized_keys file back to secure. For example, `chmod 600 authorized_keys`

3. Configure the secured TCP connection.

   a. Select **Settings > Global Settings > Logging**.

   b. Click **Add**.

   c. On the Add Loggings Settings page, select **SSH**.

   d. Enter an IP address, Log Level, TCP port, and user name.

   Note: You can specify an IPv4, IPv6, or hostname.

   e. Click **Save**.

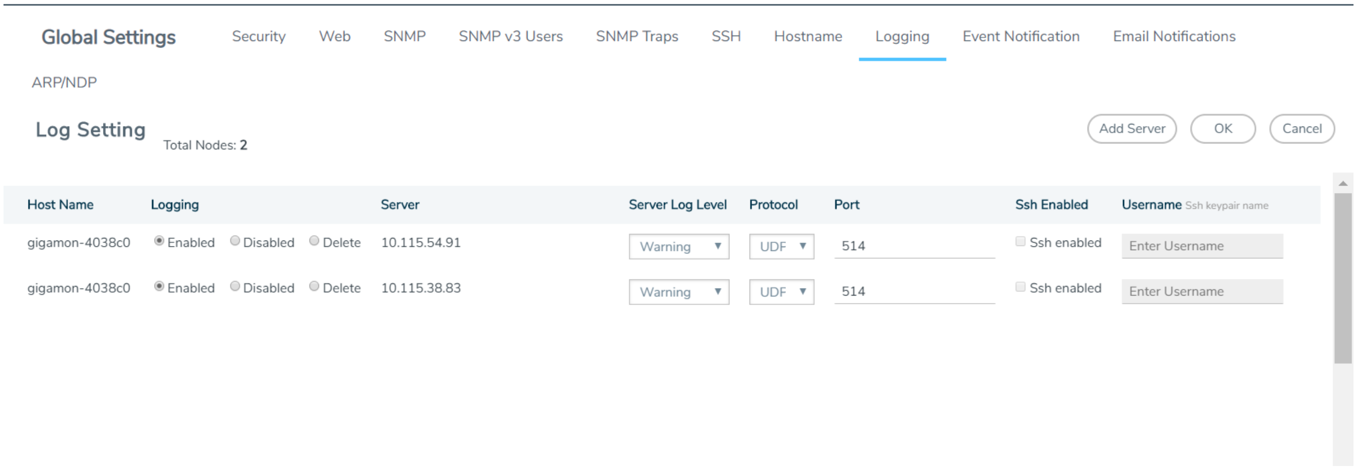
NOTES:

- To ensure the TCP connection is established, check the syslog server logs.
- If the TCP connection goes down, an attempt to re-establish the connection occurs every minute.
- If the database on the GigaVUE node is reset, a new public key will have to be generated and set up.

- In a cluster environment, the public key will be synchronized over the cluster so that all the nodes in the cluster can establish TCP/SSH connections.

Display Logging Information

To display logging information, select **Settings > Global Settings Logging**. This displays the Logging page. Figure 11Logging Page shows an example.



Log Setting

Total Nodes: **2**

Host Name	Logging	Server	Server Log Level	Protocol	Port	Ssh Enabled	Username Ssh keypair name
gigamon-4038c0	● Enabled ○ Disabled ○ Delete	10.115.54.91	Warning ▾	UDF ▾	514	□ Ssh enabled	Enter Username
gigamon-4038c0	● Enabled ○ Disabled ○ Delete	10.115.38.83	Warning ▾	UDF ▾	514	□ Ssh enabled	Enter Username

Figure 11 *Logging Page*

> **NOTE:** The SSH Enable column will display **Invalid** if SSH is enabled, but missing Username or TCP Port information.

GigaVUE-OS Security Hardening

To harden the GigaVUE operating system, GigaVUE-OS, against security threats, Gigamon fixes known vulnerabilities, keeps up-to-date any OS components that provide remote access (such as Apache, SSH, SSHD, and OpenSSL), and analyzes the system for attack vectors.

GigaVUE nodes run the GigaVUE-OS, which is hardened against the following:

- SHA1-Based Signature in TLS/SSL Server X.509 Certificate
- ICMP Timestamp Response
- TCP Timestamp Response
- Non-Standard SNMP Community Name

SHA1-Based Signature in TLS/SSL Server X.509 Certificate

Certificates generated by a third party certification authority are more secure than self-signed certificates. High strength ciphers with key lengths equal to or greater than 112 bits are also more secure than ciphers with less than 112 bits.

GigaVUE-OS supports TLS/SSL server X.509 certificates, including SHA2-256 and SHA2-512-based certificates, as well as SHA1-based certificates.

However, SHA1 has known weaknesses that expose it to collision attacks, which may allow an attacker to generate additional X.509 certificates with the same signature as the original.

Therefore, when a third party certificate is requested, SHA2-256 or SHA2-512 should be requested as the signature algorithm, and not SHA1.

To obtain a third party certificate, on Linux or Linux app (such as Cygwin), generate a private key as follows:

- openssl req -new -key privkey.pem -out cert.csr

The file, cacert.pem will be sent to a third party certificate authority, which will generate a certificate.

The ciphers supported with TLS v1.0, 1.1, and 1.2 are listed in Table 7: Supported Ciphers with TLS v1.0 and v1.1 and Table 8: Supported Ciphers with TLS v1.2.

Table 7: Supported Ciphers with TLS v1.0 and v1.1

Modern Ciphers	Classical Ciphers
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	

The ciphers supported with TLS v1.2 are listed in Table 8: Supported Ciphers with TLS v1.2.

Table 8: Supported Ciphers with TLS v1.2

Authenticated Encryption with Additional Data (AEAD) Ciphers	SHA-2 Ciphers
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc14)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc13)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc15)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	

ICMP Timestamp Response

The GigaVUE-OS does not respond to Internet Control Message Protocol (ICMP) timestamp requests.

The response to such a request is an ICMP timestamp response. The response can contain the date and time from a GigaVUE node, which could be used to exploit weak time-based random number generators in other services on the node, therefore this is disabled.

In addition, ICMP echo broadcasts, including timestamp requests and responses, are disabled, since ICMP echo requests may be used for Denial of Service (DoS) attacks, such as packet flooding.

TCP Timestamp Response

The GigaVUE-OS does not respond to Transmission Control Protocol (TCP) timestamp requests.

The response to such a request is a TCP timestamp response. The response can be used to approximate the uptime of the GigaVUE node, which can then be used in is DoS attacks.

In addition, some operating systems can be fingerprinted based on the behavior of their TCP timestamps, therefore this is disabled.

Non-Standard SNMP Community Name

Gigamon does not recommend using the default SNMP community string, public. It recommends using a non-standard SNMP community name, gigamon.

For steps to protect against SNMP vulnerabilities, refer to Recommendations for Vulnerabilities in the Use SNMP chapter.

Best Practices for Security Hardening

The following sections list best practices for security:

- Use of SNMPv1 and SNMPv2 are Not Recommended
- Use of Self-Signed Certificates are Not Recommended
- Use of FTP and TFTP are Not Recommended
- Use of Enhanced Cryptography Mode to Run Scans is Recommended
- Change the Password on admin Account
- Best Practices for Passwords

Use of SNMPv1 and SNMPv2 are Not Recommended

Using SNMPv1 and SNMPv2 are not recommended because they authenticate using unencrypted, plaintext community strings.

Using SNMPv3 is recommended for access to the SNMP agent, as well as to SNMP traps. SNMPv3 authenticates using encrypted community strings. For more information, refer to Use SNMP.

Use of Self-Signed Certificates are Not Recommended

Using self-signed TLS/SSL certificates are not recommended.

Certificates generated by a third party certification authority are recommended because they are issued by a Certification Authority (CA). Refer to SHA1-Based Signature in TLS/SSL Server X.509 Certificate for how to obtain a third party certificate.

Use of FTP and TFTP are Not Recommended

Using FTP or TFTP for file transfers is not recommended.

Using SFTP, SCP, or HTTPS is recommended for uploading or downloading files to or from GigaVUE nodes.

Use of Enhanced Cryptography Mode to Run Scans is Recommended

Using enhanced cryptography mode to run scans is recommended. Refer to Configure Enhanced Cryptography Mode for more information.

When a scan includes password brute force testing, it is recommended to disable locking users due to many attempts.

To disable lockout of accounts based on failed authentication attempts, select **Settings > Authentication > AAA**. Under Lockout, unselect **Enable Lockout**. For more information about Lockout, refer to Lockout.

Change the Password on admin Account

The default password on the admin account is admin123A!. After the first login, you must change the password to a non-default value.

If you have not changed the default password before the upgrade, you will be prompted to enter a non-default password. When upgrading through the CLI, **configuration jump-start** will automatically launch and prompt the system administrator to change the password on the **admin** account. For details, refer to the Password Policies section in the *GigaVUE-OS CLI Reference Guide*.

Messages Associated with Changing the admin Account Password

There are messages associated with changing the default password on the **admin** account since this password must be changed.

If the following message is displayed, the system administrator must change the default password on the admin account:

```
ATTENTION: Admin account password must be changed to a non-default value for
security purposes.
```

If the system administrator tries to change the password back to the default through the CLI, it will not be allowed and the following message will be displayed:

```
(config) # username admin password admin123A!% Default password is not allowed.
```

> **NOTE:** Using the **reset factory** CLI command deletes passwords on user accounts. When you login with the **admin** account, you will be prompted for a new password through the **jump-start** script.

If the node was upgraded from GigaVUE-FM and the default password is in use, the first time you log in to GigaVUE-FM after the upgrade, you are required to changed the default admin password through the CLI. GigaVUE-FM will display the following message:

```
This password is not allowed. If this is your password, you must change it
through the CLI.
```

For changing passwords and password polices, refer to Change Passwords and Set Up Basic Accounts and GigaVUE-OS Password Policies.

For best practices for other passwords, other than for the admin account, refer to Best Practices for Passwords.

Best Practices for Passwords

To maintain the highest level of security on GigaVUE HC Series and TA Series nodes, customers are strongly recommended to configure passwords for all user accounts and to change default passwords. Specifically, any user accounts that have no passwords, and the default password for the admin account.

Starting in software version 5.9.00, you must configure password for the monitor account, without which you cannot login to the device.

> **NOTE:** The monitor account is designed to give a read-only access to the GigaVUE-OS. The monitor account is disabled by default. To enable it, assign a password to the account. GigaVUE-FM users can use the monitor account as long as it is enabled (has a password).

To change the password on the default **monitor** account, do the following:

1. Log in to GigaVUE-FM as the **monitor** user.
2. Click on the **monitor** menu in the UI header and select **Change Password**.
3. On the Change Password for “monitor” page, enter a new password in **the New Password field** and confirm the password in the **Confirm New Password** field.

   When entering the new password, the system displays “Invalid Password” underneath the New Password field until the password meets the password criteria described in GigaVUE-OS Password Policies.
4. Click **Save**.

   The system logs you out of the system to reset the password. To log in again as the monitor user, use the password created in Step 3.

User accounts with no password configured should be updated to include a password. Alternatively, a user account without a password configured can be disabled by doing the following:

1. Log in as the **admin** user.
2. Select **Roles and Users > Users**.

3. On the User Setup page, select the user whose account you want to disable and then click **Edit**.
4. On the Edit User page, make sure the **Enable** checkbox is not selected.
5. Click **Save**.

   The system displays a message if the account was updated successfully and the Enabled field shows false, indicating the user account is no longer enabled.

   User accounts that do not have passwords set can also be disabled. Refer to Configure Secure Passwords Mode for details.

   To avoid any disruption of existing functionality, when the passwords for the affected user accounts have been configured, make sure to update any applications or scripts that may be affected.

License GigaVUE TA Series

Refer to the GigaVUE Licensing Guide for details.

Chassis

The Chassis page provides a detailed snapshot of a selected H Series node, providing views of cards, control cards, and ports on the chassis. It is also possible to view information about individual cards or modules fan trays, and power modules.

This chapter covers the following topics:

- Chassis View

  This section describes the following:
  - Chassis View + Transceiver View
  - Chassis View + Port View
- Table View

  This sections describes the following:
  - Actions Menu for configure/reconfigure, start up/shut down, and changing mode on a selected card
  - Change Mode for setting the card mode on a GigaVUE-TA10 or GigaVUE-TA40
  - Change Port Mode for setting the port mode

Chassis View

When you click the **Chassis** link in the Navigation pane, the Chassis page displays a graphical representation of the node. This is the Chassis View and the default. You can select this view when in the Table View by clicking the Chassis View button indicated in Figure 12Chassis View. Chassis View includes two types of views. Port View and Transceiver View. Transceiver View is the default view.

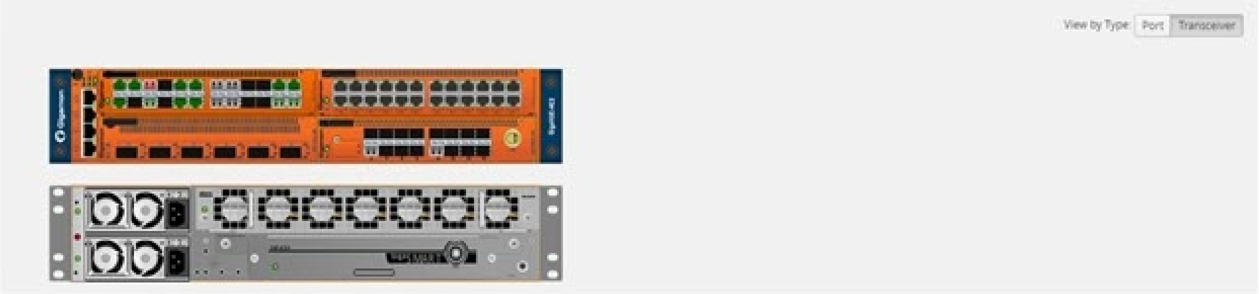


Figure 12 *Chassis View*

When a chassis is part of a cluster, the Chassis pages include a drop-down list that lets you select which chassis in the cluster to view. Figure 13Chassis View of Node in a Cluster shows an example.

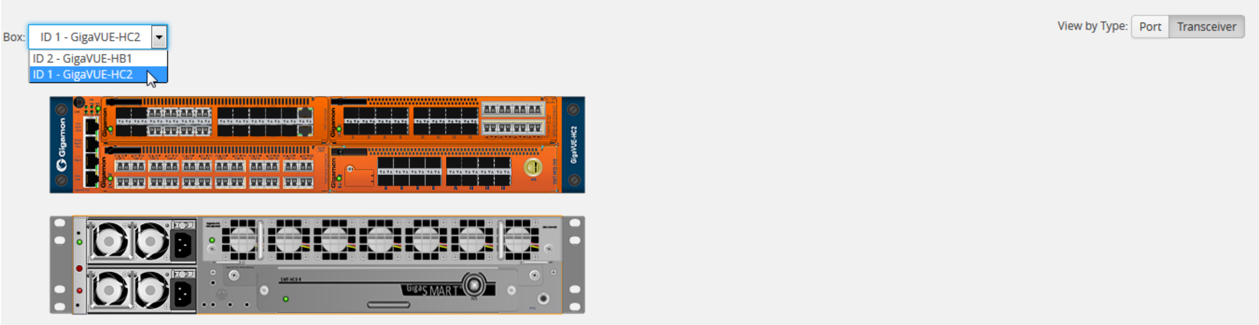


Figure 13 *Chassis View of Node in a Cluster*

From the Chassis page, you can select the following:

- Chassis View + Transceiver View

  For details, refer to Chassis View + Transceiver View.
- Chassis View + Type View

  For details, refer to Chassis View + Port View.
- Table View

  For details, refer to Table View.

NOTE: For GigaVUE-TA1, you will only see one card allocation because these are non-modular nodes.

Figure 14Chassis View—HC2 and Chassis View show some examples of chassis displayed on the Chassis page.

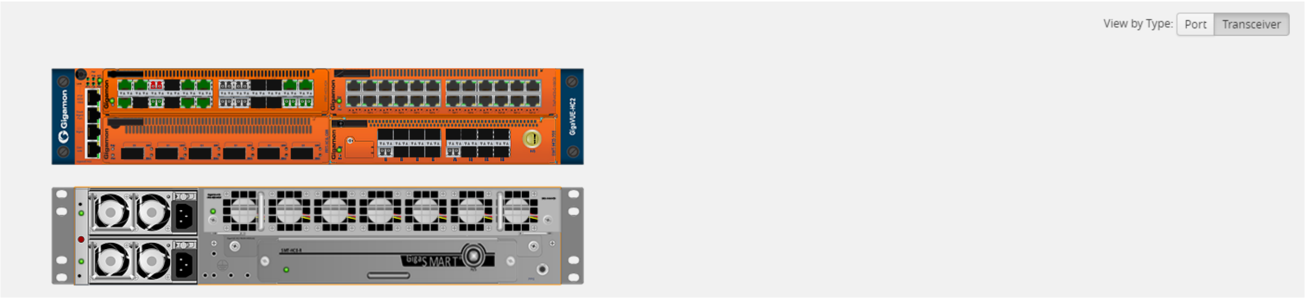


Figure 14 *Chassis View—HC2*

Hovering over or port in either Port View or Transceiver view displays information about the port: type, port ID, and alias. Hovering over a slot displays information about the slot. For details about port IDs, refer to Line Card and Module Numbering.

Chassis View + Transceiver View

The Chassis + Transceiver view selection is made by clicking the Transceiver View button on the Chassis View page. This view shows you the HC Series node with all the line cards/modules displayed. All the line cards/modules have the transceivers and LEDs displayed.

When the Chassis and Transceiver views are selected, the image of the chassis indicates which transceivers are physically available on the node and whether the ports are up or down. The colors indicate the following:

- Green—the port is up
- Red— the port is down
- Black—the transceiver is missing

Figure 15Chassis + Transceiver View shows an example of a Chassis + Transceiver View.

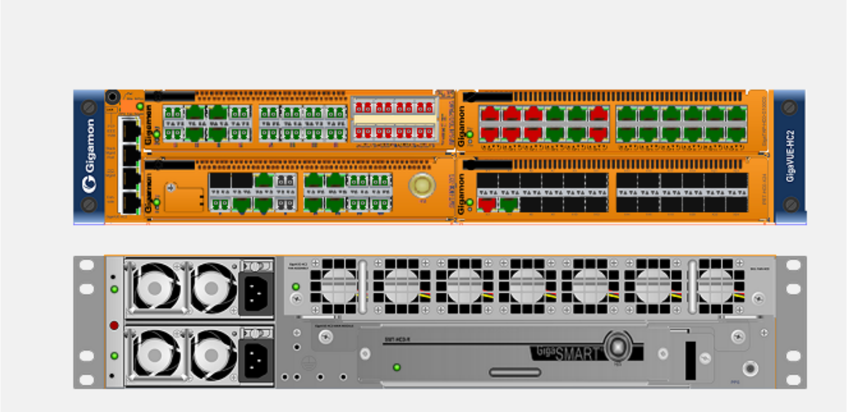


Figure 15 *Chassis + Transceiver View*

In Chassis + Transceiver View, the port type and port ID is displayed by hovering over the ports in the graphic.

Some chassis support fanout of ports, such as the GigaVUE-TA100. When fanout is used, the fanout is displayed on the Chassis page as shown in Figure 16Chassis + Transceiver View with Fanout Ports.

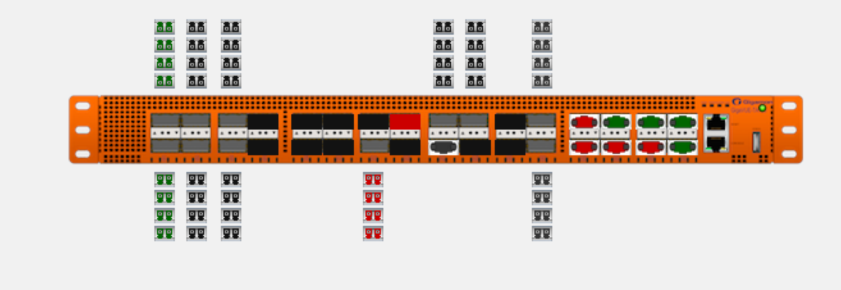


Figure 16 *Chassis + Transceiver View with Fanout Ports*

Chassis View + Port View

The Chassis + Port view selection is made by clicking the Port View button on the Chassis View page. All the line cards/modules have the port types displayed a shown in Figure 15Chassis + Transceiver View. A legend at the bottom of the page identifies the types of ports. As in Chassis + Transceiver view, the colors indicate the status of the ports.

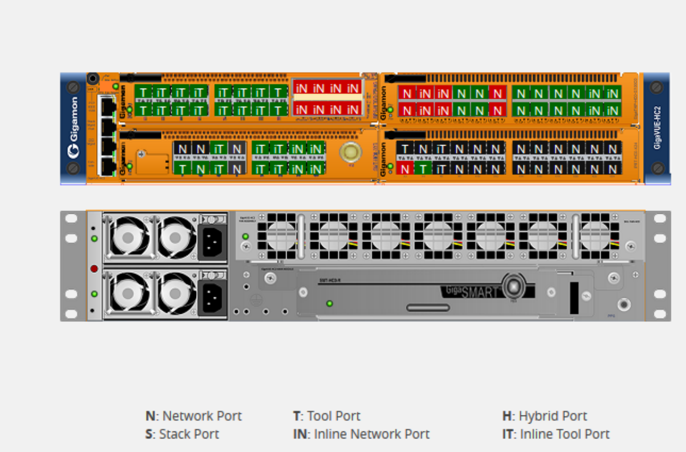


Figure 17 *Chassis View + Type View*

Line Card and Module Numbering

Line cards and modules use standard conventions for numbering network and tool ports, both on the faceplates of the line cards or modules, and in the information displayed in Chassis view when hovering over a port. On faceplates, the numbers are as follows:

100Gb Ports	Numbered with a leading **C**. For example, the PRT-HD0-C01 includes 100Gb port **C1**; PRT-HD0-C02X08 includes ports **C1** and **C2**.
40Gb Ports	Numbered with a leading **Q**. For example, the PRT-H00-Q02X32 includes 40Gb ports **Q1** and **Q2**.

10Gb/1Gb Ports	Numbered with a leading X. For example, the PRT-HC0-X24 includes 10Gb/1Gb ports X1 to X24; the bypass combo modules include 10Gb ports X1 to X16.
10/100/1000 Ports	Numbered with a leading **G**. For example, the PRT-T H00-X12G04 includes 10/100/1000 ports **G1** to **G4**.

The port labels on the line card or module faceplates use upper-case C, Q, X, and G characters to identify ports. However, Chassis View) uses lowercase notation to refer to ports (for example, c1, q1, x4, and g1).

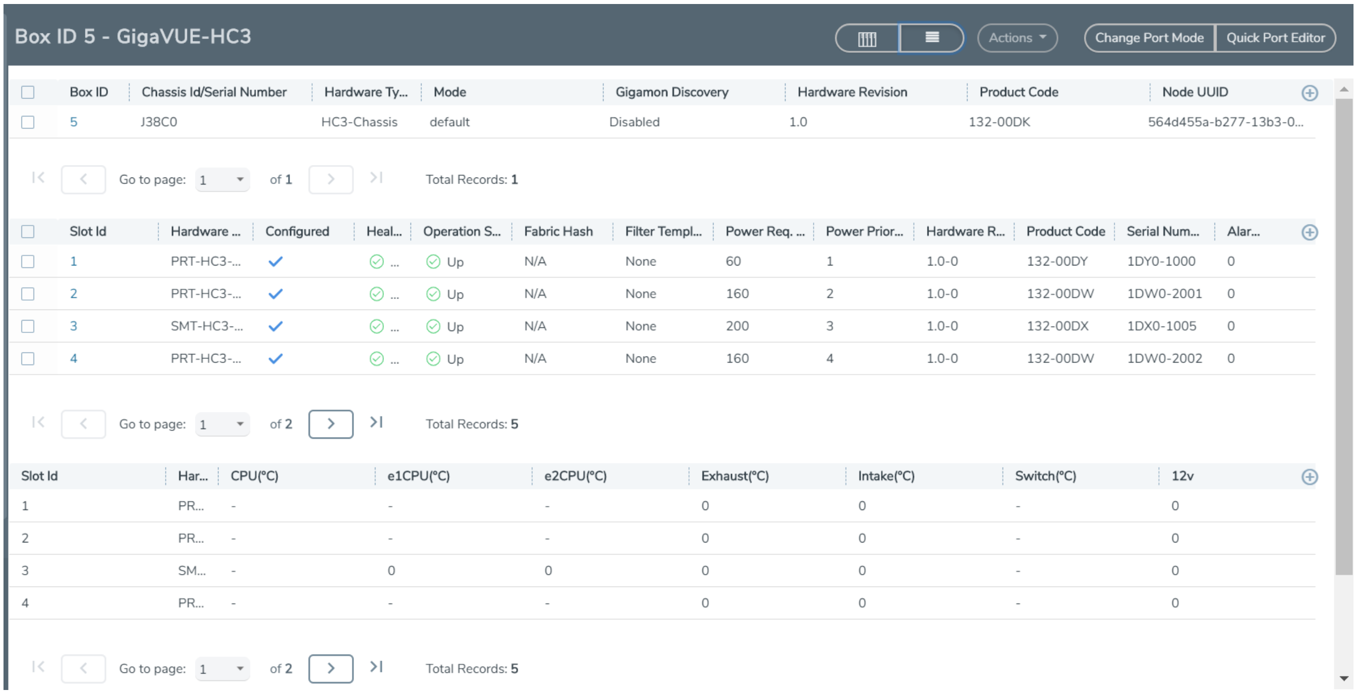
When displaying ports in Chassis View , the format is box ID/slot ID/port ID. For example, 1/1/x6 refers to box 1, slot 1, port X6.

On chassis with multiple slots/bays, the slots or bays are numbered as follows:

- **GigaVUE-HC1**: Bays are numbered as follows:
  - the base chassis in the center, is numbered 1
  - the left module is numbered 2
  - the right module is numbered 3
- **GigaVUE-HC2**: Bays are numbered 1-4 from left upper, left lower, right upper to right lower.
- **GigaVUE-HC3**: Bays are numbered 1-4 from left upper, left lower, right upper to right lower.

Table View

The Table View selection shows the HC Series or TA Series node as a table of the node properties with line card/module information, environment information (temperature and voltage), available power supplies, fan trays, and fan RPM. The health status of these is also indicated in Table View for cards, Power Supplies, and Fan Trays. Figure 18Chassis Table View for a Gigamon HC2 CCv2 shows an example of the Table View. For GigaVUE-HC2s, the Cards section also displays information about the main board, indicating whether it is in normal or 100G mode if it is equipped with Control Card version 2 (HC2 CCv2) AND 100G modules, PRT-HC0-C02. For GigaVUE-HC1, the Environment section includes a column that shows the GigaSMART CPU Temperature. To select Table View, click the Table View button.



□	Box ID	Chassis Id/Serial Number	Hardware Ty...	Mode	Gigamon Discovery	Hardware Revision	Product Code	Node UUID
□	5	J38C0	HC3-Chassis	default	Disabled	1.0	132-00DK	564d455a-b277-13b3-0...

Go to page: 1 of 1 Total Records: 1

□	Slot Id	Hardware ...	Configured	Heal...	Operation S...	Fabric Hash	Filter Templ...	Power Req. ...	Power Prior...	Hardware R...	Product Code	Serial Num...	Alar...
□	1	PRT-HC3-...	✓	✓ ...	✓ Up	N/A	None	60	1	1.0-0	132-00DY	1DY0-1000	0
□	2	PRT-HC3-...	✓	✓ ...	✓ Up	N/A	None	160	2	1.0-0	132-00DW	1DW0-2001	0
□	3	SMT-HC3-...	✓	✓ ...	✓ Up	N/A	None	200	3	1.0-0	132-00DX	1DX0-1005	0
□	4	PRT-HC3-...	✓	✓ ...	✓ Up	N/A	None	160	4	1.0-0	132-00DW	1DW0-2002	0

Go to page: 1 of 2 Total Records: 5

Slot Id	Har...	CPU(°C)	e1CPU(°C)	e2CPU(°C)	Exhaust(°C)	Intake(°C)	Switch(°C)	12v
1	PR...	-	-	-	0	0	-	0
2	PR...	-	-	-	0	0	-	0
3	SM...	-	0	0	0	0	-	0
4	PR...	-	-	-	0	0	-	0

Go to page: 1 of 2 Total Records: 5

Figure 18 *Chassis Table View for a Gigamon HC2 CCv2*

The Table View provides the following information about the chassis and its components:

Chassis Information	Description
Properties	Provides information about the chassis: Chassis ID/Serial Number, VLAN Tag Mode, Hardware Type, Mode, Gigamon Discovery, Operation Status, Hardware Revision, Product Code, and Node UUID . **NOTE:** Click on the Box ID to view the Fabric Hash setting for the chassis. For a GigaVUE-HC2 CCv2, the Mode field displays either Normal or 100G when 100Gb is enabled on the PRT-HC0-C02 module.
Cards	Describes the cards installed in each slot of the chassis. This section includes the current health status of each card. Selecting a check box next to a card allows you to perform various actions on the card with the Actions menu. For details refer to Actions Menu.
Environment	Provides temperature information about the main board and cards in the chassis.

Chassis Information	Description
Power Supplies	Describes the power supply modules installed in the chassis. This section also includes the current health status of each module. For a GigaVUE-HC2 node, the health status of both the top and bottom modules. For a GigaVUE-HC3 node, the Power Supplies section includes Power Management. Refer to *GigaVUE-HC3 Hardware Installation Guide* for details. **NOTE:** Click on the Power Module ID to view the PSU diagnostic attributes in a Quick View.
Fan Trays	Describes the fan trays installed in the chassis. This section also including the current health status of each tray.
Fan RPM	Provides the current RPM of each fan.

Actions Menu

The Actions menu allows you to perform actions on cards installed in the chassis slots when in Chassis + Table View. The Actions menu is only active when a card is selected. The actions that you can perform are as follows:

Action	Description
Configure	Selecting this action sets the port and traffic settings for the system.
Unconfigure	Selecting this action for a card removes all port and traffic settings for the system.
Enable/Disable Gigamon Discovery	Used to enable/disable Gigamon Discovery protocol
Fabric Advance Hash	Used to configure fabric advanced hashing parameters for stack GigaStreams and GigaSMART groups. For details, refer to Fabric Advanced Hashing
Start Up	Selecting this action reboots the card.
Shut Down	Selecting this action shuts down the card.
Change Mode	Used for setting card mode on a GigaVUE-TA1, GigaVUE-TA10, or GigaVUE-TA40 node. For more details, refer to Change Mode
Change VLAN Tag Mode	Used for configuring the VLAN tag mode forGigaVUE-TA25 node. For more details refer to Change VLAN Tag mode.
Enable Fabric Hash	Used for improving packet distribution on PRT-H00-Q02X32 and PRT-HD0-Q08 line cards. For details, refer to Enable Advanced Fabric Hashing

Reload a GigaSMART Line Card or Module

Occasionally, the GigaSMART line card or module will need to be reloaded for changes to take effect and to allocate resources accordingly. Reloading also provides applications with contiguous memory.

The following message displays when the GigaSMART line card or module needs to be reloaded:

Resource allocation changes have been made that require GigaSMART card 2/1/1 to be reloaded in order for them to take effect.

When this message is displayed, you cannot change the configuration relating to that application until after the reload. For example, you cannot use the GigaSMART Operation, associated with the GigaSMART Group in a map.

Use the following steps to reload a GigaSMART line card or module:

1. Switch to Table View.
2. Under **Cards**, select the GigaSMART line card or module.
3. Select **Actions > Shut Down**.

Use the following steps to bring the GigaSMART line card or module backup:

1. Switch to Table View.
2. Under **Cards**, select the GigaSMART line card or module.
3. Select **Actions > Start Up**.

Change Mode

The Actions menu has a **Change Mode** selection that is used to set the card mode on GigaVUE-TA1, GigaVUE-TA10 and GigaVUE-TA40 nodes. On the GigaVUE-TA1, GigaVUE-TA10, you can configure card modes that let either two (q1..q2) or all four (q1..q4) of the 40Gb ports operate as four logical 10Gb ports (x49..x64). On the GigaVUE-TA40, you can also configure card modes that let either of the 40Gb ports operate as four logical 10Gb ports (x1..x4). Changing the card mode is useful when deploying the GigaVUE-TA10 or the GigaVUE-TA40 in an environment that does not yet include 40Gb interfaces.

Once a 40Gb port has been configured to operate as four 10Gb ports, you will need to cable it to a breakout panel, such as PNL-M341. The breakout panel takes a 40Gb QSFP+ input from a GigaVUE-TA10 or GigaVUE-TA40 and splits it to four independent 10Gb output ports. For details on breakout panel connections, refer to the *GigaVUE TA Series Hardware Installation Guide*.

Changing the card mode resets all port and packet distribution settings, therefore, set the card mode during the initial configuration.

Configure the Card Mode on a GigaVUE-TA1 or GigaVUE-TA10

The following card modes are available for the GigaVUE-TA1 and GigaVUE-TA10:

- **48x** (default) – Four 40Gb ports (q1..q4) and 48 10Gb ports (x1..x48)
- **56x (use with breakout panel or breakout cables)** – Two 40Gb ports (q3..q4) and 56 10Gb ports. Port q1 is used as x49..x52 on the breakout panel. Port q2 is used as x53..56 on the patch panel.
- **64x (use with breakout panel or breakout cables)** – 64 10Gb ports (x1..x64). Port q1..q4 are connected at the breakout panel as follows:
  - **q1** – x49..x52
  - **q2** – x53..x56
  - **q3** – x57..x60
  - **q4** – x61..x64

To specify card modes use the following procedure:

1. Deconfigure the card by doing the following:
   a. Switch to Table View by clicking the Table View button.
   b. Under Cards, select the card to deconfigure. This activates the **Actions** menu.
   c. Select **Actions > Unconfigure**.

   NOTE: This removes all port and traffic settings for the system.
2. To set the new card mode for a GigaVUE-TA1 or GigaVUE-TA10:
   a. Select **Actions > Change Mode**
   b. For **Mode**, select 48x, 56x, or 64x.

   The settings for each available mode are summarized in Table 9: 40Gb Port Settings by Card Mode on GigaVUE-TA10 .

   c. Click **Save**.
3. Configure the card by selecting **Actions > Configure**.

Table 9: 40Gb Port Settings by Card Mode on GigaVUE-TA10

Card Mode	Physical 40Gb Interface on GigaVUE-TA10			
	q1	**q2**	**q3**	**q4**
48x (default)	40Gb (q1)	40Gb (q2)	40Gb (q3)	40Gb (q4)
56x	10Gb (x49..x52)	10Gb (x53..x56)	40Gb (q3)	40Gb (q4)
64x	10Gb (x49..x52)	10Gb (x53..x56)	10Gb (x57..x60)	10Gb (x61..x64)

Notes on GigaVUE-TA10 Card Modes

- The default card mode is 48x.
- When a 40Gb port is used as four 10Gb ports, removing the QSFP+ will affect the connections for all four 10Gb ports. For example, removing the QSFP from q1 results in a loss of signal event for x49..x52.
- The q1..q4 40Gb ports include a single link LED on the GigaVUE-TA10 faceplate. When a physical 40Gb interface is used as four 10Gb ports, the 40Gb port LED indicates the status of the **first** of the four 10Gb ports on the breakout panel (for example x49 in the x49..x52 group, x53 in the x53..x56 group, and so on). The other three ports in the group do not affect the link LED for the 40Gb port on the GigaVUE-TA10 faceplate.

Once the card mode has been configured, make the breakout panel connections. For details, refer to the *GigaVUE TA Series Hardware Installation Guide*.

Change VLAN Tag mode

Change VLAN Tag mode allows you to configure, single tagged or double tagged VLAN traffic at the chassis level for GigaVUE-TA25 and GigaVUE-TA25E. This mode can be configured based on your incoming traffic and network requirements. This configuration has two modes which are as follows:

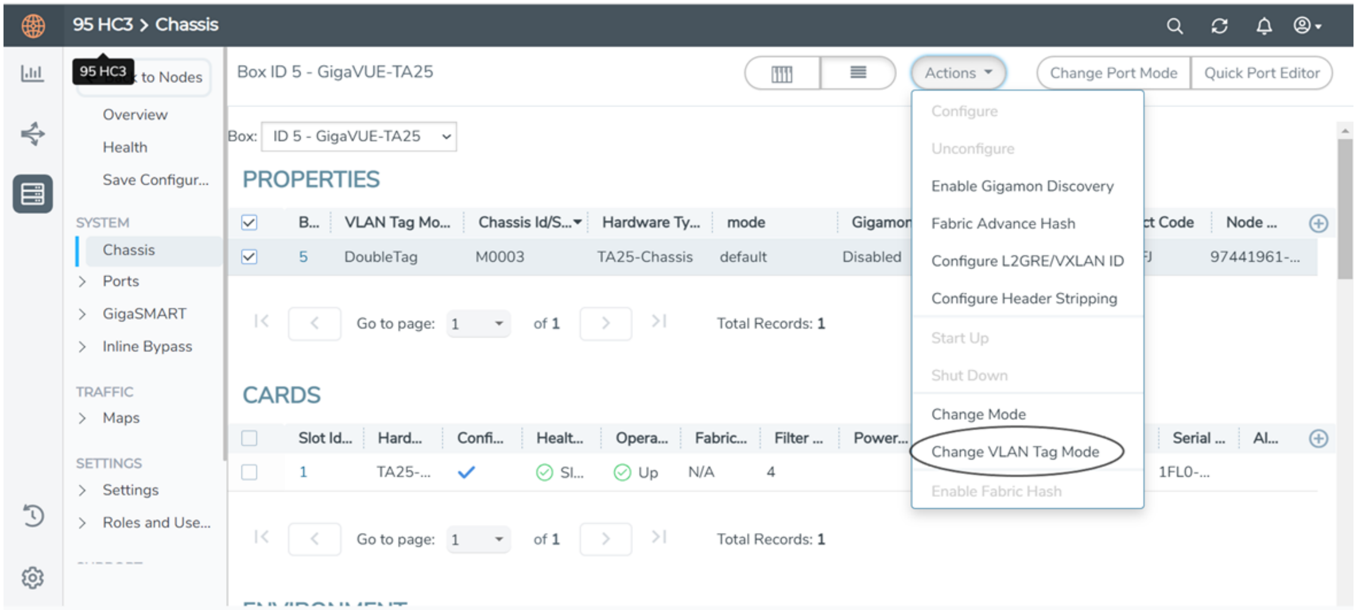
1. **Single Tag Mode**- This provides visibility of untagged and single-tagged VLAN packets. Single tagged traffic allows GigaVUE-TA25 and GigaVUE-TA25E to enable the following features:
   - VLAN rules are supported in port filters.
   - Egress VLAN stripping is supported as in legacy devices, even when the source and destination belongs to the same or different set of devices.
   - MAC rewrite functionality is supported in cluster mode.
   - When L2 circuit encapsulation tunnels or GSOP maps are in use, then the port filters will support both IPv4 and IPv6 rules.
   - This functionality is enabled even when a GigaVUE-TA25 is in a cluster. In the same cluster, there can be two GigaVUE-TA25 devices functioning with two different tag modes.

2. **Double Tag Mode**-This is the default mode, which supports both single and double tagged VLAN packets. When the deployment environment needs visibility to all types of packets i.e untagged or single-tagged/double tagged or priority VLAN tagged (VLAN Tag 0) packets, then this is the recommended operating mode. In this mode the above features enabled in single-tagged mode will exist as a limitation for GigaVUE-TA25 and GigaVUE-TA25E. For GigaVUE-TA25E the limitation; when L2 circuit encapsulation tunnels or GSOP maps are in use, then the port filters will support both IPv4 and IPv6 rules is not applicable in E-tag mode.

Configure Change VLAN Tag

The chassis page has a **Actions** button. To configure either single or double tagged VLAN do the following:

1. Select your GigaVUE-TA25 node.
2. Click on **Actions** buttons and select **Change VLAN Tag Mode**.



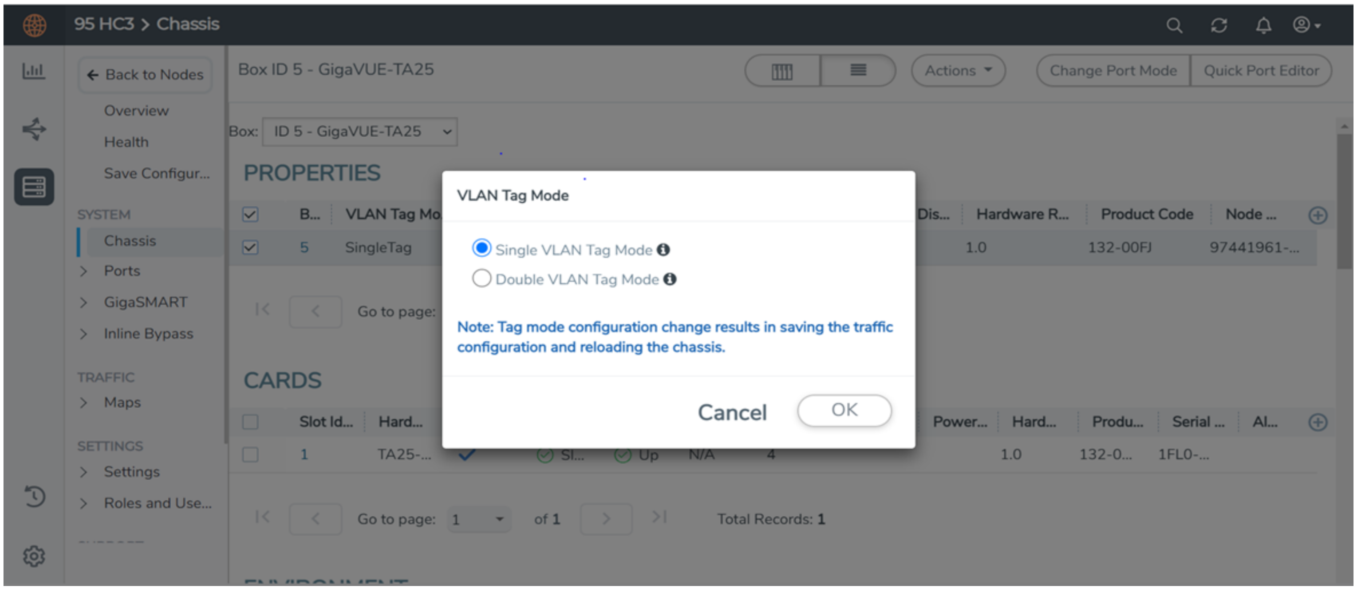
☑	B...	VLAN Tag Mo...	Chassis Id/S...	Hardware Ty...	mode	Gigamon	ct Code	Node ...
☑	5	DoubleTag	M0003	TA25-Chassis	default	Disabled	FJ	97441961-...

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

□	Slot Id...	Hard...	Confi...	Healt...	Opera...	Fabric...	Filter ...	Power...	Serial ...	Al...
□	1	TA25-...	✓	✓ Sl...	✓ Up	N/A	4		1FL0-...	

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

3. Select the VLAN Tag mode as required.
4. Confirm the selection and click on **OK.**.
5. Once the VLAN tag is configured the device will save the traffic and initiate reloading the device.



VLAN Tag Mode

● Single VLAN Tag Mode

○ Double VLAN Tag Mode

Note: Tag mode configuration change results in saving the traffic configuration and reloading the chassis.

Cancel OK

Rules and Notes

1. While configuring the VLAN tag mode the chassis will be reloaded only if it is in UP state. Otherwise it will apply the configuration without reloading the chassis. The user will be notified about the reload. After confirmation, the active configuration will be applied and the chassis will be reloaded after saving the active configuration.
2. If double tagged packets enter a single tag mode in GigaVUE-TA25 chassis then the inner VLAN would be dropped during egress.
3. Modifying tag-mode via *config switch-to* operation is supported whereas it is not supported via *config text-apply* operation.
4. In a Single tag-mode, adding vlan port-filter-rule along with VLANs matching the ingress-vlan-tag(on network-port)/add-vlan-header gsop in the transit/second map is not supported due to platform limitation.
5. In single-tag mode, priority tagged VLAN (VLAN TAG 0) packets are stripped off the VLAN tag at egress. It is recommended to use double tag mode in this case.

Change Port Mode

Change port mode can be configured only on selected platforms. The port breakout modes are as follows:

- **none**—Specifies no port breakout mode. This is the default mode for all GigaVUE nodes.
- **4x10G**—Specifies the **4x10G** port breakout mode. This mode provides a 4 x 10Gb breakout option for 100Gb/40Gb ports. The **4x10G** mode only applies to GigaVUE-TA40, GigaVUE-TA100, GigaVUE-TA200, GigaVUE-TA100-CXP, the PRT-HD0-C06X24 line card on GigaVUE HD Series, and the PRT-HC3-C08Q08, PRT-HC3-C16, SMT-HC3-C05, and BPS-HC3-C25F2G modules on GigaVUE-HC3.

> **NOTE:** Starting in software version 5.5, GigaVUE-TA40 supports 4x10G breakout at port level. Port breakout mode in GigaVUE-TA40 is configured as follows:

    - 24 out of the 32 ports provide 4x10Gb breakout support. The first 12 ports and the last 12 ports provide support for breakout functionality with 96 sub-ports operating as 10Gb ports
  - Ports q1 to q12 and q21 to q32 support breakout functionality
  - Ports q13 to q20 do not support breakout functionality
    - Port are named as q1x1....q1x4, q2x1...q2x4 (similar to other hardware devices) to support the breakout functionality
- **4x25G**—Specifies the **4x25G** port breakout mode. This mode provides a 4 x 25Gb breakout option for 100Gb QSFP28 SR ports. The **4x25G** mode only applies to GigaVUE-TA200 and the PRT-HC3-C08Q08, PRT-HC3-C16, and SMT-HC3-C05 modules on GigaVUE-HC3.
- **2x40G**—Specifies the **2x40G** port breakout mode. This mode provides a 2 x 40Gb breakout option for 100Gb/40Gb ports. The **2x40G** mode only applies to the PRT-HC3-C08Q08 module on GigaVUE-HC3.

For the BPS-HC3-C25F2G module on GigaVUE-HC3, refer to the *GigaVUE-HC3 Hardware Installation Guide*.

The 100Gb ports that support **4x10G** mode can operate at 40Gb speed with QSFP+ SR or PLR4 transceivers. When a parent port is configured in **4x10G** mode, it can be broken out into four 10Gb ports, called subports. The subports will all have the same speed (10Gb). Subports will have x1 to x4 appended to their port ID, for example, 1/1/c2x1.

The 100Gb ports that support **4x25G** mode can be broken out into four times 25Gb ports, called subports. The subports will all have the same speed (25Gb). Subports will have x1 to x4 appended to their port ID, for example, 1/1/c2x1.

The 100Gb ports that support **2x40G** mode can operate at 40Gb speed with QSFP+ SR and LR transceivers. When a parent port is configured in **2x40G** mode, it can be broken out into two 40Gb ports, called subports. The subports will all have the same speed (40Gb). Subports will have q1 to q2 appended to their port ID, for example, 1/1/c1q1 and 1/1/c1q2.

In general, subports created from port breakout modes can function as network, tool, or hybrid ports, as well as GigaStream port members, but they cannot function as stack ports. However, starting in software version 5.3, 10Gb stacking is supported only on GigaVUE-TA100 and PRT-HC3-C08Q08 on GigaVUE-HC3 when ports are broken out into **4x10G** mode.

> **NOTE:** On the PRT-HD0-C06X24 line card on GigaVUE HD Series, when 40Gb ports are broken out into 4 X 10Gb subports, no ports on that line card can be used as stack-links, not any other C port or any X port.

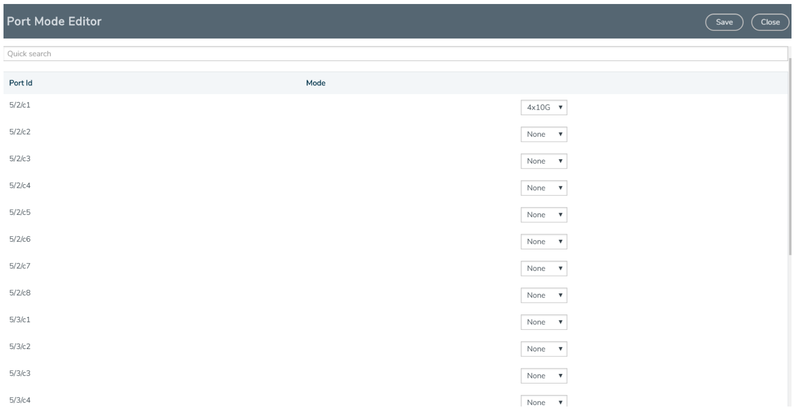
Each port can only have one mode.

The Chassis page has a Port Mode Editor available. The Port Mode Editor is used to set ports to breakout mode.To configure a port breakout mode, do the following:

1. Click **Change Port Mode**.

   > **NOTE:** The **Change Port Mode** button is only active on nodes that support it.

   The Port Mode Editor page shown in Figure 19Port Mode Editor displays.



Port Id	Mode
5/2/c1	4x10G ▾
5/2/c2	None ▾
5/2/c3	None ▾
5/2/c4	None ▾
5/2/c5	None ▾
5/2/c6	None ▾
5/2/c7	None ▾
5/2/c8	None ▾
5/3/c1	None ▾
5/3/c2	None ▾
5/3/c3	None ▾
5/3/c4	None ▾

Figure 19 *Port Mode Editor*

2. Select the **Port Mode** for the ports that you want configure: **none**, **4x10G**, **4x25G**, or **2x40G**. For example, set port 36/1/c3 to **4x10G**.

   Use the Quick search field to find a specific port. For example, entering 36/1/c3 in the Quick search field displays the ports with the IDs 36/1/c3, 36/1/c30, 36/1/c31, 36/1/c32.

3. Click **Save**.

   The system returns you to the Chassis View page. For example on GigaVUE-TA100, the fanout ports are displayed in the chassis view as shown in Figure 20Breakouts Displayed on a GigaVUE-TA100 Chassis. In Figure 20Breakouts Displayed on a GigaVUE-TA100 Chassis, the ports that are set to **4x10G** show four additional ports.

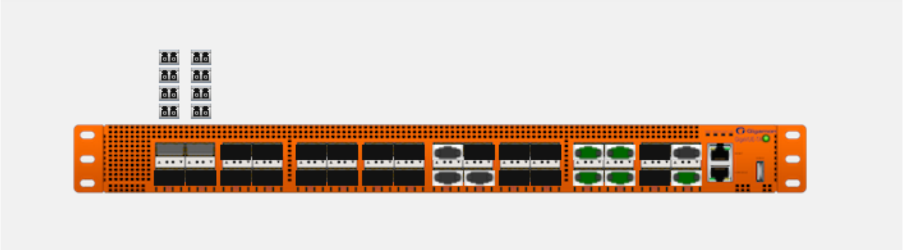


Figure 20 *Breakouts Displayed on a GigaVUE-TA100 Chassis*

After setting the port breakout mode, the ports will need break-out cables or breakout panel (PNL-M341 or PNL-M343). For breakout panel information, refer to the respective *Hardware Installation Guide*.

Enable Advanced Fabric Hashing

The Enable Fabric Hash option is used to enable advanced fabric hashing on a specified card and slot. Advanced fabric hashing is supported on all GigaVUE-HC series devices and GigaVUE-TA series devices.

Advanced Fabric Hash can only be enabled or disabled while in Chassis Table View. To enable or disable Advanced Fabric Hashing, do the following:

1. Select **Chassis** in the main navigation pane.
2. Switch the Chassis page to Table View.
3. Under **Cards**, find the line card on which you want to enable fabric hash and select the card. The **Fabric Hash** field for the card indicates the current state of fabric hash. In Enable Advanced Fabric Hashing, fabric hash is disabled on the selected line card.
4. Select **Actions**
   - If the fabric hash is currently disabled, the **Actions** menu shows **Enable Fabric Hash**. Click on the menu selection to enable.
   - If the fabric hash is currently enabled, the **Actions** menu shows **Disable Fabric Hash**. Click on the menu selection to disable.

Fabric Advanced Hashing

Fabric Advanced Hashing is used to enable advanced fabric hashing on a chassis in GigaStream stack links and GigaSMART groups. The Fabric Advanced Hash option lets you select the criteria for sending matching flows to the same destination port within stack links.

The existing gigastream hashing can be applied only to tool/hybrid/circuit ports. Fabric advanced hashing hashes traffic based on the ipsrc, ipdst, protocol, ip6src, ip6dst. You can also select the various fields to configure hashing on stack links.

Fabric advanced hashing applies to the following modules:

- GigaVUE-HC1
- GigaVUE-HC2
- GigaVUE-HC2+
- GigaVUE-HC3-v1
- GigaVUE-HC3-v2
- GigaVUE-TA40
- GigaVUE-TA100
- GigaVUE-TA200

Fabric Advanced Hash can only be enabled or disabled while in Chassis Table View. To enable or disable Fabric Advanced Hashing, do the following:

1. Select **Chassis** in the main navigation pane.
2. Switch the Chassis page to Table View.
3. Select the **Box ID** under Properties and select **Actions**.
4. Select the required **Fabric Advanced Hash** type from the drop-down.
5. The following options are available:

- **All:** Selects all criteria
- **Default**: Sets the fabric advanced hash algorithm to its default settings
- **None**: Clears all fields from advanced hash
- **Fields**: Allows you to select the required fields for advanced hash.

NOTE: If **Fabric Advanced Hash** is already configured, click the **Box-ID** field to view the Fabric Advanced Hash configuration in a Quick View.

Manage Roles and Users—GigaVUE-OS

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

- About Role-Based Access
- Configure Role-Based Access and Setting Permissions in GigaVUE Nodes

About Role-Based Access

GigaVUE HC Series nodes use role-based access to manage access to the Gigamon Visibility Platform. Through GigaVUE-FM, you can create roles and assign users to those roles, allowing you to partition separate sets of tool ports for different groups of users while different sets of network ports are shared. This makes it possible to provides different groups of users with different analysis needs to have full access to the packets they need for their tools.

Notes:

- To take advantage of GigaVUE-FM, Gigamon highly recommends that you have the same user name and password (with roles) registered with the physical node(s). In doing so, GigaVUE-FM provides the ability to manage and monitor physical devices with all of its features.
- If a user has full access (super admin or admin) on GigaVUE-FM but limited access on the node, they will be able to view the traffic and all the ports from the Dashboard page, Audit logs and Reports but will not be able to configure the node itself.

- If the user with the same name is created on GigaVUE-FM and the node but the passwords are different, the user will be able to view all the ports on the node from GigaVUE-FM but will not be able to configure the node from GigaVUE-FM. In order to have full access, it is required that both the username and passwords be identical on the node as well as GigaVUE-FM. To avoid such situations it is recommended to use centralized authorization servers such as LDAP, RADIUS or TACACS+.

For more detailed information related to role-based access, refer to the following sections:

- Role-Based Access and Flow Mapping®
- Locks and Lock Sharing
- ■ Admin

Role-Based Access and Flow Mapping®

Flow Mapping® allows different users to share network ports. Because Flow Mapping® sends a packet matching multiple maps to the destination specified by the map with the highest priority, you must exercised caution when adjusting maps on shared network ports. Administrators can change the priority of maps to ensure that packets are sent to the desired destination.

Permission can also be associated with maps based on roles. For more information about map permissions, refer to Set Map-Sharing Permission Levels

Set Map-Sharing Permission Levels

Maps can be shared with one or more roles. When sharing a map, the map owner or Admin designates which roles have which permissions. There are four map-sharing permission levels:

Permission Level	Description
View	Role can view the map but cannot make any changes.
Listen	Role can add or remove tool ports they own[1]. This is equivalent to *subscribing* to a map.
Edit	Role can delete and edit the map, can remove any network ports, can add network ports they own[1], and can add or remove tool ports they own[1].
Owner	Role can perform all the Read/Write functions and assign map sharing permission levels.

[1] *Requires Level 2 or Level 3 access, based on the user's role membership.*

NOTE: Map-Sharing Permissions are only available to node level users. GigaVUE-FM users cannot be added for this level of permissions.

To set permissions for a map, do the following:

1. Select **Maps** in the Navigation pane, then go to the **Maps** page.
2. Select the map, and then click **Edit**.
3. Go to the **Map Permissions** section of the **Edit Map** page.
4. Click in the **Owner**, **Edit**, **Listen**, or **View** field and select roles from the drop-down list.

Locks and Lock Sharing

Short-term analysis needs are always changing, occasionally creating situations where one user may temporarily need exclusive access to a port. Rather than create new roles and associations in situations like this, a user can lock a port to which they have Level 2+ access, preventing other users from changing settings. Locks can also be shared with other users, allowing users to collaborate. Sharing a locked port provides the account with whom the port is shared the same port permissions as the account sharing the port. For example, if User X has Level 2 permissions on port 12/5/x3, User X can share a lock on 12/5/x3 with any other user account, providing them with Level 2 permissions regardless of their normal privileges on the port, if any.

For information about permission levels and how to set locks and lock-sharing, refer to Set Locks and Lock-Shares.

Create Roles

This section describes the steps for creating roles and assigning user to those roles. Before creating roles, refer to About Role-Based Access. However, GigaVUE nodes have three built-in roles for specifying which users have access to a given port. These roles are:

- **Admin**

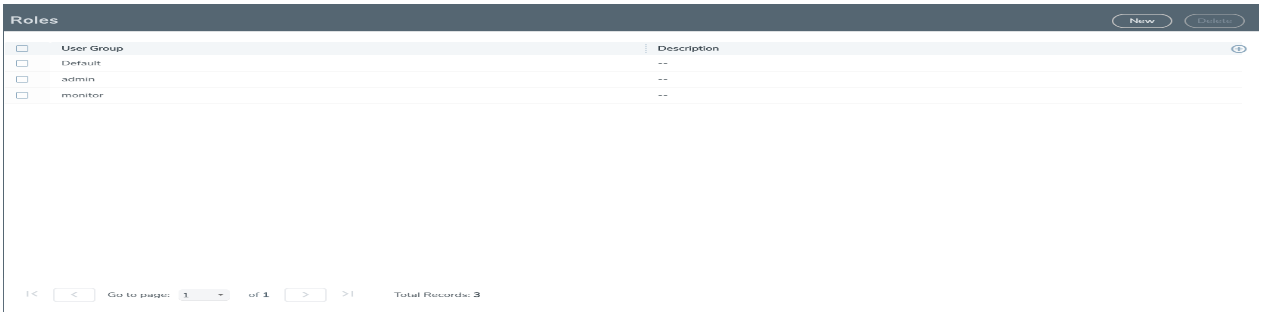
  This role provides access to all command modes, including Standard, Enable, and Configure. Admin users also have access to all commands and all ports. They are also members of all groups.
- **Default**

  This role also provides access to all command modes. Users with the Default role has no access to unassigned ports. New users are created with the Default role automatically. However, you can remove it if you do not want to allow a user access to unassigned ports
- **Monitor**

This role provides view-only access to ports and configurations. Administrators create additional custom *roles* and assign them to users together with the Default role. For example, if you create a role named Security_Team and assign it to tool port 5/1/x2, users assigned the Security_Team role are able to access tool port 5/1/x2. Conversely, users without a role that gives them some access to tool port 5/1/x2 will not even be able to see it in GigaVUE-FM. Users can have multiple assigned roles, allowing administrators to fine-tune access to the Visibility Platform.

To create roles and assign users to those roles, do the following:

1. Select **Roles and Users** in the Navigation pane, then select the **Roles** page.



□	User Group	Description
□	Default	--
□	admin	--
□	monitor	--

Total Records: 3

2. Click **New**.
3. On the **New Role** page, do the following:
   - Enter a role in the **Role Name** field. For example, Security_Team.
   - (Optional) Enter a description of the role in the **Descriptions** field.
4. Click **Save**.
5. Add users to the role. Refer to Add Users.

Configure Role-Based Access and Setting Permissions in GigaVUE Nodes

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

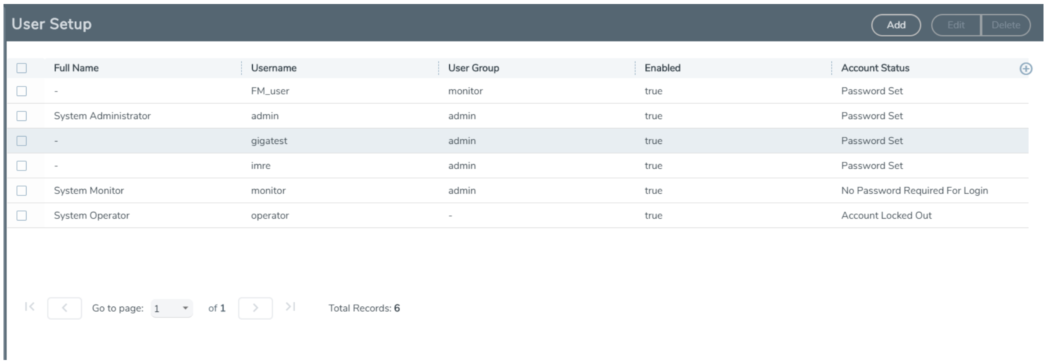
- Add Users
- Create Roles
- Associate Roles with Port Permissions
- Set Locks and Lock-Shares
- Set Map-Sharing Permission Levels

Add Users

This section provides the steps for adding users to the GigaVUE-OS nodes. Users are also assigned to roles that set their access permissions. Refer to the Create Roles section for more details.

To add users, do the following:

1. Select **Roles and Users > Users.** The **User Setup** page displays.



☐	Full Name	Username	User Group	Enabled	Account Status
☐	-	FM_user	monitor	true	Password Set
☐	System Administrator	admin	admin	true	Password Set
☐	-	gigatest	admin	true	Password Set
☐	-	imre	admin	true	Password Set
☐	System Monitor	monitor	admin	true	No Password Required For Login
☐	System Operator	operator	-	true	Account Locked Out

Go to page: 1 of 1 Total Records: 6

2. Click **Add**. The **Add New User** page displays.
3. On the Add New User page:
   - Enter a user name for this account in **User Name** field.
   - Enter the user's actual name in the **Name** field.
   - Enter a password for the user in the **Password** field and in the **Confirm Password** field. Refer to the Password Policies section in the GigaVUE-OS CLI Reference Guide.

   > **NOTE:** GigaVUE-FM prompts you to enter your password. Enter your password and click **Submit**.

   - Assign a role to the user by clicking in **Capability** field and selecting a role from the drop-down list. For the steps to create a role, refer to Create Roles.
4. Select **Enable** to enable the user's account, and then click **Save**.
5. The added users will then be listed in the **User Setup** page. In GigaVUE-OS, this list will also display the **Last Login** and **Number of Login Attempts** of a user.

Associate Roles with Port Permissions

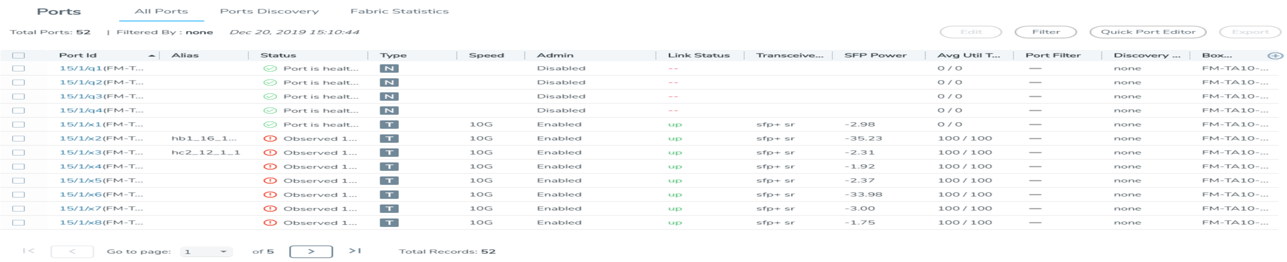
Users are assigned roles based on their user group. Each user group is given permission to specific ports on the node. There are four port-based permission levels, which are as follows:

Permission Level	Description
Level 1	The user can view the port but cannot make any changes to port

Permission Level	Description
	settings or maps. When applied to a network port, the user can view maps attached to the network port. This level is used for users who only need to monitor the activities of the port.
Level 2	The user can use the port for maps, create tool-mirror to or from the port, and change egress port filters. The user can configure port-lock, lock-share, and all traffic objects except port-pair. Also includes all Level 1 permissions.
Level 3	The user can configure port parameters (such as administrative status of the port, speed, duplex, and autonegotiation), as well as create port pairs. Also includes all Level 2 and Level 1 permissions.
Level 4	The user can change the port type. Also includes all Level 3, 2, and 1 permissions.

To associate roles with port permission, do the following:

1. Select **Ports** in the Navigation pane, then go to **Ports > All Ports**.
2. Select the port or ports on which you want to set permissions.



Ports | All Ports | Ports Discovery | Fabric Statistics

Total Ports: **52** | Filtered By : **none** *Dec 20, 2019 15:10:44*

□	Port Id	Alias	Status	Type	Speed	Admin	Link Status	Transceive...	SFP Power	Avg Util T...	Port Filter	Discovery ...	Box...
□	15/1/q1(FM-T...		Port is healt...	N		Disabled	--			0 / 0	—	none	FM-TA10-...
□	15/1/q2(FM-T...		Port is healt...	N		Disabled	--			0 / 0	—	none	FM-TA10-...
□	15/1/q3(FM-T...		Port is healt...	N		Disabled	--			0 / 0	—	none	FM-TA10-...
□	15/1/q4(FM-T...		Port is healt...	N		Disabled	--			0 / 0	—	none	FM-TA10-...
□	15/1/x1(FM-T...		Port is healt...	T	10G	Enabled	up	sfp+ sr	-2.98	0 / 0	—	none	FM-TA10-...
□	15/1/x2(FM-T...	hb1_16_1...	Observed 1...	T	10G	Enabled	up	sfp+ sr	-35.23	100 / 100	—	none	FM-TA10-...
□	15/1/x3(FM-T...	hc2_12_1_1	Observed 1...	T	10G	Enabled	up	sfp+ sr	-2.31	100 / 100	—	none	FM-TA10-...
□	15/1/x4(FM-T...		Observed 1...	T	10G	Enabled	up	sfp+ sr	-1.92	100 / 100	—	none	FM-TA10-...
□	15/1/x5(FM-T...		Observed 1...	T	10G	Enabled	up	sfp+ sr	-2.37	100 / 100	—	none	FM-TA10-...
□	15/1/x6(FM-T...		Observed 1...	T	10G	Enabled	up	sfp+ sr	-33.98	100 / 100	—	none	FM-TA10-...
□	15/1/x7(FM-T...		Observed 1...	T	10G	Enabled	up	sfp+ sr	-3.00	100 / 100	—	none	FM-TA10-...
□	15/1/x8(FM-T...		Observed 1...	T	10G	Enabled	up	sfp+ sr	-1.75	100 / 100	—	none	FM-TA10-...

Go to page: 1 of **5** Total Records: **52**

3. Click **Edit**.
4. In the Permissions section of the **Ports** page, assign roles to the permissions levels.
5. Click **Save**.

Set Locks and Lock-Shares

This section provides the procedures for setting port locks and lock-sharing. Before doing these procedures, refer to Locks and Lock Sharing. The procedures for setting lock and lock-sharing are as follows:

- Remove a Lock from a User’s Port
- Remove a User’s Lock-Share
- Lock a Port for a User

Remove a Lock from a User’s Port

To remove a user’s lock from a port, administrators do the following:

1. Select **Ports** in the Navigation pane, then go to **Ports > All Ports**.
2. Select the port on which you want to remove a lock.
3. Click **Edit**.
4. Clear the **Lock Port** check box.

Remove a User's Lock-Share

To remove a user's lock-share, administrators do the following:

1. Select **Ports** in the Navigation pane, then go to **Ports > All Ports**.
2. Select the port or ports on which you want to remove a lock-share.
3. Click **Edit**.
4. Click on the **Lock shared with Users** field and remove the user.
5. Click **Save**.

Lock a Port for a User

To lock a port for a user, administrators can do the following:

1. Select **Ports > Ports > All Ports**.
2. Select the port or ports on which you want to remove a lock.
3. Click **Edit**.
4. Select **Lock Port** if it is not already selected.
5. Click on the **Lock shared with Users** field and add the user.

Reboot and Upgrade Options

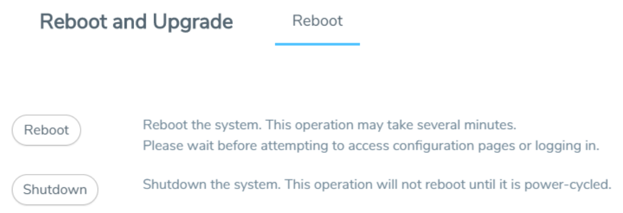
This section describes how to upload and upgrade images on GigaVUE nodes. For more detailed instructions on the upgrade paths available, refer to the *GigaVUE H Series Upgrade Guide* and *GigaVUE TA Series Upgrade Guide*. The major sections include:

- Reboot the Nodes
- Upgrade the Software
- Work with Configuration Files in the Configurations Page

Reboot the Nodes

Use the Reboot page to reboot the node. The reboot steps are as follows:

1. Using administrator user credentials, log in to GigaVUE-FM for the node to reboot.
2. Select **Settings > Reboot and Upgrade > Reboot**. The Reboot page displays as shown in Figure 21Reboot Page.



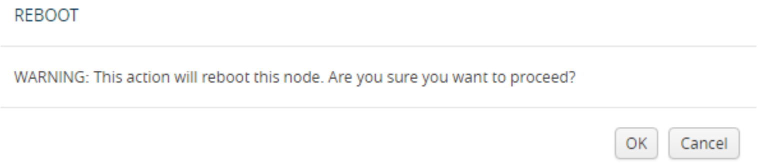
Reboot the system. This operation may take several minutes.
Please wait before attempting to access configuration pages or logging in.

Shutdown the system. This operation will not reboot until it is power-cycled.

Figure 21 *Reboot Page*

3. Click **Reboot**. A dialog will appear asking if you want to proceed.
4. To reboot the node, do either of the following:
   - Reboot

     If no changes have been made to the current configuration, the dialog shown in the following figure appears. Click **OK** to reboot the node.


REBOOT

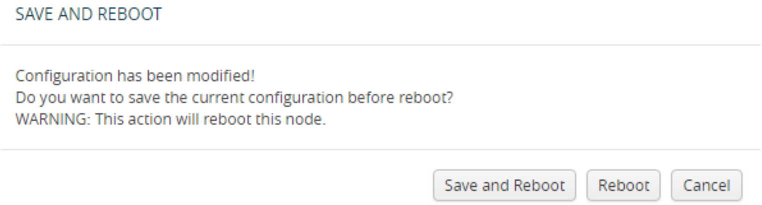
WARNING: This action will reboot this node. Are you sure you want to proceed?

Figure 22 *Reboot Dialog*

   - Save the configuration and reboot

     If there are any changes to the current configuration, the reboot dialog displays a warning that current configuration has been modified as shown in the following figure. Click **Save and Reboot** to save the configuration before reboot.

     Note: If you click Reboot, the configuration will not be saved and any changes to the configuration will be lost after reboot.


SAVE AND REBOOT

Configuration has been modified!
Do you want to save the current configuration before reboot?
WARNING: This action will reboot this node.

Figure 23 *Save and Reboot*

A dialog displays indicating that the running configuration was saved and system reboot initiated successfully. Click **OK**. When the login page appears, you can log back in.

Upgrade the Software

This section provides the steps for upgrading the software version on a standalone GigaVUE node.

In a cluster configuration, if you try to update the software through GigaVUE-FM, the following message is displayed across the Images tab:

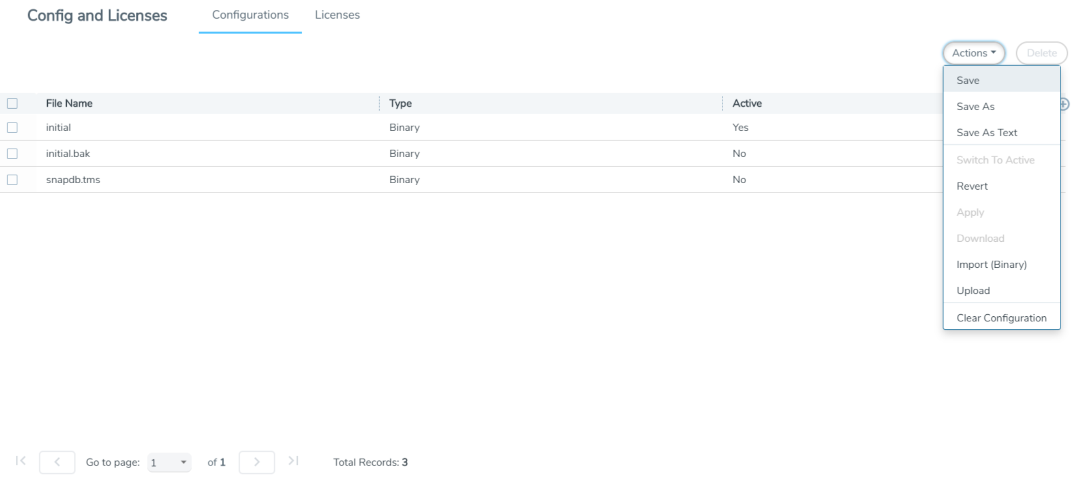
```
This is just a WARNING. It is recommended that you use the CLI to upgrade software
on the GigaVUE HC Series nodes when in a cluster.
```

> **Important:** The default password on the admin account is admin123A!. If the node is upgraded through the **configuration-jumpstart** command, the password for the admin user is required to be set to a non-default value. This will be the password when the admin user logs into GigaVUE-FM after the upgrade.

Save the Configuration

Before upgrading the software, save your current running configuration by doing the following:

1. Select **Setting > Config and Licenses > Configurations > Actions**.
2. Select **Action > Save** menu as shown in the following figure.



File Name	Type	Active
initial	Binary	Yes
initial.bak	Binary	No
snapdb.tms	Binary	No

Go to page: 1 of 1 Total Records: 3

> **NOTE:** You can also save the current configuration by selecting **Admin > Save Configuration** a shown in the following figure.

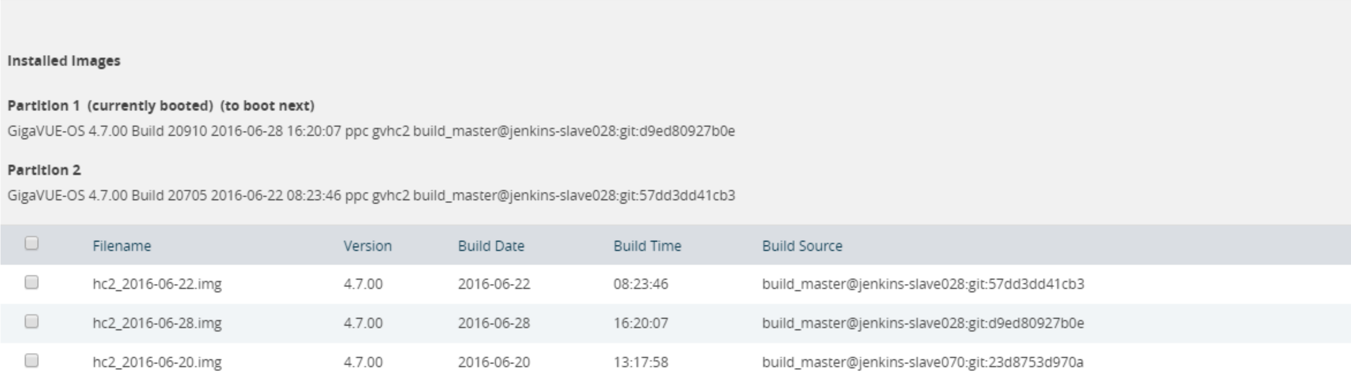
3. If you used the **Action** menu, confirm that you want to save the configuration by Clicking **Save** on the dialog screen that displays, as follows:

Upgrade the Software

Use the following steps to upgrade the software:

1. Access the GigaVUE node using a Web browser and log in with administrator user credentials.
2. Select **Settings > Reboot and Upgrade > Images**.

   The Images page shows the currently installed images and indicates the which image will boot next. Figure 24Active Images Page Showing Both Partitions shows an example where three images are currently installed. To change the image that will boot next select, **Action > Switch Boot Partition**.



Installed Images

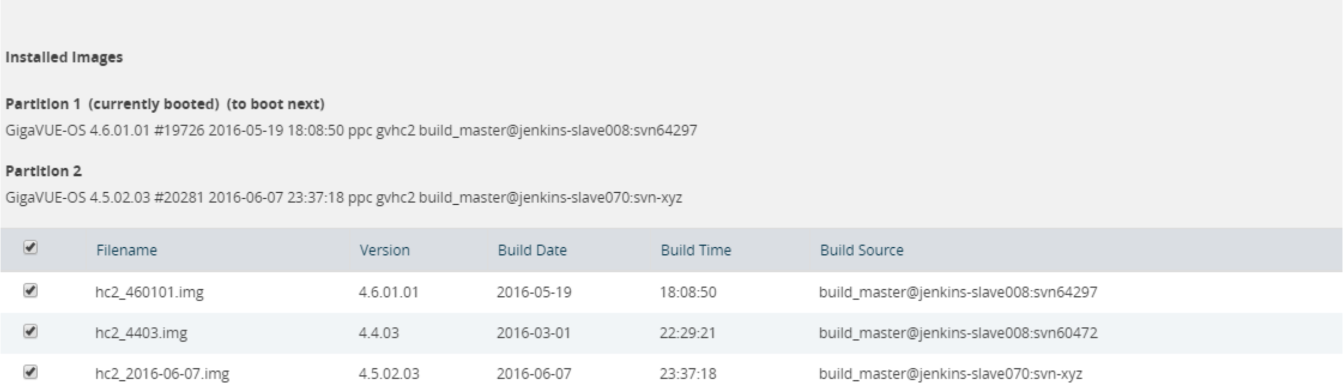
Partition 1 (currently booted) (to boot next)
GigaVUE-OS 4.7.00 Build 20910 2016-06-28 16:20:07 ppc gvhc2 build_master@jenkins-slave028:git:d9ed80927b0e

Partition 2
GigaVUE-OS 4.7.00 Build 20705 2016-06-22 08:23:46 ppc gvhc2 build_master@jenkins-slave028:git:57dd3dd41cb3

☐	Filename	Version	Build Date	Build Time	Build Source
☐	hc2_2016-06-22.img	4.7.00	2016-06-22	08:23:46	build_master@jenkins-slave028:git:57dd3dd41cb3
☐	hc2_2016-06-28.img	4.7.00	2016-06-28	16:20:07	build_master@jenkins-slave028:git:d9ed80927b0e
☐	hc2_2016-06-20.img	4.7.00	2016-06-20	13:17:58	build_master@jenkins-slave070:git:23d8753d970a

Figure 24 *Active Images Page Showing Both Partitions*

3. Remove all the currently uploaded images.
   a. As shown in Figure 25All Image Files Selected, select the check boxes.
   b. Click **Delete**.



Installed Images

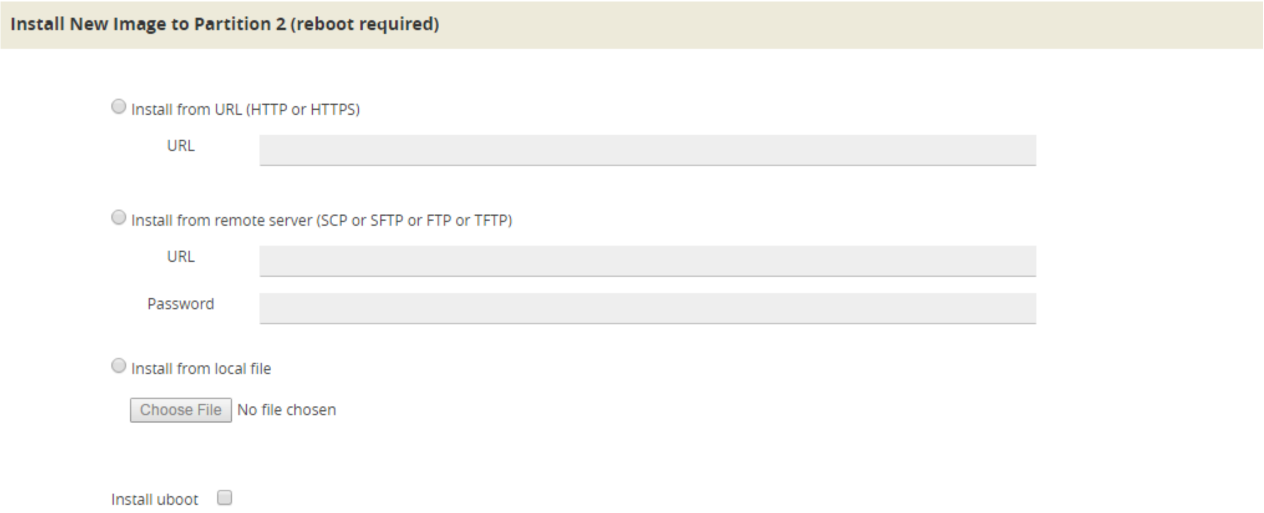
Partition 1 (currently booted) (to boot next)
GigaVUE-OS 4.6.01.01 #19726 2016-05-19 18:08:50 ppc gvhc2 build_master@jenkins-slave008:svn64297

Partition 2
GigaVUE-OS 4.5.02.03 #20281 2016-06-07 23:37:18 ppc gvhc2 build_master@jenkins-slave070:svn-xyz

☑	Filename	Version	Build Date	Build Time	Build Source
☑	hc2_460101.img	4.6.01.01	2016-05-19	18:08:50	build_master@jenkins-slave008:svn64297
☑	hc2_4403.img	4.4.03	2016-03-01	22:29:21	build_master@jenkins-slave008:svn60472
☑	hc2_2016-06-07.img	4.5.02.03	2016-06-07	23:37:18	build_master@jenkins-slave070:svn-xyz

Figure 25 *All Image Files Selected*

4. On the Images page, click **New** to access a new application image. The Install New Image page displays as shown in Figure 26Install a New Image Page.



Install New Image to Partition 2 (reboot required)

○ Install from URL (HTTP or HTTPS)

URL

○ Install from remote server (SCP or SFTP or FTP or TFTP)

URL

Password

○ Install from local file

Choose File No file chosen

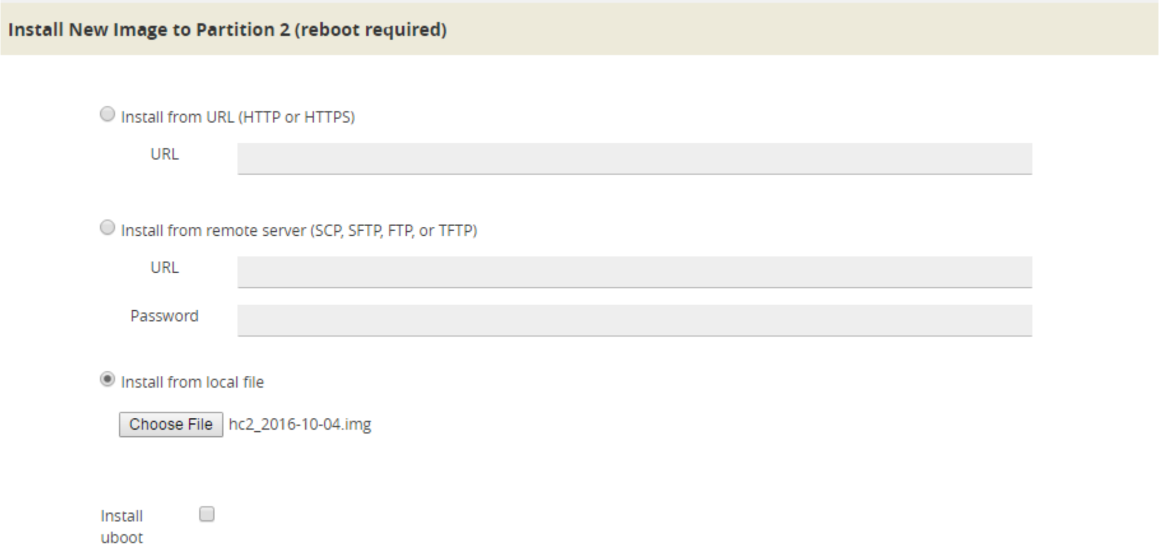
Install uboot □

Figure 26 *Install a New Image Page*

5. Select the method for installing the new image, which is one of the following:
   - **Install from URL** — Enter the URL from which to fetch the image.
   - **Install from scp or sftp** — Enter the URL and password of the SCP or SFTP server from which to fetch the image.
   - **Install from local file** — Use this option to upload the image file from your local environment. Click **Choose File** to select the file.

   > **NOTE:** The image must match the type of control card system (for example, HCCv2, GigaVUE-TA1, or GigaVUE-HC2).

   In Figure 27Local File Selected for Install, a local file is selected for the install.



Install New Image to Partition 2 (reboot required)

○ Install from URL (HTTP or HTTPS)

URL

○ Install from remote server (SCP, SFTP, FTP, or TFTP)

URL

Password

● Install from local file

Choose File hc2_2016-10-04.img

Install uboot □

Figure 27 *Local File Selected for Install*

6. Click **OK** after the software path is selected. A progress bar appears below the title bar.

   The new software is uploaded and installed. It is then active upon the next reboot.

7. To make the image effective, reboot the system.

   Refer to Reboot the Nodes for the steps to reboot the system.

Upgrade Uboot and PLD

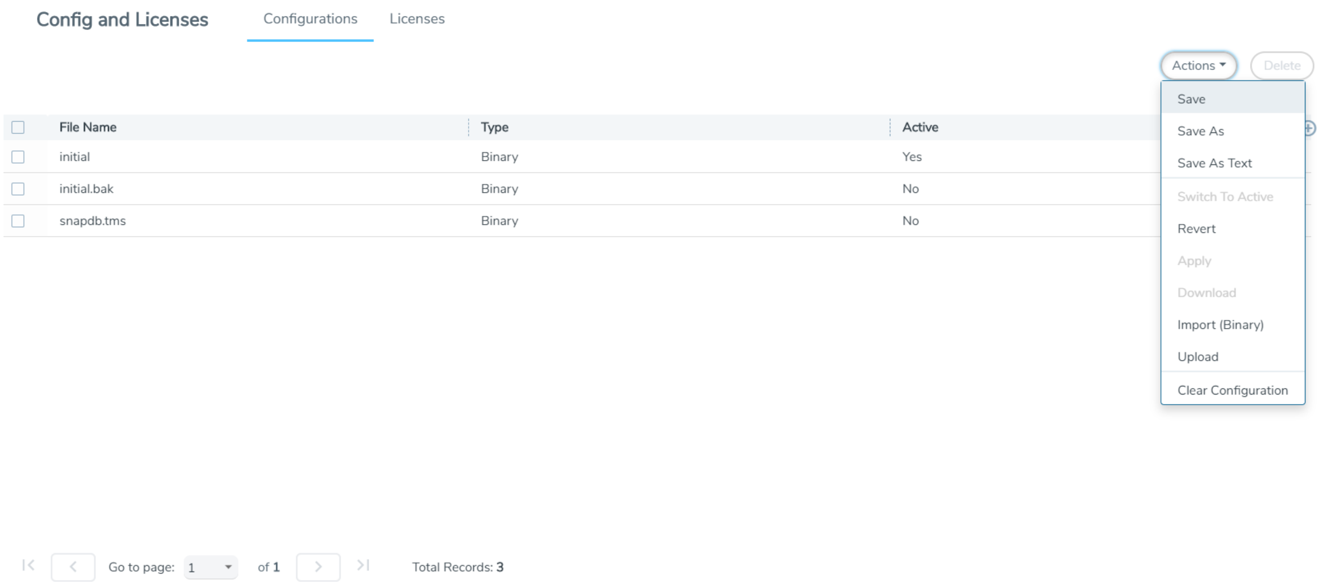
Use the following steps to upgrade Uboot and Programmable Logic Device (PLD):

1. Access the GigaVUE node using a Web browser and log in with administrator user credentials.
2. Select **Settings > Reboot and Upgrade > PLD and Uboot**.
3. For Uboot upgrade, check **Uboot** to upgrade to a new Uboot version, then click **Upgrade**.
4. For PLD upgrade, check **PLD** to upgrade Programmable Logic Devices (PLDs) such as Field Programmable Gate Arrays (FPGAs) on GigaVUE-HC3 nodes.
5. Select the slot, then click **Upgrade**.

Work with Configuration Files in the Configurations Page

GigaVUE-OS provides the ability to save and restore configuration files including all of the settings in place on the system at any time.

To work with configuration files, use the options available when you select **Settings > Config and Licenses > Configurations**, which displays the Configuration Files page shown in Figure 28Configuration Files Page.



□	File Name	Type	Active
□	initial	Binary	Yes
□	initial.bak	Binary	No
□	snapdb.tms	Binary	No

Figure 28 *Configuration Files Page*

The following sections describe how to set the options:

- Configuration File Options

- Configuration Actions
- Upload a Configuration
- Import a Configuration

Configuration File Options

The Configuration Files page lists the configuration files currently saved on the node. The last booted configuration file is listed with Yes in the Active column. From here, you can perform the following tasks when you select a configuration file:

- Click **Switch To Active** to load the selected configuration file, applying its settings.
- Click **Delete** to remove the selected file from the system.
- Click **Download** to download the file to your local environment.
- Click **Action** to select various operations to perform on the files. For details, refer to Configuration Actions.

Configuration Actions

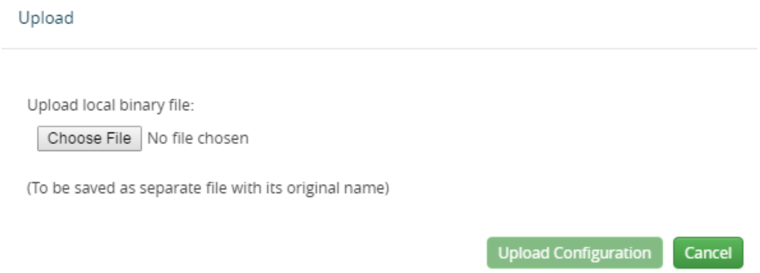
The active configuration is the combination of the last booted configuration file and all unsaved commands that led to the current running configuration. On the Configuration page, you can perform the following tasks with the **Actions** menu:

- Click **Action > Save** to save the running configuration to the active configuration file (the one listed in bold in the Configuration Files table, above).
- Click **Action > Revert** to discard the running configuration and apply the contents of the active configuration file.
- Click **Action > Save As** to save the running configuration to a new file and make it active. Use the adjacent field to provide a name for the new configuration file.
- Click **Action > Upload** to upload a binary configuration file. For details, refer to Upload a Configuration.
- Click **Action > Import** to import a configuration file. For details, refer Import a Configuration.

Upload a Configuration

Use the Upload Configuration options to send configuration files from the local system to the GigaVUE node. To upload a configuration file, do the following:

1. Select **Actions > Upload**. The Upload dialog displays as follows:



Upload

Upload local binary file:

(To be saved as separate file with its original name)

2. On the Upload Dialog, click **Choose File** to upload the binary file.
3. After the file is uploaded, click Upload Configuration.

   The file is saved on the GigaVUE node with its original name. This is handy when you've saved some standard configuration files to your system using the Save command in the Configuration Files section above.

Import a Configuration

To retrieve a saved configuration file from a remote host, using HTTP, HTTPS, SCP, SFTP, FTP, or TFTP, do the following:

1. Select the **Action > Import**. The Import Configuration Files page displays.
2. Select the **Protocol** to use, which is one of the following: HTTP, HTTPS, SCP, SFTP, FTP, or TFTP.
3. Supply the IP address or hostname of the remote host in the **Hostname or IP Address** field.
4. Provide the credentials used to log in to the system by entering the user name in the **Remote Username** field and the user's password in the **Remote Password** field.
5. In the File Path field, provide the filename and filename path on the remote system.
6. Click **Import**.

Backup and Restore

Backing up and restoring nodes is a time consuming process. GigaVUE-FM lets you back up and restore the configuration of all of the managed GigaVUE nodes, including H Series, TA Series, and G Series. At the end of the backup or restoring process an event is posted that indicates a success or failure of the backup. For G Series nodes, you can also use the Bulk Configuration feature. For more information, refer to Bulk Configuration.

This chapter covers the following topics:

- Nodes and Cluster Backup
- Node and Cluster Restore
- What Is Saved In a Configuration File
- Save a Configuration File
- Share Configuration Files with Other GigaVUE H Series Nodes

Nodes and Cluster Backup

This section describes how to backup HC Series, TA Series, and G-Series nodes. When a node is backed up, the backup file is saved in local storage on the machine where Fabric Manager is installed. The filename is the timestamp of the backup. Starting from 5.5, backups are in text based and binary formats. For security reasons, text configuration files do not include plain text passwords, such as SMTP passwords, AAA keys (RADIUS or TACACS+), or private keys in RSA/DSA identities. When a cluster is backed up, a backup file is created for the leader only.

You can schedule node or nodes and node clusters for immediate backup or scheduled backups to occur at a specified time. For example, you can schedule a backup for a particular day, week, month, or date.

Notes:

- Prior to GigaVUE-FM 3.2, backup file for physical nodes were in a binary format. Starting with GigaVUE-FM 3.2 backup and restore files use a text based format and binary backup or restore on physical nodes is not supported. If you are upgrading from a version lower than 3.2, you can backup your configuration prior to upgrading to the current version of GigaVUE-FM if you desire, but the files will be in a binary format. Existing binary backups are not visible to the current version of GigaVUE-FM. For binary backups, you must back up the node using the CLI commands rather than GigaVUE-FM. For more information about the CLI commands, refer to the *GigaVUE-OS CLI Reference Guide*.
- Clusters can be backed up only if the Leader in the cluster is licensed.
- For clusters with software version 4.6 or lower and a nat-enabled setup, GigaVUE-FM does not support the backup/restore operation. For nat-enabled clusters with software version 4.7 or higher, GigaVUE-FM supports backup/restore.
- For a cluster, the cluster name is the actual cluster’s name. For example, Gigamon-Cluster.
- For a restore operation on a cluster, cluster name changes are not supported. The cluster name must be the same as when the backup was made.
- For standalone devices the cluster name is the IP of the device.

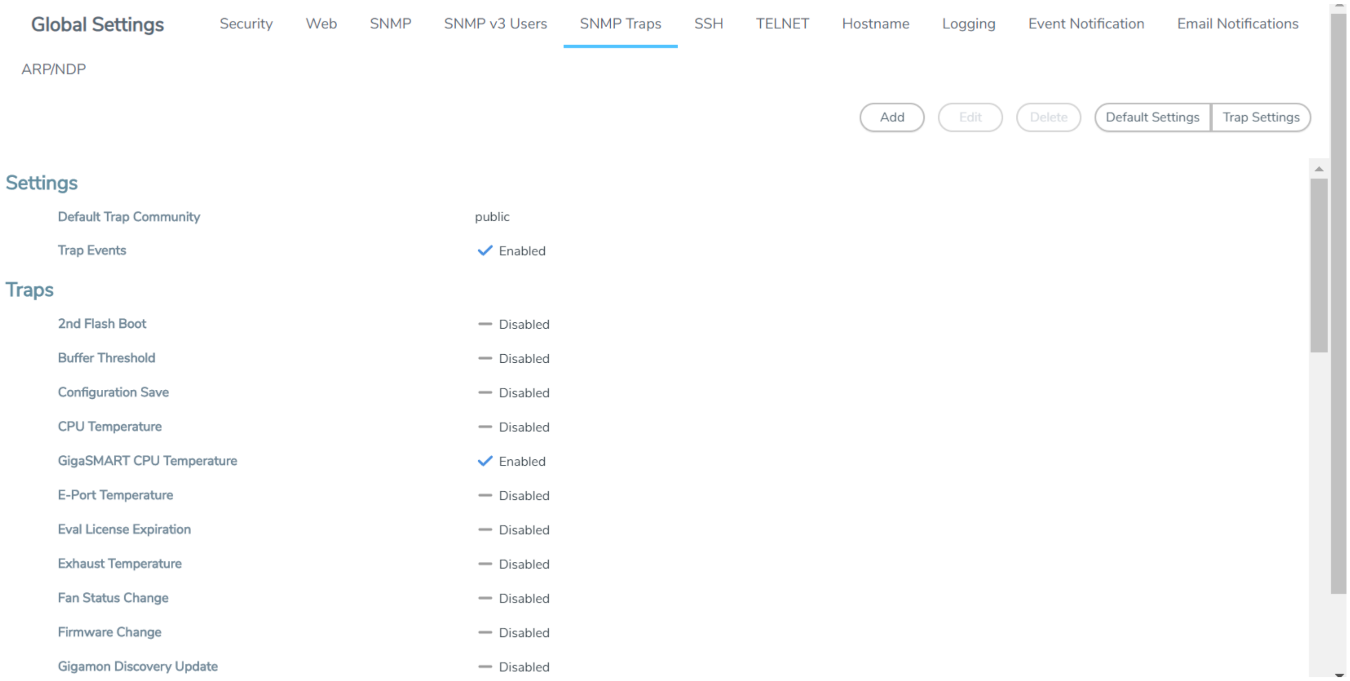
Enable Events for Backup

If you want to see fine-grained events on the node during the backup process, you need to enable the *configuration save* SNMP trap. To enable the trap, do the following:

1. Click **Physical** on the top navigation bar. On the **Physical Nodes** page, select the node on which you want to enable the trap.
2. Select **Settings > Global Settings > SNMP Traps**. The SNMP Trap page is displayed.
3. Click **Trap Settings.**

4. On the Edit SNMP Trap Setting page, select **Configuration Save**.
5. Click **Add**.

   The system returns to the SNMP Traps page and displays an event message that the SNMP trap is enabled as shown in Figure 29SNMP Trap Configuration Save Enabled.



Settings

Default Trap Community public

Trap Events ✓ Enabled

Traps

2nd Flash Boot — Disabled

Buffer Threshold — Disabled

Configuration Save — Disabled

CPU Temperature — Disabled

GigaSMART CPU Temperature ✓ Enabled

E-Port Temperature — Disabled

Eval License Expiration — Disabled

Exhaust Temperature — Disabled

Fan Status Change — Disabled

Firmware Change — Disabled

Gigamon Discovery Update — Disabled

Figure 29 *SNMP Trap Configuration Save Enabled*

BackUp Nodes and Clusters

To backup a node, nodes, or clusters, do the following:

1Click **Physical** on the top navigation bar.

2On the Physical Nodes page, select the node, nodes, or clusters that you want to backup.

1. Select **Actions > Backup**. The Backup page displays, showing the nodes selected for backup.
2. Select one of the following:
   - **Immediate—** Allows the back up to occur immediately.
   - **Scheduled—**Allows you to schedule a time for the backup or have reoccurring backups. For information about scheduled backup, refer to How to Schedule Backups for details on how to create a schedule.
3. Click **OK**.

   If you selected **Immediate** in Step 2, the system returns to the Physical Nodes page and displays an event message about the start of the backup proces. You can also use the **Alarms/Events** to monitor progress.

If you selected **Scheduled**, the next backup occurs according to the schedule.

How to Schedule Backups

When creating a backup of nodes and clusters, you can create a schedule for performing regular backups of selected nodes and clusters. This allows you to backup the devices managed by GigaVUE-FM at best times, such as when you expect network traffic to be the least.

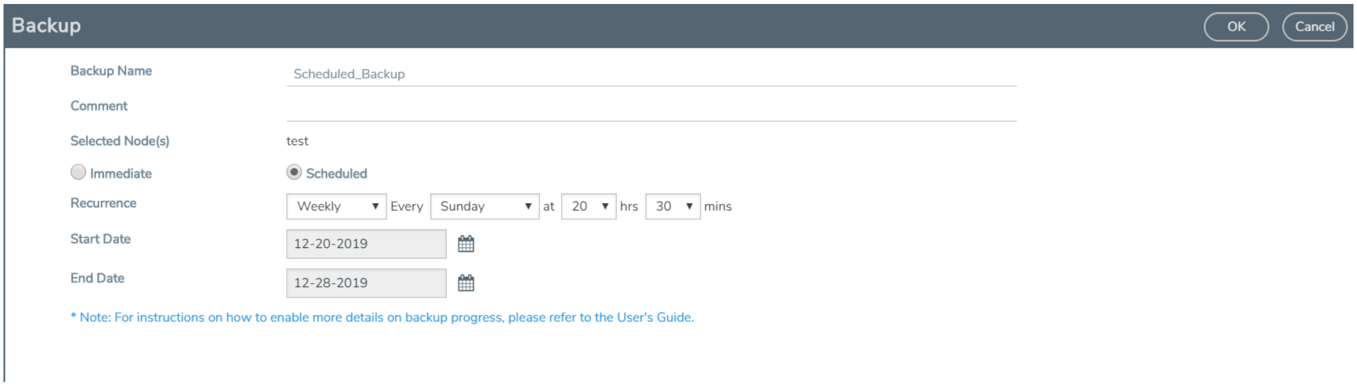
To set a schedule for backing up a nodes and clusters, do the following:

1. Click **Physical** on the top navigation bar.
2. On the Physical Nodes page, select the **Node IP** for each node that you want to backup.
3. Click **Actions > Backup**.

   The Backup page shows the number of nodes selected for backup.
4. Select **Scheduled**.

   The GigaVUE-FM time clock is based on ESX host time. Make sure that you have synchronized clock before any scheduling operation.

   Figure 30Nodes Selected for Scheduled Backups shows an example of nodes with scheduled backups. In this example, the weekly backups start on December 20 and occurs every Saturday at 8:30 pm until December 28.



Backup

Backup Name: Scheduled_Backup

Comment:

Selected Node(s): test

○ Immediate ● Scheduled

Recurrence: Weekly Every Sunday at 20 hrs 30 mins

Start Date: 12-20-2019

End Date: 12-28-2019

* Note: For instructions on how to enable more details on backup progress, please refer to the User's Guide.

Figure 30 *Nodes Selected for Scheduled Backups*

5. From the **Recurrence** drop-down list, select one of the following:

Table 10: Recurrence Options

Option	Description
Once Only	Select this option for scheduling one time backup. Set a start date and start time for the backup to begin.
Daily	Select this option for scheduling daily backups. Set a start date and time for the backup to recur once a day.

Option	Description
	Set an end date to determine until when the backup must recur.
Weekly	Select this option for scheduling weekly backups. Set a day, time, start date and end date for the weekly backup to recur.
Monthly	Select this option for scheduling backups once a month. Set a specific day of the month for the backup to recur. For example, if you want the backup to occur on every 15th day of the month, select 15th. Set a time, start date, and end date for the monthly backup to recur.
Yearly	Select this option for scheduling backups once a year. Set a specific day, month, time, start date, and end date for the yearly backup to recur.

6. Click **OK**. To monitor the progress of the event select Alarms/Events in the main navigation pane.

Once you have scheduled a recurring backup, the scheduled backup will appear as a scheduled task on the Scheduled Tasks page. To view tasks, select **Tasks > Scheduled Tasks**.

Download Backup Files

Because backup files are text-based and binary format, you can edit them in a text editor. You can restore the device configuration in binary format and view the configurations in text format. This is useful when you want to make modification before restoring the backup such as an error occurring during restore.

After creating a backup file as described in BackUp Nodes and Clusters, you can down load the file 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** to open the Backup Files page.

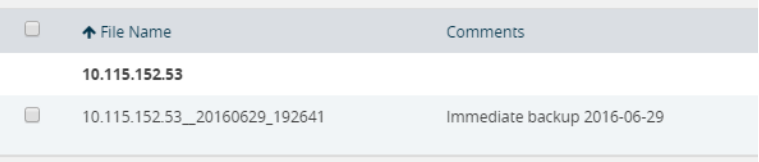
   The Backup Files page lists the backup files created from a scheduled or immediate backup.
3. Click the “Show Config” link on the backup record row to view the file contents of the file you wish to restore.
4. From the preview panel, click **Download**.
5. The backup file will be downloaded to the local environment.

Add Comments to Backup File

Starting in GigaVUE-FM 3.4, you can add a comment to the backup file that displays on the Backup Files page. A comment is useful for identifying particular backup files. To add a comment, do the following:

1. On the Backup Files page, select the file to which you want to add a comment.
2. Select **Edit**.
3. On the Edit page, enter a comment about the backup file in the **Comment** field.
4. Click **OK**.

   The comment is added to the comment field for the backup file. The following figure shows an example.



□	↑ File Name	Comments
	10.115.152.53	
□	10.115.152.53_20160629_192641	Immediate backup 2016-06-29

Set Do Not Purge Flag

> **NOTE:** GigaVUE-FM runs a background task every 12 hours that purges the backup files and restore logs if the number of backup files for a node is greater than 10. The oldest backup files are purged first. You can set a **Do Not Purge** flag so that backup files are not removed when a purge occurs. Files with the Do Not Purge flag set are not included in the automatic 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 that you do not want to be purged.
4. Select **Actions > Enable Do Not Purge**.

   A check mark appears in the Do No Purge field for the selected backup file.

To remove Do Not Purge for the backup file, select **Actions > Disable Do Not Purge**.

Delete Backup Files

To delete a backup file, do the following:

1. On the right side of the top navigation bar, click ⚙.

   1On the left navigation pane, select **System > Backup/Restore > Physical Nodes**.
2. Select one or more filenames on the Backup Files page.

3. Click **Delete**.

   The system displays a dialogue to confirm that you want to delete the file.

4. Click **OK**.

Backup files obtained from standalone nodes before they joined the cluster are called orphaned backup files. GigaVUE-FM does not allow you to delete an orphaned device-backup file. You must first delete the files from /var as well as from the database. Contact Gigamon Customer support to delete the files from the database. You can also refer to the knowledge base article for more details.

Node and Cluster Restore

Starting with GigaVUE-FM 3.2, backup files are text based and binary format. GigaVUE-FM restores the device configurations in binary format and allows you to view the configurations in text format. During the restore process, the commands listed in the configuration file are executed. If any error occur during the restore process, the text-based file makes it possible to edit the file and attempt to restore the configuration again by uploading and applying the modified file.

When restoring clusters, you can modify the file before uploading and applying it to the cluster. However, the modified file must have the same name as the backup file that was downloaded. If you change the file name, GigaVUE-FM will reject the file during the upload operation. The configuration file is applied to the current leader in a cluster and this node could be a different node than the one when the backup was done.

Notes:

- GigaVUE-FM does not support the restore operation if the cluster name changes. The cluster name should have the same name at the time of the restore operation as it did at the time of the backup operation.
- Text-based and Binary format backed up configurations created directly on the node, using the CLI , are also available for restoring from the GigaVUE-FM.
- In the Device Restore process, leader preferences for the cluster are only updated to the leader after restoring; they are not propagated to any of the standby nodes.

Restore Nodes and Clusters

To restore nodes or clusters, do the following:

1Click **Physical** on the top navigation bar.

1. On the Physical Nodes page, select the IP address for each node or cluster that you want to restore.

   2Select **Actions > Restore**.

   The Restore From File page displays, showing the file names from which to restore.

2. Select the configuration to restore by clicking the check box next to the file name. Only one configuration can be selected with a restore action.
3. Click **OK**.

View Restore Logs

Restores are a binary-based restore and use a fail-continue option during the restore process. If any errors occur, they are logged to the a restore log file. You can download and view the restore logs by doing the following:

1. On the right side of the top navigation bar, click ⚙.
2. On the left navigation pane, select **System > Backup Files > Physical Nodes**. The Backup Files page shows the list of existing backup files.
3. Click the **Restore Log Files** link.

   The Restore Logs page displays the restore logs currently available. If no restore action has occured, the restore logs page will be empty.

What Is Saved In a Configuration File

Configuration files store all of the settings in place on the GigaVUE H Series node when the file was saved—everything necessary to restore the node to its exact state when the file was saved. This includes:

- Map settings
- Port aliases
- Port parameters, including duplex, medium, speed, cable length, and so on
- Port-groups
- Port-pair settings
- Tool-mirror settings
- Port-type settings
- GigaStream settings

- All settings shown by the **show system** command
- User accounts, groups, and roles
- SNMP server/trap settings
- TACACS+, RADIUS, and LDAP servers
- NTP servers
- Syslog servers
- Host names
- Mgmt port IP settings
- Logging settings, including email notifications

Save a Configuration File

To save a configuration file, do the following:

1. Select **Settings > Config and Licenses > Configurations**.

   The Configuration files page displays.

2. Select **Actions** > **Save** the currently running configuration.

   > **NOTE:** If the you want to switch between multiple saved configuration files, you can use the **Switch to Active** button after selecting an existing configuration file.

3. When confirmation dialog displays, click **Save** to save the GigaVUE H Series node's current systems to the active configuration file.

   You can also save the GigaVUE H Series node's current systems to a new filename by selecting **Actions > Save As**, entering a filename in the **New Filename** field of the confirmation dialog, and then clicking **Save**.

In addition to saving the current configuration, you can do the following from the **Action** menu:

- **Revert**—reverting discards the running configuration and changes to the active configuration file.
- **Reset**—resetting changes the running and active configuration to the factory default. The active licenses, host keys, and configuration for network connectivity is preserved.
- **Upload**— allows you to upload files from the local drive. Click Browse to locate the file, and then **Upload Configuration** to upload the local file.
- **Import**—importing opens the **Import Configuration files** page. This page allows you to use external hosts that use protocols such as SFTP, FTP, TFTP or SCP. You can upload from a URL or IP address.

Share Configuration Files with Other GigaVUE H Series Nodes

You can apply a configuration file created on one node to a second node. Keep in mind the following notes:

- All configuration settings that are not related to packet distribution (maps, tool-mirrors, port-pairs, and GigaStream) are reusable on the new node.
- Configuration settings related to packet distribution are tied to the chassis ID from the node on which they were saved. You can move these to the new node using either of the following methods:
  - Delete the old node (no chassis) and provision a new one, using a new box ID, if required.

- If the box ID and module configuration of the new node is the same as the old node, you can perform a node migration using the procedure in the **Hardware Installation Guide**.

Use SNMP

This chapter describes how to use the SNMP features on the GigaVUE H Series and TA Series nodes. Refer to the following sections for details:

- SNMP and Clusters
- Configure SNMP Notifications
  - Configure the SNMP Server and Notification Destinations
  - Configure SNMP v3 Users
  - Enable Notifications
  - Delete a Destination for SNMP Notifications
  - Enable or Disable Events for SNMP Notifications
  - Receive Traps
  - View Associated Log Messages
- Enable the SNMP Server

SNMP and Clusters

When working with a cluster of GigaVUE H Series nodes, you configure SNMP hosts and notification events from the leader/VIP address. The settings are then pushed to each node. However, when a clustered node sends an SNMP notification, it is sent from its own Mgmt port, not from the leader/VIP address.

In addition, you browse each individual clustered node's MIB separately, not over the VIP/leader.

NOTE: A GigaVUE TA Series node can never assume the role of a leader in a clustered environment.

Configure SNMP Notifications

GigaVUE H Series nodes can send SNMP v1/v2c/v3 traps to specified destinations based on a variety of events on the node. Configuring SNMP traps consists of the following major steps:

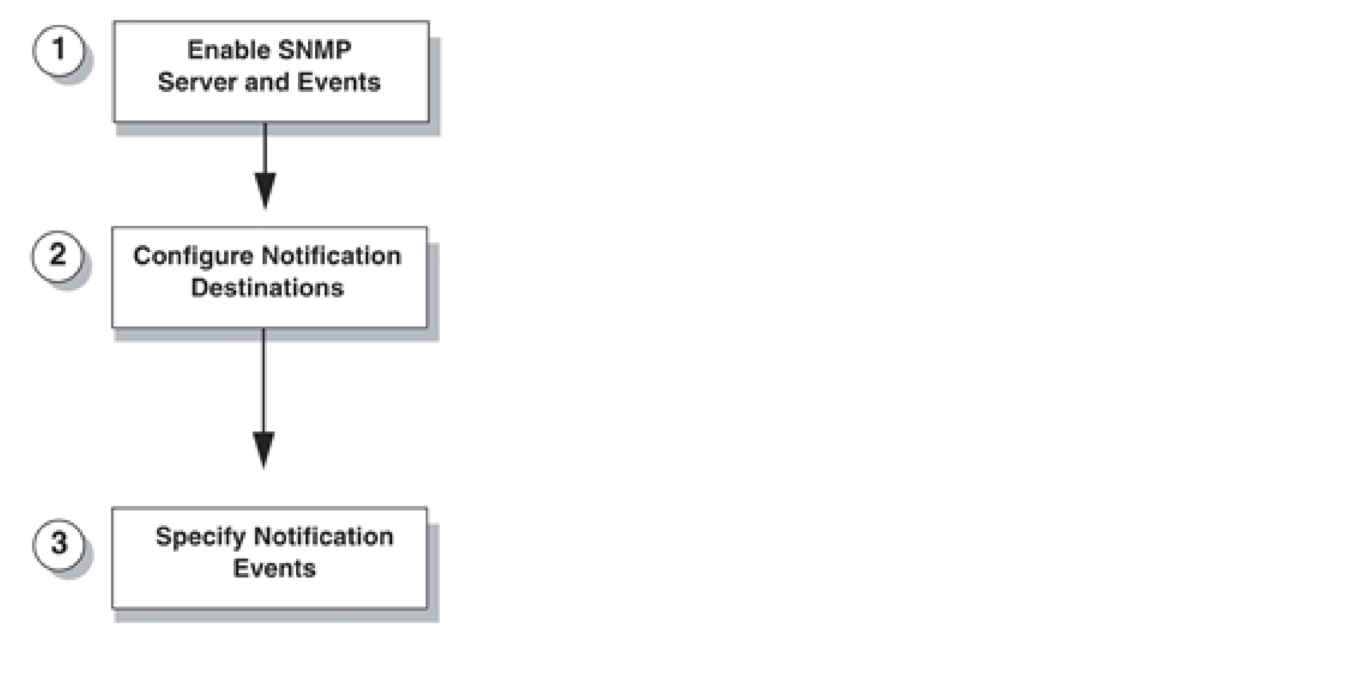

1
Enable SNMP Server and Events
2
Configure Notification Destinations
3
Specify Notification Events

Figure 31 *Configuring SNMP Notifications*

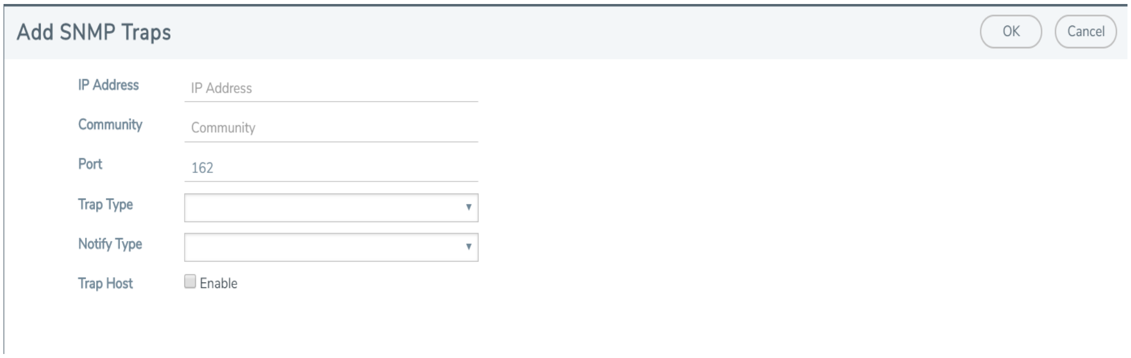
Configure the SNMP Server and Notification Destinations

The SNMP server on the GigaVUE H Series or TA Series must be enabled in order to send traps. This is done on the ADD SNMP Trap page, where you also you specify the destinations for SNMP notifications sent from the GigaVUE H Series or GigaVUE TA Series node.

> **NOTE:** The recommended maximum number of SNMP trap destinations is five (5).

To specify a notification destination and enable the SNMP sever, do the following:

1. Select **Settings > Global Settings > SNMP Traps**.
2. Click **Add**. The Add SNMP Traps page shown in Figure 35Edit SNMP Settings Page displays.


Add SNMP Traps

IP Address: IP Address
Community: Community
Port: 162
Trap Type:
Notify Type:
Trap Host: □ Enable

Figure 32 *Add SNMP Traps Page*

3. Configure the notification destination by doing the following:

a. Enter the IP address for the trap destination in the **IP Address** field.

b. Enter the community string in the **Community** field. For example, public.

c. Enter the server port number in the **Port** field.

d. Click in the **Trap Type** field and select **v2c**, **v1** or **v3** for the drop-down list.

If you select v3, you will also need to configure the SNMP v3 Users. Refer to Configure SNMP v3 Users.

e. Click in the Notify Type field and select **trap** or **inform.**

f. (Optional) If you selected v3 for Trap Type, enter the v3 username in the **v3 user** field.

g. Select **Enable** for **Trap Host** to enable the host.

4. Click **Save**.

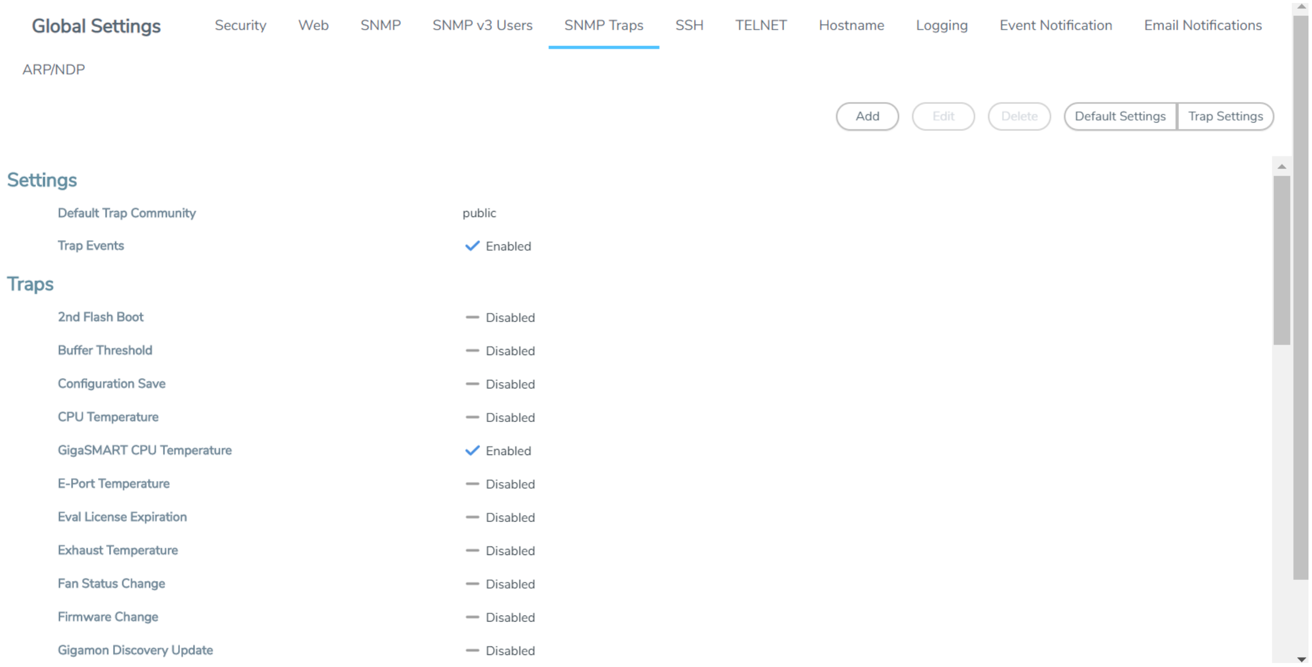
Configure SNMP v3 Users

If v3 is selected for the Trap Type when adding an SNMP trap, the SNMPv3 users also need to be configured. To configure an SNMP v3 user, do the following:

1. Select **Settings > Global Settings > SNMP v3 Users**.
2. Click **New**.
3. Enter the information for the SNMP v3 user.
   - **Username**—the name of the v3 user
   - **User**—Enables the user specified in the **Username** field when selected.
   - **Authentication Type**—the authentication type is either **md5** or **sha1**, which specified the mechanism to use for password hashing.
   - **Privacy Type**—the privacy type specifies the level of encryption for the password, which is either **des** or **aes-128**.
   - **Authentication Password**—the password used to authenticate the user specified by **Username**.
   - **Privacy Password**—a privacy password associated with the user specified by **Username** if a privacy type is specified. If no privacy type is specified, and a privacy password is entered, the default privacy type is aes-128.
4. Click **Save**.

Enable Notifications

Once the GigaVUE H Series or TA Series SNMP server is enabled, you can enable the sending of SNMP notifications from the SNMP through the SNMP page shown in Figure 33SNMP Settings Page.



Settings

Default Trap Community	public
Trap Events	✓ Enabled

Traps

2nd Flash Boot	— Disabled
Buffer Threshold	— Disabled
Configuration Save	— Disabled
CPU Temperature	— Disabled
GigaSMART CPU Temperature	✓ Enabled
E-Port Temperature	— Disabled
Eval License Expiration	— Disabled
Exhaust Temperature	— Disabled
Fan Status Change	— Disabled
Firmware Change	— Disabled
Gigamon Discovery Update	— Disabled

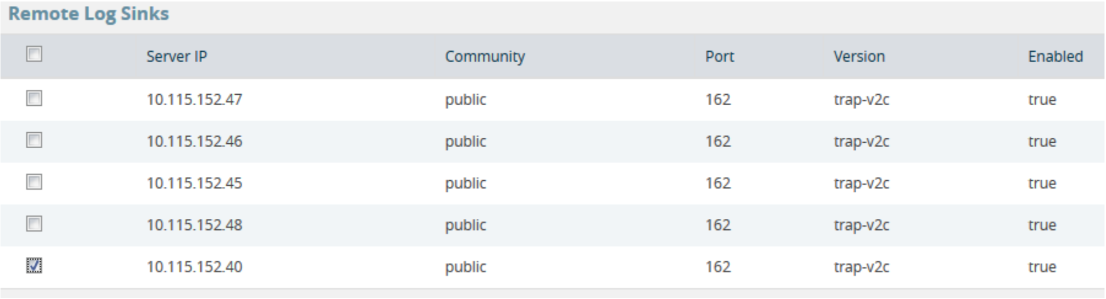
Figure 33 *SNMP Settings Page*

The GigaVUE H Series and GigaVUE TA Series SNMP server is enabled so that management stations can poll the node remotely using standard SNMP commands (**Get**, **GetNext**, and **Walk**). The GigaVUE H Series and GigaVUE TA Series nodes support MIB polling using the standard MIB-II OIDs.

Delete a Destination for SNMP Notifications

To delete a destination for SNMP notifications, do the following:

1. Select **Settings > Global Settings > SNMP Traps**.
2. Scroll to the bottom of the SNMP Traps page, and select the destination to delete under Remote Log Sinks. In Figure 34Notification Destination Selected, 10.115.152.40 is selected.



Remote Log Sinks

□	Server IP	Community	Port	Version	Enabled
□	10.115.152.47	public	162	trap-v2c	true
□	10.115.152.46	public	162	trap-v2c	true
□	10.115.152.45	public	162	trap-v2c	true
□	10.115.152.48	public	162	trap-v2c	true
☑	10.115.152.40	public	162	trap-v2c	true

Figure 34 *Notification Destination Selected*

3. Click **Delete**.
4. A verification dialog appears, asking if you want to delete the record. Click **OK**.

An event is generated indicating that the record was successfully deleted.

Enable or Disable Events for SNMP Notifications

To enable or disable events for SNMP Notifications:

1. From the device view, go to **System > Settings > Global Settings > SNMP Traps**.
2. Click **Trap Settings**. The Edit SNMP Trap Settings page opens.
3. Select or clear the **Enable** check box for the SNMP trap that you want to enable or disable.
4. Click **OK**.

Receive Traps

The GigaVUE H Series node's MIB is available for download from the Gigamon Documentation Library. The name of the MIB is GIGAMON-SNMP-MIB. Contact Technical Support for details.

Once you have received a copy of the MIB, you can compile it into your SNMP Management software to view intelligible descriptions of the OIDs included in the notifications.

View Associated Log Messages

SNMP events have log messages associated with them. The following table shows the log messages for each SNMP event.

Table 11: Log messages Associated with SNMP Event

SNMP Event	Description	Log Message
2ndflashboot	Secondary flash boot notification (for GigaVUE-TA100, GigaVUE-TA100-CXP, GigaVUE-HC1, and GigaVUE-HC3)	/gv/snmp/events/SecondFlashBoot
bufferoverusage	Buffer usage threshold crossing notification	/gv/snmp/events/buffer_threshold
gigasmartcputemp	GigaSMART engine temperature (for GigaVUE-HC1)	/gv/snmp/events/GigaSMARTCPUTemp
configsave	Configuration saved notification	
cputemp	CPU temperature notification (for GigaVUE-TA100, GigaVUE-TA100-CXP, GigaVUE-HC1, and GigaVUE-HC3)	/gv/snmp/events/CPUTemp
eporttemp	GigaSMART CPU (e1/e2 port) temperature notification (for	/gv/snmp/events/EPortTemp

SNMP Event	Description	Log Message
	GigaVUE-HC3)	
evallicensereminder	Evaluation license expiration notification	/gv/snmp/events/EvalLicenseReminder
exhausttemp	Exhaust temperature notification (for GigaVUE-TA100, GigaVUE-TA100-CXP, GigaVUE-HC1, and GigaVUE-HC3)	/gv/snmp/events/ExhaustTemp
fanchange	Fan status change notification	/gv/snmp/events/ResetSystem
firmwarechange	Firmware change notification	/gv/snmp/events/FirmwareChange
gdpupdate	GDP update notification	/gv/snmp/events/GdpUpdate
gscpuutilization	GigaSMART CPU utilization crossing threshold notification	/gv/snmp/events/CpuUtilization
gspacketdrop	GigaSMART packet drop notification	/gv/snmp/events/GsPacketDrop
gsresourceutilization	GigaSMART resource utilization notification	/gv/snmp/events/GsIsslResourceUtilization
ibstatechange	Inline bypass forwarding state change notification	/gv/snmp/events/IbStateChange
inlinetoolrecovery	Inline tool recovery notification	/gv/snmp/events/InlineToolRecovery
linkspeedstatuschange	Port link status or port speed change notification	/gv/snmp/events/LinkSpeedStatusChange
lowportutilization	Port utilization low threshold crossing notification	/gv/snmp/events/BelowThreshold
modulechange	Module change notification	/gv/snmp/events/ModuleChange
operationmode	Operational mode change notification	/gv/snmp/events/SystemModeChange
opticstemp	Optics (transceiver) temperature notification (for GigaVUE-TA100, GigaVUE-TA100-CXP, and GigaVUE-HC3)	/gv/snmp/events/OpticsTemp
packetdrop	Packet drop notification	/gv/snmp/events/PacketDrop
policytrigger	Policy triggered notification	/gv/snmp/events/PolicyTriggered
portutilization	Port utilization high threshold crossing notification	/gv/snmp/events/OverThresholdChange
powerchange	Power supply status change notification	/gv/snmp/events/PowerChange
processcputhreshold	Process CPU threshold notification	/gv/snmp/events/CcProcessCpuThreshold
processmemthreshold	Process memory threshold notification	/gv/snmp/events/CcProcessMemThreshold
rxtxerror	Packet receive (RX) or transmit	/gv/snmp/events/RxTxError

SNMP Event	Description	Log Message
	(TX) error	
switchcputemp	Switch CPU temperature notification (for GigaVUE-TA100, GigaVUE-TA100-CXP, GigaVUE-HC1, and GigaVUE-HC3)	/gv/snmp/events/SwitchCPUTemp
syscputhreshold	System CPU threshold notification	/gv/snmp/events/CcSystemCpuThreshold
sysmemthreshold	System memory threshold notification	/gv/snmp/events/CcSystemMemThreshold
systemreset	System reset notification	/gv/snmp/events/ResetSystem
tunnelstatus	Tunnel status notification	/gv/gs/snmp/events/TunnelGwStatusChange
tunneldesstatus	Tunnel destination status notification	/gv/gs/snmp/events/TunnelDestStatusChange
unexpectedshutdown	Unexpected system shut down notification	/gv/snmp/events/UnexpectedShutdown
userauthfail	User authentication failure notification	/gv/snmp/events/UserAuthFail
vportstatuschange	vport status change notification	/gv/snmp/events/VportStateChange
watchdogreset	Watchdog monitor reset notification	/gv/snmp/events/WatchdogReset

The following is a sample log message:

```
sysdump-hc2-144-20150506-150207/messages.1:May 6 14:26:33 hc2-144 mgmtd[1829]:
[mgmtd.INFO]: EVENT: /gv/snmp/events/LinkSpeedStatusChange
```

Enable the SNMP Server

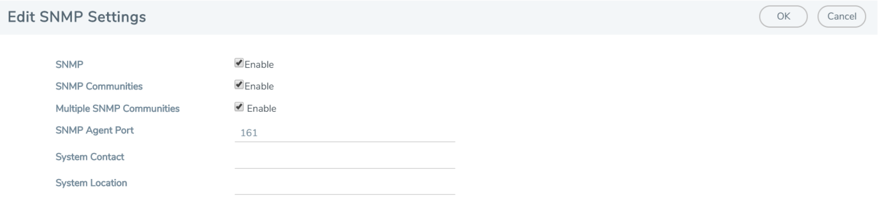
You can enable the GigaVUE H Series or GigaVUE TA Series SNMP server so that the SNMP management side can send SNMP requests by using **Get**, **GetNext**, and **GetBulk** SNMP commands to poll the node. The GigaVUE H Series and GigaVUE TA Series supports public MIBs, including partial MIB-II (ifTable and ifXTable).

The GigaVUE H Series and GigaVUE TA Series SNMP server is enabled so that management stations can poll the node remotely using standard SNMP commands (**Get**, **GetNext**, and **Walk**). The GigaVUE H Series and GigaVUE TA Series nodes support MIB polling using the standard MIB-II OIDs. You can retrieve statistics for any of the data ports. For a sample of ifIndex numbers, as well as a list of the supported statistics from the ifTable and ifXTable, refer to Available SNMP Statistics for Data Ports.

You can also load Gigamon’s MIB to view private MIB values.

To enable the SNMP server:

1. Select **Settings > Global Settings > SNMP**.
2. On the SNMP page, click **Settings**. The Edit SNMP Settings page displays as shown in Figure 35Edit SNMP Settings Page



SNMP ☑ Enable
SNMP Communities ☑ Enable
Multiple SNMP Communities ☑ Enable
SNMP Agent Port 161
System Contact
System Location

Figure 35 *Edit SNMP Settings Page*

3. Select **Enable** for SNMP.
4. Click **Save**.

Configure Other SNMP Server Settings

It is only required to select **Enable** to turn on the SNMP server. However, you should also configure the standard MIB-II contact information variables (syscontact and syslocation), the community string, and, optionally, the port.

To configure these additional settings, do the following:

1. Select Settings > Global Settings > SNMP.
2. Click Settings.
3. On the Edit SNMP Settings page, configure one ore more of the other SNMP server settings:
   - Enable SNMP Communities
   - Enable Multiple SNMP Communities.
   - Enter the system contact in the System Contact field.
   - Enter the system location in the System Location field.

   You can also change the settings that you configured in Configure the SNMP Server and Notification Destinations.
4. Click **Save**.

Recommendations for Vulnerabilities

For SNMP recommended best practices for vulnerabilities such as, Multiple Vendor SNMP public Community String Information Disclosure, refer to: http://www.kb.cert.org/vuls/id/107186

Gigamon makes the following recommendations to protect against SNMP vulnerabilities:

- Use the Gigamon ready-only community string (gigamon) to send traps and informs.
- Disable the default public community string.
- Use SNMPv3 to send traps and informs.
- Use a different port number from the default (162).

Available SNMP Statistics for Data Ports

When you poll a Mgmt port on the GigaVUE H Series and GigaVUE TA Series node, it provides MIB-II statistics for all data (network and tool) ports. Data ports are numbered sequentially with ifIndex numbers starting from the leftmost slot (slot 1) and proceeding sequentially through all slots. Within a slot, ports are numbered sequentially starting with the 10Gb ports and then the 10/100/1000 ports. For example, on a PRT-H00-X12G04 line card, ports number sequentially from 1/1/x1..1/1/x12 and then g1..g4.

You can use the **ifDescr** OID to correlate an ifIndex with a data port number on the GigaVUE H Series node. For example, the following table shows how ifIndex numbers are assigned to PRT-H00-X12G04 cards in slot 1 and slot 2 in the GigaVUE H Series node:

ifDescr OID	Value for a PRT-H00-X12G04 in Slots 1/2
ifDescr.1; Value (OctetString)	1/1/x1
ifDescr.2; Value (OctetString)	1/1/x2
ifDescr.3; Value (OctetString)	1/1/x3
ifDescr.4; Value (OctetString)	1/1/x4
ifDescr.5; Value (OctetString)	1/1/x5
ifDescr.6; Value (OctetString)	1/1/x6
ifDescr.7; Value (OctetString)	1/1/x7
ifDescr.8; Value (OctetString)	1/1/x8
ifDescr.9; Value (OctetString)	1/1/x9
ifDescr.10; Value (OctetString)	1/1/x10
ifDescr.11; Value (OctetString)	1/1/x11
ifDescr.12; Value (OctetString)	1/1/x12
ifDescr.13; Value (OctetString)	1/1/g1
ifDescr.14; Value (OctetString)	1/1/g2
ifDescr.15; Value (OctetString)	1/1/g3
ifDescr.16; Value (OctetString)	1/1/g4
ifDescr.17; Value (OctetString)	1/2/x1
ifDescr.18; Value (OctetString)	1/2/x2
ifDescr.19; Value (OctetString)	1/2/x3

ifDescr OID	Value for a PRT-H00-X12G04 in Slots 1/2
ifDescr.20; Value (OctetString)	1/2/x4
ifDescr.21; Value (OctetString)	1/2/x5
ifDescr.22; Value (OctetString)	1/2/x6
ifDescr.23; Value (OctetString)	1/2/x7
ifDescr.24; Value (OctetString)	1/2/x8
ifDescr.25; Value (OctetString)	1/2/x9
ifDescr.26; Value (OctetString)	1/2/x10
ifDescr.27; Value (OctetString)	1/2/x11
ifDescr.28; Value (OctetString)	1/2/x12
ifDescr.29; Value (OctetString)	1/2/g1
ifDescr.30; Value (OctetString)	1/2/g2
ifDescr.31; Value (OctetString)	1/2/g3
ifDescr.32; Value (OctetString)	1/2/g4

SNMP Statistics

The supported SNMP statistics (32-bit counters) from the ifTable are as follows:

- ifInOctets
- ifInUcastPkts
- ifInNUcastPkts
- ifInDiscards
- ifInErrors
- ifInUnknownProtos
- ifOutOctets
- ifOutUcastPkts
- ifOutNUcastPkts
- ifOutDiscards
- ifOutErrors

The supported SNMP statistics (64-bit counters) from the ifXTable are as follows:

- ifHCInOctets
- ifHCInUcastPkts
- ifHCInMulticastPkts
- ifHCInBroadcastPkts
- ifHCOutOctets
- ifHCOutUcastPkts
- ifHCOutMulticastPkts

- ifHCOutBroadcastPkts

Monitor Utilization

This chapter describes how to monitor the system health information and port utilization on the GigaVUE H Series and GigaVUE TA Series nodes. It also provides commands to enable the system health threshold checks and set the buffer thresholds for port utilization. Refer to the following sections for details:

- View System Health Information
- Work with Port Utilization Measurements
- Configure Alarm Buffer Thresholds

View System Health Information

You can view the system health information for a specified node or for each node in a cluster by displaying the system health statistics. The system health statistics provide visibility into the CPU and memory usage, and the processes that are consuming the largest amount of CPU and memory resources in the node.

The **show system-health** command displays the CPU and memory utilization percentage for different time intervals, hence providing historical trends for CPU and memory utilization.

Optional SNMP notifications are triggered when the aggregate system CPU or memory usage exceeds the pre-defined threshold values.

Refer to the following sections for details:

- Display the System Health Statistics
- Enable the System Health Threshold Notification
- Configure the System Health Threshold

Display the System Health Statistics

Use the **show system-health** command to display the system CPU and memory statistics for all of the nodes in the cluster.

Use the **show system-health box-id <box id>** command to display the system CPU and memory statistics for a specified node in the cluster.

The CPU utilization statistics display the CPU load average over the last 1 minute, 5 minute, and 15 minute intervals. The CPU usage is displayed over the last 5 secs, 1 minute, and 5 minutes. 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.

The memory usage statistics display the total, used, and free amount of physical and swap memory available, as well as the memory usage for all the processes, with the process consuming the largest amount of memory displayed at the top.

Table 12: Statistics for CPU Utilization describes the statistics for CPU utilization:

Table 12: Statistics for CPU Utilization

Statistic	Description
CPU load average	Measure of CPU utilization during the time interval of 5 seconds, 1 minute, and 5 minutes. This measure indicates whether the CPU is over-utilized or under-utilized.
CPU usage	Percentage of time during which the CPU is processing the operating system and programs.
Core CPU (CPU1, CPU2, CPU3, and so on)	Percentage of time spent by the core CPUs running the user space processes (user), running the kernel (system), and being in idle state (idle).
Process	Programs running in the specified node or all of the nodes in the cluster. The CPU statistics for the processes displays the Process ID (PID) and CPU usage. The statistics can be sorted by CPU usage. The data is displayed for the time interval of 5 seconds, 1 minute, 5 minutes, and total (in milliseconds).

NOTE: When the node is restarted, the 5 seconds, 1 minute, 5 minute, and 15 minute statistics will not be exactly for the same intervals, until the full interval has elapsed and the history is available.

NOTE: When a new device is added to GigaVUE-FM, it takes one stats cycle for the above values to be reflected in the GigaVUE-FM GUI.

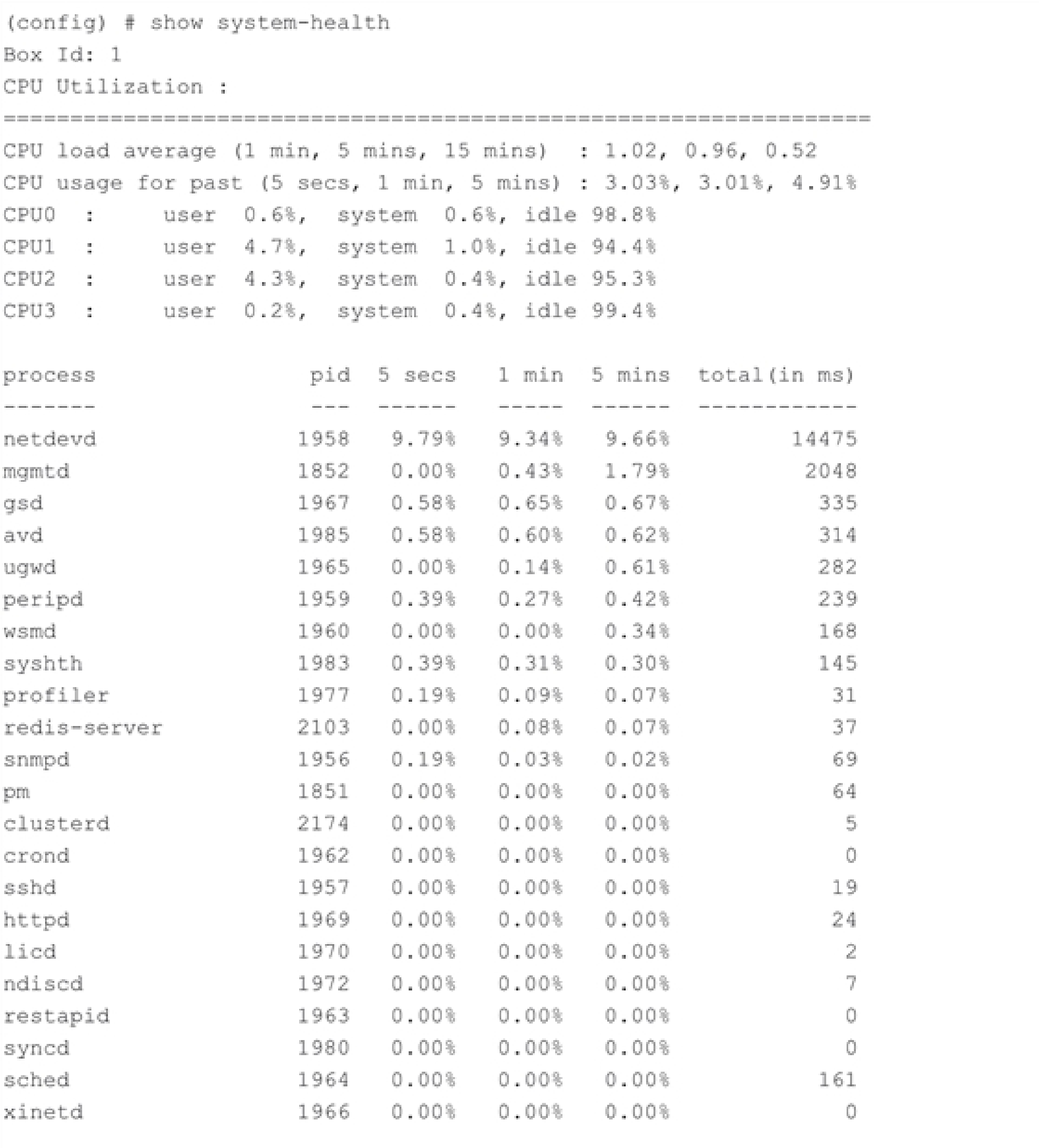
The following table describes the statistics for memory utilization:

Table 13: Statistics for Memory Utilization

Statistic	Description
Physical	Total, used, and free amount of physical memory consumed by the specified node or each node in the cluster.
Swap	Total, used, and free amount of swap memory consumed by the specified node or each node in the cluster.

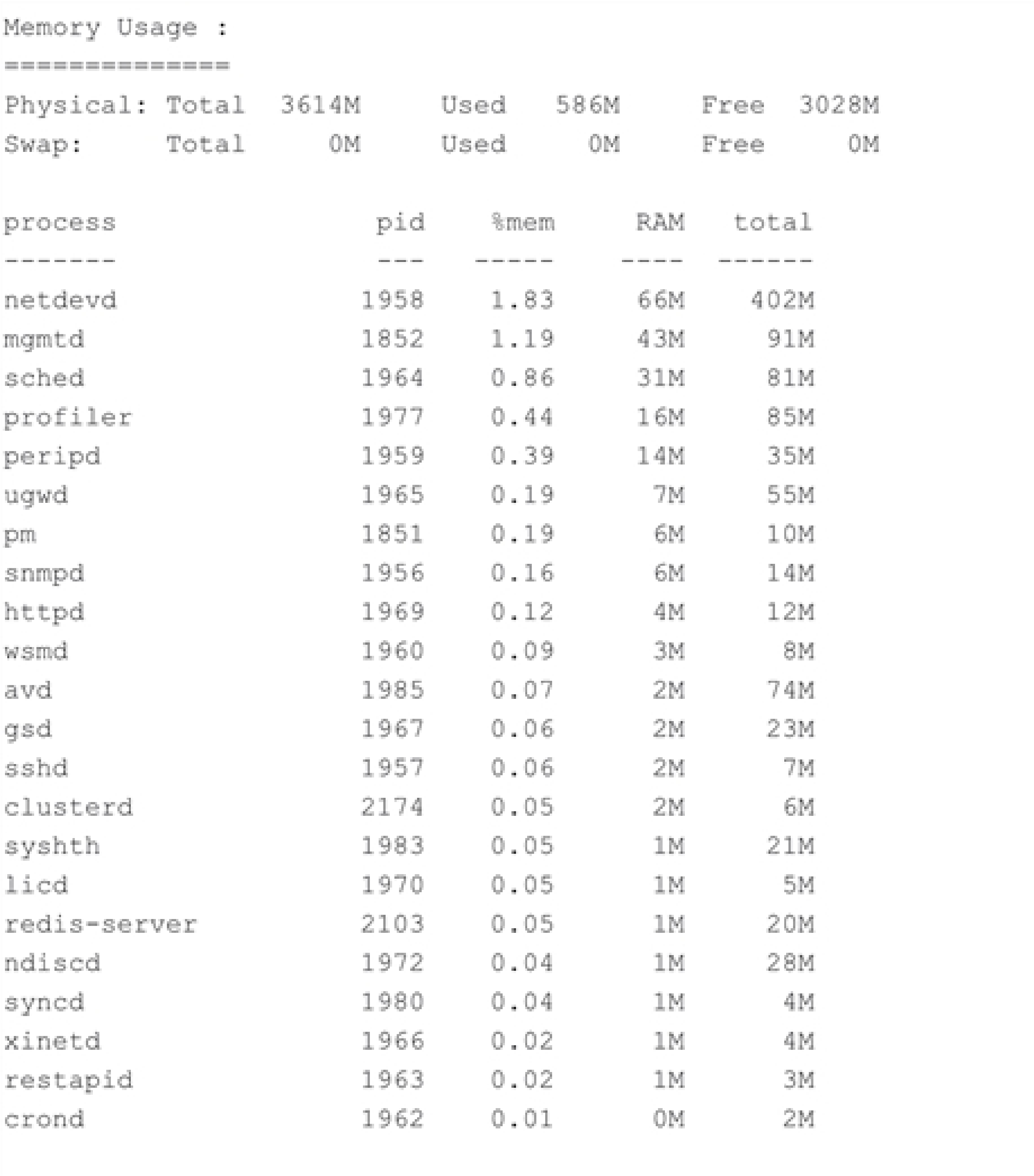
Statistic	Description
Process	Programs running in the specified node or all of the nodes in the cluster. The memory statistics for the processes displays process ID (PID), percentage of memory (%mem), RAM, and total memory used. The statistics can be sorted by %mem. The memory usage data is displayed in megabytes (Mb).

The following is an example of the **show system-health** command:



```
(config) # show system-health
Box Id: 1
CPU Utilization :
=================================================================
CPU load average (1 min, 5 mins, 15 mins)  : 1.02, 0.96, 0.52
CPU usage for past (5 secs, 1 min, 5 mins) : 3.03%, 3.01%, 4.91%
CPU0  :     user  0.6%,  system  0.6%, idle 98.8%
CPU1  :     user  4.7%,  system  1.0%, idle 94.4%
CPU2  :     user  4.3%,  system  0.4%, idle 95.3%
CPU3  :     user  0.2%,  system  0.4%, idle 99.4%

process                pid  5 secs   1 min  5 mins  total(in ms)
-------                ---  ------   -----  ------  ------------
netdevd               1958   9.79%   9.34%   9.66%         14475
mgmtd                 1852   0.00%   0.43%   1.79%          2048
gsd                   1967   0.58%   0.65%   0.67%           335
avd                   1985   0.58%   0.60%   0.62%           314
ugwd                  1965   0.00%   0.14%   0.61%           282
peripd                1959   0.39%   0.27%   0.42%           239
wsmd                  1960   0.00%   0.00%   0.34%           168
syshth                1983   0.39%   0.31%   0.30%           145
profiler              1977   0.19%   0.09%   0.07%            31
redis-server          2103   0.00%   0.08%   0.07%            37
snmpd                 1956   0.19%   0.03%   0.02%            69
pm                    1851   0.00%   0.00%   0.00%            64
clusterd              2174   0.00%   0.00%   0.00%             5
crond                 1962   0.00%   0.00%   0.00%             0
sshd                  1957   0.00%   0.00%   0.00%            19
httpd                 1969   0.00%   0.00%   0.00%            24
licd                  1970   0.00%   0.00%   0.00%             2
ndiscd                1972   0.00%   0.00%   0.00%             7
restapid              1963   0.00%   0.00%   0.00%             0
syncd                 1980   0.00%   0.00%   0.00%             0
sched                 1964   0.00%   0.00%   0.00%           161
xinetd                1966   0.00%   0.00%   0.00%             0
```



```
Memory Usage :
==============
Physical: Total  3614M     Used   586M     Free  3028M
Swap:     Total     0M     Used     0M     Free     0M

process                 pid    %mem     RAM   total
-------                 ---   -----    ----  ------
netdevd                1958    1.83     66M    402M
mgmtd                  1852    1.19     43M     91M
sched                  1964    0.86     31M     81M
profiler               1977    0.44     16M     85M
peripd                 1959    0.39     14M     35M
ugwd                   1965    0.19      7M     55M
pm                     1851    0.19      6M     10M
snmpd                  1956    0.16      6M     14M
httpd                  1969    0.12      4M     12M
wsmd                   1960    0.09      3M      8M
avd                    1985    0.07      2M     74M
gsd                    1967    0.06      2M     23M
sshd                   1957    0.06      2M      7M
clusterd               2174    0.05      2M      6M
syshth                 1983    0.05      1M     21M
licd                   1970    0.05      1M      5M
redis-server           2103    0.05      1M     20M
ndiscd                 1972    0.04      1M     28M
syncd                  1980    0.04      1M      4M
xinetd                 1966    0.02      1M      4M
restapid               1963    0.02      1M      3M
crond                  1962    0.01      0M      2M
```

Enable the System Health Threshold Notification

The system health thresholds are pre-defined. When the CPU and memory utilization crosses the pre-defined threshold values, SNMP events are generated.

For example, assuming the memory utilization threshold value for the process ‘netdevd’ is 1GB and the system health threshold is enabled, when the memory utilization for netdevd crosses 1GB, an SNMP trap can be generated.

These SNMP events help in troubleshooting. Collect this information and report it to Gigamon Technical Support. A Gigamon Technical Support personnel can use this information to resolve the CPU and memory utilization issues. Refer to Contact Technical Support on page 345.

Use the following command to enable the system health threshold for all the nodes in the cluster:

```
(config) # system-health threshold enable
```

You can also enable the system health threshold for a specified node. For example, if you want to enable the system health threshold for box ID 10, then use the following command:

```
config) # system-health box-id 10 threshold enable
```

Use the following command to disable the system health threshold:

```
(config) # no system-health threshold enable
```

Configure the System Health Threshold

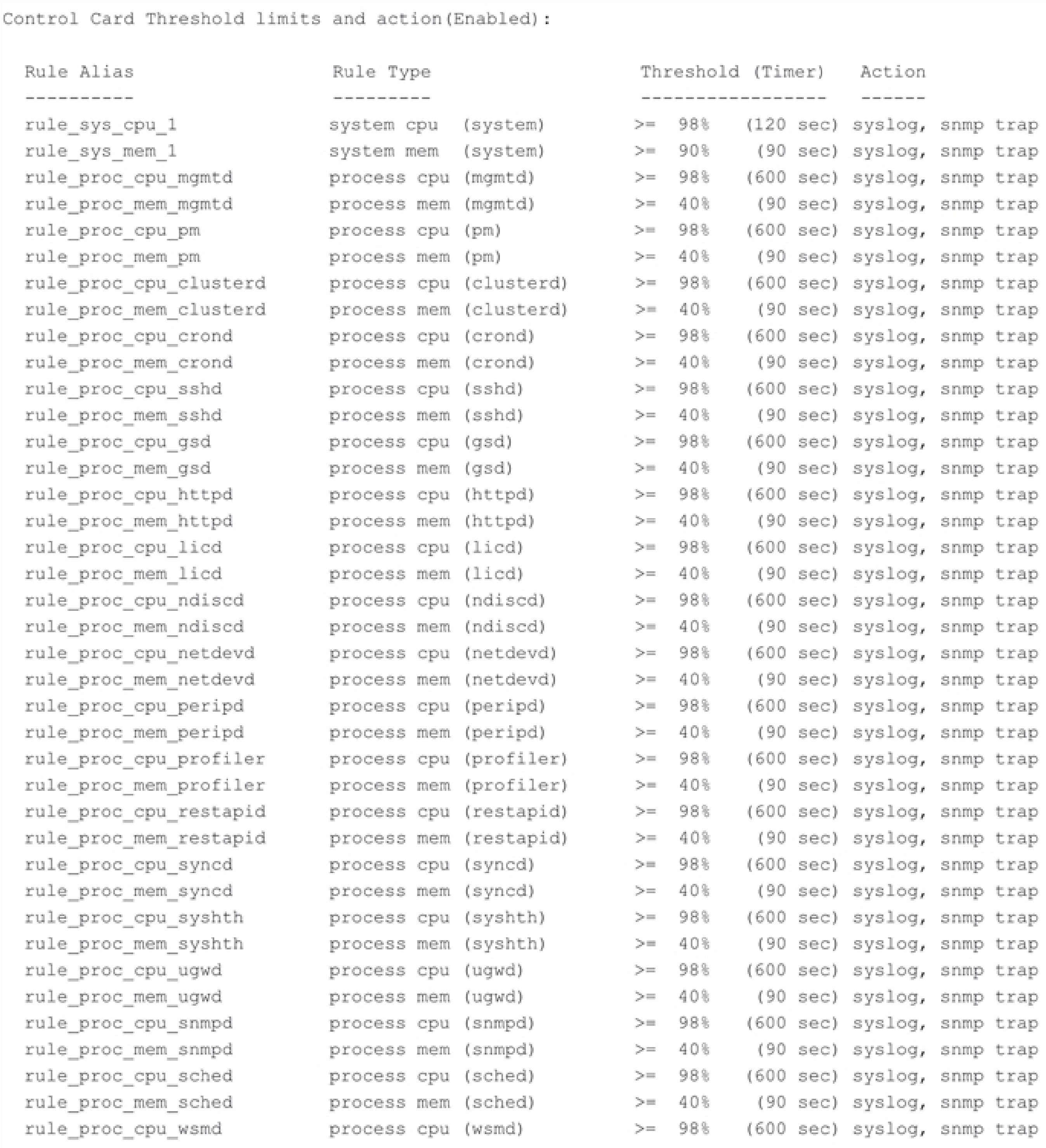
Use the following command to view the system health configuration:

```
(config) # show system-health config
```

Use the following command to view the system health configuration for a specified node:

```
(config) # show system-health config box-id <box id>
```

An example of the system health configuration is as follows:



```
Control Card Threshold limits and action(Enabled):

  Rule Alias                  Rule Type                    Threshold (Timer)   Action
  ----------                  ---------                    -----------------   ------
  rule_sys_cpu_1              system cpu  (system)         >=  98%   (120 sec) syslog, snmp trap
  rule_sys_mem_1              system mem  (system)         >=  90%    (90 sec) syslog, snmp trap
  rule_proc_cpu_mgmtd         process cpu (mgmtd)          >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_mgmtd         process mem (mgmtd)          >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_pm            process cpu (pm)             >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_pm            process mem (pm)             >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_clusterd      process cpu (clusterd)       >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_clusterd      process mem (clusterd)       >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_crond         process cpu (crond)          >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_crond         process mem (crond)          >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_sshd          process cpu (sshd)           >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_sshd          process mem (sshd)           >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_gsd           process cpu (gsd)            >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_gsd           process mem (gsd)            >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_httpd         process cpu (httpd)          >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_httpd         process mem (httpd)          >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_licd          process cpu (licd)           >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_licd          process mem (licd)           >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_ndiscd        process cpu (ndiscd)         >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_ndiscd        process mem (ndiscd)         >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_netdevd       process cpu (netdevd)        >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_netdevd       process mem (netdevd)        >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_peripd        process cpu (peripd)         >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_peripd        process mem (peripd)         >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_profiler      process cpu (profiler)       >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_profiler      process mem (profiler)       >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_restapid      process cpu (restapid)       >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_restapid      process mem (restapid)       >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_syncd         process cpu (syncd)          >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_syncd         process mem (syncd)          >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_syshth        process cpu (syshth)         >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_syshth        process mem (syshth)         >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_ugwd          process cpu (ugwd)           >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_ugwd          process mem (ugwd)           >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_snmpd         process cpu (snmpd)          >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_snmpd         process mem (snmpd)          >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_sched         process cpu (sched)          >=  98%   (600 sec) syslog, snmp trap
  rule_proc_mem_sched         process mem (sched)          >=  40%    (90 sec) syslog, snmp trap
  rule_proc_cpu_wsmd          process cpu (wsmd)           >=  98%   (600 sec) syslog, snmp trap
```

View the System Health Events

Use the following command to view the system health events:

(config) # show system-health status

Use the following command to view the system health events for a specified node:

```
(config) # show system-health status box-id <box id>
```

Enable System Health Events for SNMP Notifications

You may want to enable the system health related SNMP notification events to receive emails when the CPU or memory utilization exceeds the pre-configured threshold values.

Use the following commands to enable the system health related SNMP notification events:

```
(config) # snmp-server notify event process-cpu-threshold
(config) # snmp-server notify event process-mem-threshold
(config) # snmp-server notify event system-cpu-threshold
(config) # snmp-server notify event system-mem-threshold
```

For details on the **snmp-server notify event** command, refer to the *"snmp-server"* section in the *GigaVUE-OS CLI Reference Guide*.

View the System Health Diagnostics

Use the following command to view a detailed diagnostics of system health for troubleshooting:

```
(config) # show diag detail
```

The detail command displays diagnostic information about fabric statistics, system-health, and inline SSL statistics detail, in addition to the diagnostic information displayed in **show diag**.

An upload option on the **show diag detail** command lets you upload the output to a specified URL using HTTP, HTTPS, FTP, TFTP, SCP, SFTP

```
(config) # show diag detail upload <upload URL>
```

Work with Port Utilization Measurements

The GigaVUE H Series and GigaVUE TA Series nodes include the port utilization features summarized in the following table:

Feature	CLI Command
View Port Utilization Percentage You can view the percentage utilization measurement over the last second for one or more ports. Refer to View Port Utilization.	**show port utilization all** **box-id <box ID>** **port-list <port list>** **slot <slot ID>**
Configure Percentage Utilization You can configure the utilization percentage at which the GigaVUE H Series node will generate high or low utilization alarms for a port. Utilization alarms are forwarded as SNMP notifications to all SNMP notification destinations configured in the CLI. Refer to Configure Port Utilization Thresholds and Notifications.	**port <port list> alarm low-utilization-threshold <percentage>port <port list> alarm high-utilization-threshold <percentage>**

Port Utilization Availability by Port Type

You can view port utilization for all network, tool, hybrid, and stack link ports on the GigaVUE H Series or GigaVUE TA Series node.

View Port Utilization

Use the **show port utilization** command to view the percentage utilization measurement over the last second for one or more ports.

If you use the **show port utilization** command without any arguments, the last measured utilization values for all ports in the node (or cluster, if configured) are shown.

Format of show port utilization Output

The **show port utilization** command lists the utilization for all requested ports with the port number, port type, port speed, receive (rx) utilization percentage (network and stack ports), transmit (tx) utilization percentage (tool, hybrid, and stack ports), alarm threshold (high and low), and the last time the threshold was exceeded on either the transmit or receive direction.

The following table shows sample output for a **show port utilization port 13/1/x1** command.

			Utilization		Threshold		Last time threshold triggered	
Port	Type	Speed (Mb/s)	Tx	Rx	High	Low	Tx	Rx
13/1/x1	network	10000	-	3.25	70	30	-	-

Examples

The following commands provide some examples how to view port utilization in the CLI:

Command	Comments
show port utilization port-list 1/1/x1..x4	This command displays port utilization for ports 1/1/x1, 1/1/x2, 1/1/1/x3, and 1/1/x4.
show port utilization port-list streamdisk	This command displays port utilization for the port with the alias **streamdisk**.
show port utilization	This command displays port utilization for all ports in the node or cluster.

Port Utilization Thresholds

Use CLI commands to set the thresholds for high and low utilization alarms on a port. When a threshold is exceeded, the GigaVUE H Series node will write a utilization alarm to syslog and forward it to all configured SNMP notification destinations.

Argument	Description
port <port list>	Specifies the ports to which the percentage utilization threshold will be applied. Specify one of the following: **port-id <bid/sid/pid>port-alias <port-alias>port-list <bid/sid/pid_x..pid_y> (range) or <bid/sid/pid_x,bid/sid/pid_y,bid/sid/pid_z> (list)**
alarm high-utilization-threshold <0~100> alarm low-utilization-threshold <0~100>	Specifies the high and low utilization thresholds on a port, as a percentage. The thresholds specify the value at which the GigaVUE H Series node will log an alarm for the specified ports. By default, the thresholds are **0**, which means disabled.

> **NOTE:** Network ports always use an Rx threshold; tool ports always use Tx. Stack ports and hybrid ports use both Rx and Tx; the same threshold is used for each.

Utilization Alarm/SNMP Notification Generation

Utilization alarms are written to syslog and forwarded to all SNMP management stations configured as notification destinations. For SNMP notifications to be generated, forwarded, and displayed correctly in your SNMP management station, all of the following must be true:

Requirement	Description
SNMP Enabled	Use the **snmp-server enable** options to turn on the node's SNMP functionality and enable notifications.
SNMP Destinations Configured	Use the **snmp-server host** options in the CLI to specify the IP addresses for SNMP notification destinations.
SNMP Notifications Enabled for Utilization Alarms	Use the **portutilization** argument for the **snmp-server notify event** command to enable high utilization notifications. For example: **(config) # snmp-server notify event portutilization** Use the **lowportutilization** argument for the **snmp-server notify event** command to enable low utilization notifications. For example: **(config) # snmp-server notify event lowportutilization** Refer to Configure Port Utilization Thresholds and Notifications.
GigaVUE MIB Compiled at Management Station	You can obtain Gigamon's latest private MIB file by contacting **support@gigamon.com**.

Refer to Use SNMP for information on configuring the GigaVUE H Series node's SNMP features.

Configure Port Utilization Thresholds and Notifications

There are two port utilization alarms:

- lowportutilization—Utilization Alarm Low Status Change
- portutilization—Utilization Alarm High Status Change

Use the high utilization threshold to detect high port utilization. Use the low utilization threshold to detect low port utilization. Or use both thresholds.

When configuring the alarm utilization threshold values on ports, you cannot configure a low utilization threshold value that is greater than the current high utilization threshold value. For example, if you have configured low utilization threshold values as '40' and high utilization threshold value as '60', then you cannot change the low utilization threshold value to '70' and high utilization threshold values to '90' (because the new low utilization threshold value 70 is greater than the configured high utilization threshold high value which is 60). To configure these values, you must first reset the threshold values to '0' and then set the new values

The thresholds for these alarms are configured as a percentage using the **port** command as follows:

(config) # port 1/1/x1 alarm low-utilization-threshold 30(config) # port 1/1/x1 alarm high-utilization-threshold 70

To enable SNMP notifications when these thresholds are exceeded, use the **snmp-server** command as follows:

(config) # snmp-server notify event lowportutilization(config) # snmp-server notify event portutilization

An SNMP notification will be sent when a threshold is exceeded in any 5-second interval. A clear notification will be sent when the threshold is no longer exceeded. Clear notifications are sent for both rx and tx directions, for both porttutilization and lowporttutilization.

The thresholds can be disabled by setting them to zero, as follows:

(config) # port 1/1/x1 alarm low-utilization-threshold 0(config) # port 1/1/x1 alarm high-utilization-threshold 0

If a threshold has been exceeded, but is then disabled, a clear notification will be sent.

Examples:

- When the high utilization threshold is set to 70% and the traffic on the port rises above 70%, if the porttutilization alarm is enabled, it will be sent. If the traffic then falls below 70%, a clear notification (clearing the high threshold) will be sent.
- When the low utilization threshold is set to 30% and the traffic on the port falls below 30%, if the lowporttutilization alarm is enabled, it will be sent. If the traffic then rises above 30%, a clear notification (clearing the low threshold) will be sent. The lowporttutilization alarm will also be sent if there is no traffic or if the traffic is between 0 and 30%.
- When the high utilization threshold is set to 70% and the traffic on the port rises above 70%, if the porttutilization alarm is enabled, it will be sent. If the high utilization threshold is then disabled, a clear notification will be sent.

Configure Alarm Buffer Thresholds

Often network ports are utilized at rates below 50%. If several network ports are aggregated, there is a risk of oversubscribing the tool ports. Alarm buffer thresholds are used to monitor the congestion within the GigaVUE node caused by microbursts or by oversubscription of tool ports.

The buffer usage on any port remains at zero until the maximum line rate of the port is reached. When the usage crosses 100% either instantaneously, in the microburst case, or prolonged, in the oversubscription case, there is congestion.

The internal buffer on the GigaVUE node can absorb a certain number of packet bursts. During congestion, packets are buffered in the chassis and the buffer usage is reported on the corresponding ports and in the corresponding direction: rx (ingress) and tx (egress).

Reporting the buffer usage provides a trend of how the microbursts are causing congestion, so more tool ports can be added before packets are dropped. Buffer usage is measured in intervals of 5 seconds. The peak buffer usage within a 5-second interval is reported. Use the **show profile** commands to see trends of buffer usage over time.

When buffer usage is less than or equal to zero, there is no congestion, so no packets are dropped due to buffer unavailability.

When buffer usage is greater than zero, there is congestion. When buffer usage is greater than zero on any port in any direction, there is a chance that the packets (that caused the buffer usage to increase) are dropped due to unavailable buffers. However, it is unlikely to see packet drops due to buffer unavailability when the buffer usage on a port is less than 5%.

The buffer usage feature is supported on all ports and module types on the GigaVUE-HC3 and GigaVUE-HC2 (equipped with Control Card version 1 only).

Refer to the following sections for configuring buffer thresholds and for configuring a notification that can be sent when a threshold is exceeded:

- Set Alarm Buffer Thresholds
- Configuration Example
- Buffer Usage Alarm

Set Alarm Buffer Thresholds

Use the **card slot <slot id> alarm buffer-threshold** command to set an alarm buffer threshold on the slots of a GigaVUE node.

The card level threshold indicates usage levels of the node.

The following table describes the arguments:

Argument	Description
card slot <slot ID>	Specifies the slot.
alarm buffer-threshold <0-100%>	Sets the alarm buffer threshold for a slot, as a percentage. By default, the threshold is set to **0**, which disables the threshold. **NOTE:** On the GigaVUE-HC2 and GigaVUE-HC3, this command configures the same alarm buffer threshold on all the slots in the chassis.

The following are examples of configuring alarm buffer thresholds on slots:

Command	Comments
(config) # card slot 4/1 alarm buffer-threshold 30	Configures the alarm buffer threshold on box id 4 and slot 1.
(config) # no card slot 4/1 alarm buffer-threshold	Removes the alarm buffer threshold on box id 4 and slot 1.

Use the **port <port list> alarm buffer-threshold** command to set rx (ingress) and tx (egress) alarm buffer thresholds on a port.

The port level thresholds indicate usage levels of each port.

The following table describes the arguments:

Argument	Description
port <port list>	Specifies the ports to which the alarm buffer threshold is to be applied. Use one of the following formats for the port-list: **port-id <bid/sid/pid>port-alias <port-alias>port-list <bid/sid/pid_x..pid_y> (range) or <bid/sid/pid_x,bid/sid/pid_y,bid/sid/pid_z> (list)**
alarm buffer-threshold <0-100%> | rx <0-100%> | tx <0-100%>	Specifies the alarm buffer threshold on a port. You can specify the alarm buffer threshold in the rx and tx directions on network and stack type ports and in the tx direction on tool type ports. By default, the threshold is set to **0**, which disables the threshold.

For details on the CLI command, refer to the *"card"* and *"port"* sections in the *GigaVUE-OS CLI Reference Guide* .

Configuration Example

The following example configures two network ports, one tool port, and a passall map and configures alarm buffer thresholds on the ports.

Step	Description	Command
1.	Configure two network ports and a tool port.	**(config) # port 12/1/x5..x6 type network (config) # port 12/1/x2 type tool**
2.	Configure buffer thresholds on each port.	**(config) # port 12/1/x5 alarm buffer-threshold 30** **(config) # port 12/1/x6 alarm buffer-threshold 32** **(config) # port 12/1/x2 alarm buffer-threshold 35**

Step	Description	Command
3.	Create a passall map.	**(config) # map-passall alias bufExample(config map-passall alias bufExample) # from 12/1/x5..x6 (config map-passall alias bufExample) # to 12/1/x2(config map-passall alias bufExample) # exit(config) #**
4.	Display buffer statistics.	**(config) # show buffer port 12/1/x5,12/1/x6,12/1/x2 (config) # show profile current buffer(config) # show profile history buffer**

Use the following command to display the buffer statistics on the ports.

(config) # show buffer port 12/1/x5,12/1/x6,12/1/x2

```
  Port      Buffer Usage (%)  Last Time Exceeds Threshold             Buffer Alarm Threshold
  (%)
            RX        TX      RX                       TX                       RX
  TX
  ---------------------------------------------------------------------------------------------
  ---
  12/1/x5   41        N/A     2014/07/01 17:30:07.371  N/A                      30
  N/A12/1/x6   39        N/A     2014/07/01 17:30:07.378  N/A                      32
     N/A12/1/x2   N/A       37      N/A                      2014/07/01 17:30:07.384  N/A
        35
```

Use the following command to display the current buffers:

(config) # show profile current buffer all

```
        12/1/x2 counters    value---------------------------
                       RX:  0                 TX:  37         RX Config:  0          TX
      Config:  35Last Time Exceeding:  2014/07/01 17:30:07.384
        12/1/x5 counters    value---------------------------
                       RX:  41                TX:  0          RX Config:  30          TX
      Config:  0Last Time Exceeding:  0
        12/1/x6 counters    value---------------------------
                       RX:  39                TX:  0          RX Config:  32          TX
      Config:  0Last Time Exceeding:  0
```

Use the following command to display the last minute of buffer history for a specific port:

(config) # show profile history buffer 12/1/x5 min

```
      ===================================Port: 12/1/x5 minute history
      report=====================================
              Counter Name      0 sec ago     5 secs ago    10 secs ago    15 secs ago
      ============   ============   ============   ============   ===========
                       RX:             44             44             44             44
             TX:              0              0              0              0          RX
      Config:            30             30             30             30          TX Config:
                 0              0              0              0
              Counter Name    20 secs ago    25 secs ago    30 secs ago    35 secs ago
      ============   ============   ============   ============   ===========
                       RX:             44             44             44             44
             TX:              0              0              0              0           RX
      Config:            30             30             30             30          TX Config:
                 0              0              0              0
```

```
        Counter Name    40 secs ago    45 secs ago    50 secs ago    55 secs ago
============   ============   ============   ============   ===========
                 RX:             44             44             44             44
       TX:              0              0              0              0          RX
Config:             30             30             30             30          TX Config:
           0              0              0              0
```

Buffer Usage Alarm

When a buffer usage threshold has exceeded its configured percentage, a message is logged, and optionally, an SNMP notification is sent to all configured destinations.

Use the following command to configure the notification that is sent when the buffer usage has exceeded the configured threshold:

(config) # snmp-server notify event bufferoverusage

The SNMP notification will be sent when a threshold is exceeded in any 5-second interval. Once the notification is sent, there is a 30 second holdoff time before the notification is sent again.

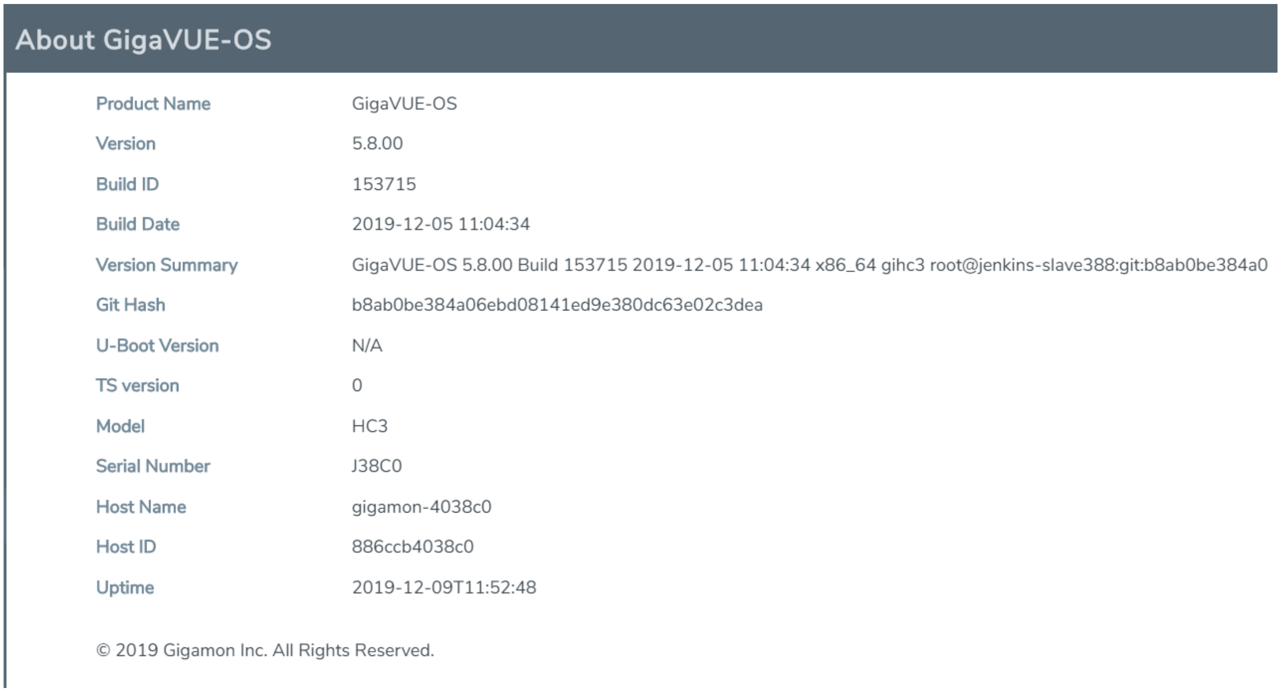
About

To view the About page (refer to the following figure):

1. On the left navigation pane, click on 🗄 and select **Physical**.
2. Click on a node listed in the page.
3. In the Node Overview page, select **About** (under support).

The **About** provides the following information:

- Product Name—The name of the product, GigaVUE-OS.
- Version—The current version running. For example, 4.8.00.
- Build ID and Build Date—information about when the current build was created.
- Version Summary—a detailed description of the currently installed version.
- Git Hash—additional build information.
- U-Boot Version—the currently installed u-boot version.
- CPLD Version—system information.
- TS Version—system information. This field displays information only when a timestamp card is inserted in the chassis.
- Model—the node model. For example, GigaVUE-HC2.
- Host Name—the host name assigned to the node. For information about setting the host name, refer to Configure the Host Name
- Uptime—the date that the current version was installed and the number of hours, minutes, and seconds that the node has been running.



About GigaVUE-OS

Product Name	GigaVUE-OS
Version	5.8.00
Build ID	153715
Build Date	2019-12-05 11:04:34
Version Summary	GigaVUE-OS 5.8.00 Build 153715 2019-12-05 11:04:34 x86_64 gihc3 root@jenkins-slave388:git:b8ab0be384a0
Git Hash	b8ab0be384a06ebd08141ed9e380dc63e02c3dea
U-Boot Version	N/A
TS version	0
Model	HC3
Serial Number	J38C0
Host Name	gigamon-4038c0
Host ID	886ccb4038c0
Uptime	2019-12-09T11:52:48

© 2019 Gigamon Inc. All Rights Reserved.

Figure 36 *About Page*

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:

- One numerical character
- One upper case character
- One lower case character
- One special character

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

Users of GigaVUE Fabric Manager have access to the Linux shell of GigaVUE-FM. Log in to GigaVUE-FM through SSH and you will land on the command line prompt. With this access, you can troubleshoot issues and perform certain operations. Refer to the following sections for details:

- GigaVUE-FM CLI Commands
- Post Installation Configurations
- Post Installation Configurations (Refer to GigaVUE-FM Installation and Upgrade Guide)

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 to install such additional software.

Important: Installing Third-party software in GigaVUE-FM can have harmful effects on the operation of GigaVUE-FM. Uninstall all third-party software prior to contacting Gigamon Support for troubleshooting.

GigaVUE-FM CLI Commands

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
    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

      jump-start
      logging [<fqdn>[:<port>]] [facility <facility>] [priority <priority>] [udp|tcp|tls]
      no logging <fqdn>[:<port>]
      reset factory halt
      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|[enable] <server1>[,<server2>[,...]}
          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>
```

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: **fmctl configuration backup <absolute path name of backup file>** Use the following command to restore the system configurations from the backup: **fmctl 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: **fmctl image fetch ftp://robh:xray@192.168.1.10/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**: **fmctl image fetch scp://bbochy:catch1@192.168.1.75:/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: **fmctl 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: **fmctl 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: **fmctl image install gigamon-gigavue-fm-**

Argument	Description
	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: **fmctl image boot next** Use the folloaing command to boot the image file on the specified partition: **fmctl image boot location 1** **NOTE:** GigaVUE-FM reboots immediately.
image delete [force] <filename>	Deletes the named image file. For example: **fmctl 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: **fmctl image rename myimage newimage**
image show	Displays the last boot partition. For example: **fmctl image show**
jump-start	Runs the configuration wizard for the initial setup of GigaVUE-FM. Refer to Perform Initial Configuration. **NOTE:** When you change the IP address of the GigaVUE-FM instance using the jump-start configuration, the internal database and the in-memory caches of the GigaVUE-FM instance are not updated. The Database continues to have the IP address of the old GigaVUE-FM, and the image upgrade using the internal server option does not work. To fix this, you must restart the GigaVUE-FM instance after upgrade.
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: **fmctl logging 1.2.3.4:9514 facility * priority debug tcp**

Argument	Description
	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.
no logging <fqdn>[:<port>]	Removes the logging server configuration. For example: **fmctl no logging 1.2.3.4:9514**
reset factory halt	Resets the GigaVUE-FM instance to the default configuration and shuts down the system. For example: **fmctl reset factory halt**
set UI admin password <new password>	Configures a new admin password for the GigaVUE-FM UI only. 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-FMinstance. For example: **fmctl 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: **fmctl 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: **fmctl --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: **fmctl --interface eth1 set mapping fm 10.10.10.1** Use the following command to remove the mapping: **fmctl --interface eth1 set mapping fm**

Argument	Description

[options{--help|--interface <interface name>}] {get|show} {ip|ntp|hostname|domain|fqdn}	Use to either fetch or display the IP address, NTP configurations, host name, domain name, or FQDN .
	For example:
	fmctl --interface eth1 get {ip|ntp|hostname|domain|fqdn}
	fmctl --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: **fmctl --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: **fmctl --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|[enable] <server1> [,<server2>[,...]}	Use to enable or disable NTP for synchronization of the system's clock. For example, the following command disables NTP: **fmctl --interface eth1 set ntp disable** You choose to enable NTP and add NTP servers. For example, the following command enables NTP and adds a NTP server: **fmctl --interface eth1 set ntp enable 192.168.1.10**
[options{--help|--interface <interface name>}] set hostname <hostname>	Configures the hostname. For example: **fmctl --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: **fmctl --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. **fmctl --interface eth1 set fqdn myfm gigamon.com**

Argument	Description
[options{--help|--interface <interface name>}] set/get/show searchdomains [<domain1>[,<domain2>[,...]]]	Displays a list of domains for the current GigaVUE-FM For example: **fmctl --interface eth1 set searchdomains** **fmctl --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: **fmctl --interface eth1 set nameservers** **fmctl --help get | show nameservers**
[options{--help|--interface <interface name>}] show backup	Displays the configurations that were backed up. For example: **fmctl --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. **fmctl --unlock UI <username>**

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
gigamonSnmpTapRelayChangeNotificatio	.1.3.6.1.4.1.2	TrapTapRelayChange	N/A	N/A

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
n	6866.1.1.7			
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
gigamonSnmpOverThresholdChangeNotification	.1.3.6.1.4.1.26866.1.1.12	TrapOverThreshold	N/A	N/A
gigamonSnmpBatterryLevelChangeNotification	.1.3.6.1.4.1.26866.1.1.13	TrapBatteryLevelChange	FM Alarm support currently not available	N/A
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

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
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
gigamonSnmpCPUTemperatureNotification	.1.3.6.1.4.1.26866.1.1.30	TrapCpuTemperature	DeviceCpu Temperature Unhealthy	Device CPU Temperature Unhealthy
gigamonSnmpSecondaryFlashBootNotification	.1.3.6.1.4.1.26866.1.1.31	TrapSecondaryFlashBoot	N/A	N/A
gigamonSnmpOperationalModeNotificati	.1.3.6.1.4.1.2	TrapOperationalModeChangeTr	N/A	N/A

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
on	6866.1.1.32	apOperationalModeChanged		
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	.1.3.6.1.4.1.26866.1.1.42	TrapTunnelGwStatus	Tunnel Port Unhealthy	Tunnel Port Unhealthy
gigaSmartTunnelDestStatus	.1.3.6.1.4.1.26866.1.1.43	TrapTunnelDestIpStatus	Tunnel Port Unhealt	Tunnel Port Unheal

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
			hy	thy
gigamonSnmpIpGwStatusNotification	.1.3.6.1.4.1.26866.1.1.44	TrapIpGwStatusUpdate	IP Interface Unhealthy	IP Interface Unhealthy
gigamonSnmpTrapThrottleReport	.1.3.6.1.4.1.26866.1.1.45	TrapThrottleReport	N/A	N/A
gigamonSnmpClusterRoleChangeNotification	.1.3.6.1.4.1.26866.1.1.46	TrapClusterRoleChange	N/A	N/A
gigamonSnmpClusterNodeJoinNotification	.1.3.6.1.4.1.26866.1.1.47	TrapClusterNodeJoin	N/A	N/A
gigamonSnmpClusterNodeLeaveNotification	.1.3.6.1.4.1.26866.1.1.48	TrapClusterNodeLeave	N/A	N/A
gigamonSnmpClusterNodeJoinFailNotification	.1.3.6.1.4.1.26866.1.1.49	TrapClusterNodeJoinFail	N/A	N/A
gigamonSnmpVportStateChangeNotification	.1.3.6.1.4.1.26866.1.1.50	TrapVportStatusChange	Virtual Port Unhealthy	Virtual Port Unhealthy
gigamonSnmpTrapIsslResource	.1.3.6.1.4.1.26866.1.1.51	TrapGSIsslResourceUtilization	N/A	N/A
gigamonSnmpGigaSMARTCPUTemperatureNotification	.1.3.6.1.4.1.26866.1.1.52	TrapGigaSMARTCpuTemperature	N/A	N/A
gigamonSnmpLicenseExpireNotification	.1.3.6.1.4.1.26866.1.1.53	TrapLicenseExpirationReminder	N/A	N/A
gigamonSnmpBatteryPresenceNotification	.1.3.6.1.4.1.26866.1.1.54	TrapBatteryPresence	N/A	N/A
gigamonSnmpBatteryTestNotification	.1.3.6.1.4.1.26866.1.1.55	BatteryTestStatusNotifWrapper	N/A	N/A
gigamonSnmpBatteryTemperatureNotification	.1.3.6.1.4.1.26866.1.1.56		FM Alarm support currently not availabl	N/A

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
			e	
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	TrapSFPCompatability	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
gigamonSnmpNearCpuTemperatureNotification	.1.3.6.1.4.1.26866.1.1.68	TrapNearCpuTemp	N/A	N/A
gigamonSnmpBcmSocTemperatureNotifi	.1.3.6.1.4.1.2	TrapBcmSocTemp	N/A	N/A

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
cation	6866.1.1.69			
gigamonSnmpCpuSocTemperatureNotification	.1.3.6.1.4.1.2 6866.1.1.70	TrapCpuSocTemp	N/A	N/A
gigamonSnmpCpuHibernationStatusNotification	.1.3.6.1.4.1.2 6866.1.1.71	TrapCPUHibernation	N/A	N/A
gigaSmartNetFlowResourceAllocationFailed	.1.3.6.1.4.1.2 6866.1.1.72	TrapNetflowResourceAllocation Failed	N/A	N/A
gigamonSnmpSysdumpStatusNotification	.1.3.6.1.4.1.2 6866.1.1.73	TrapSysdumpGeneration	N/A	N/A
gigamonSnmpInlineToolHbStatusChangeNotification	.1.3.6.1.4.1.2 6866.1.1.74	TrapInlineToolHbChange	Inline Tool Unhealthy	N/A
gigamonSnmpInlineToolOperStatusChangeNotification	.1.3.6.1.4.1.2 6866.1.1.75	InlineToolStateChange	Inline Tool Unhealthy	N/A
gigamonSnmpInlineToolGroupOperStatusChangeNotification	.1.3.6.1.4.1.2 6866.1.1.76	InlineToolGroupStateChange	Inline Tool Group Unhealthy	N/A
gigamonSnmpInlineNetForwardingStatusChangeNotification	.1.3.6.1.4.1.2 6866.1.1.77	InlineNetworkStateChange	Inline Network Unhealthy	N/A
gigamonSnmpInlineNetLagForwardingStatusChangeNotification	.1.3.6.1.4.1.2 6866.1.1.78	InlineNetworkLagStateChange	Inline Network Lag Unhealthy	N/A
gigamonSnmpGsAppCoreCrashNotification	.1.3.6.1.4.1.2 6866.1.1.79	GsAppCoreCrash	N/A	N/A
gigamonSnmpGsDumpStatusNoti	.1.3.6.1.4.1.2 6866.1.1.80	TrapGsDumpStatus	N/A	N/A

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
fication				
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
gigamonSnmpSwitchBoard2TemperatureNotification	.1.3.6.1.4.1.26866.1.1.84	TrapSwitchBoard2Temperature	Switch Board 2 Temperature Unhealthy	N/A

SNMP Traps	Object Identifier (MIB)	GigaVUE-FM Event	GigaVUE-FM Alarm	Link to Corrective Actions for Alarms
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
gigamonPowerSupplyHardwareMismatchNotification	.1.3.6.1.4.1.26866.1.1.87	TrapPowerSupplyHardwareMismatch	N/A	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
VmmVcenterAdded	vCenter Added
VmmVcenterDeleted	vCenter Deleted
VmmVcenterConnectionStateChanged	vCenter Connection State Changed
VmmVcenterConnected	vCenter Connected
VmmVcenterDisconnected	vCenter Disconnected
VmmVcenterInventoryCompleted	vCenter Inventory Completed
VmmVmPoweredOn	VM powered on
VmmVmPoweredOff	VM powered off
VmmHostPoweredOn	Host powered on
VmmHostPoweredOff	Host powered off
VmmHostAdded	Host added
VmmHostRemoved	Host removed
VmmHostMultiGvm	Host has Multiple Gvms
VmmHostNetworkConfiged	Host Network reconfiged
VMMHostMoveInCluster	Host Moved In Cluster
VmmVmDisconnected	VM disconnected
VmmVmConnected	VM connected
VmmVmRemoved	VM removed
VmmVmCreated	VM created

GigaVUE-FM Event	Description
VmmVmRenamed	VM renamed
VmmVmResetting	VM resetting
VmmVmSuspended	VM suspended
VmmVmGuestShutdown	VM Guest shutdown
VmmVmGuestReboot	VM Guest rebooted
VmmVmStartMigrating	vMotion started
VmmVmMigrated	vMotion completed
VmmPortAdded	vNIC added
VmmPortEdited	vNIC configuration changed
VmmPortRemoved	vNIC removed
VmmDvsPortLinkDown	DVS Port Link Down
VmmDvsPortLinkUp	DVS Port Link Up
VmmGvmNoIp	GigaVUE-VM does not have an IP
VmmGvmPinToHost	GigaVUE-VM pinned to host
VmmGvmUnPinFromHost	GigaVUE-VM unpinned from host
VmmError	Vmm error
OpenStackConnectionStateChanged	Openstack Connection State Changed
OpenStackInventoryUpdateStarted	OpenStack Inventory Update Started
OpenStackInventoryUpdateCompleted	OpenStack Inventory Update Completed
OpenStackInstanceInventoryUpdateFailed	OpenStack Instance Inventory Update Failed
deviceHealthChanged	OpenStack Fabric Deployment Inventory Update Failed
OpenStackConnectionTriggeredInventoryUpdateStarted	OpenStack Connection Triggered Inventory

GigaVUE-FM Event	Description
	Update Started
OpenStackConnectionTriggeredInventoryUpdateCompleted	OpenStack Connection Triggered Inventory Update Completed
OpenStackConnectionTriggeredInventoryUpdateFailed	OpenStack Connection Triggered Inventory Update Failed
OpenStackProjectLimitExceeded	OpenStack Project Limit Exceeded
VmmGvTapControllerInstallStarted	G-vTAP Controller VM install started
VmmGvTapControllerInstallComplete	G-vTAP Controller VM install completed
VmmGvTapControllerCameOnline	G-vTAP Controller VM came online
VmmGvTapControllerInstallFailed	G-vTAP Controller VM Install Failed
VmmVSeriesControllerInstallStarted	V Series Controller VM install started
VmmVSeriesControllerInstallComplete	V Series Controller VM install completed
VmmVSeriesControllerInstallFailed	V Series Controller VM install failed
VmmVSeriesNodeInstallStarted	V Series Node VM install started
VmmVSeriesNodeInstallFailed	V Series Node VM install failed
VmmVSeriesNodeInstallComplete	V Series Node VM install completed
VmmGvTapControllerUpgradeStarted	G-vTAP Controller upgrade started
VmmGvTapControllerUpgradeComplete	G-vTAP Controller upgrade completed
VmmGvTapControllerUpgradeFailed	G-vTAP Controller

GigaVUE-FM Event	Description
	upgrade failed
VmmVSeriesControllerUpgradeStarted	V Series Controller upgrade started
VmmVSeriesControllerUpgradeComplete	V Series Controller upgrade completed
VmmVSeriesControllerUpgradeFailed	V Series Controller upgrade failed
VmmVSeriesNodeUpgradeStarted	V Series Node upgrade started
VmmVSeriesNodeUpgradeFailed	V Series Node upgrade failed
VmmVSeriesNodeUpgradeComplete	V Series Node upgrade completed
VmmNsxvAgentUpdated	NSX-V Agent Created/Updated
VmmNsxvAgentDeleted	NSX-V Agent Deleted
VmmNsxvProfileUpdated	NSX-V Profile Created/Updated
VmmNsxvProfileDeleted	NSX-V Profile Deleted
VmmNsxvServiceInstanceCreated	NSX-V Service Instance Created
VmmNsxvServiceInstanceDeleted	NSX-V Service Instance Deleted
NsxtLicenseExpire	VMware NSX-T License Has Expired
AwsConnectionStateChanged	AWS Connection Status Changed
AwsInventoryUpdateStarted	AWS Inventory Update Started
AwsInventoryUpdateCompleted	AWS Inventory Update Completed
AwsInstanceInventoryUpdateFailed	AWS Instance Inventory Update Failed
AwsConnectionTriggeredInventoryUpdateStarted	Aws Connection Triggered

GigaVUE-FM Event	Description
	Inventory Update Started
AwsConnectionTriggeredInventoryUpdateCompleted	Aws Connection Triggered Inventory Update Completed
AwsConnectionTriggeredInventoryUpdateFailed	Aws Connection Triggered Inventory Update Failed
AwsFabricDeploymentInventoryUpdateFailed	AWS Fabric Deployment Inventory Update Failed
AwsLicenseExpire	AWS License Has Expired
AzureConnectionStateChanged	Azure Connection Status Changed
AzureInventoryUpdateStarted	Azure Inventory Update Started
AzureInventoryUpdateCompleted	Azure Inventory Update Completed
AzureVMInventoryUpdateFailed	Azure VM Inventory Update Failed
AzureFabricDeploymentInventoryUpdateFailed	Azure Fabric Deployment Inventory Update Failed
AzureLicenseExpire	Azure License Has Expired
AzureConnResGrpLimitExceeded	Azure Connection Resource Group Limit Exceeded
AzureConnectionTriggeredInventoryUpdateStarted	Azure Connection Triggered Inventory Update Started
AzureConnectionTriggeredInventoryUpdateCompleted	Azure Connection Triggered Inventory Update Completed
AzureConnectionTriggeredInventoryUpdateFailed	Azure Connection Triggered Inventory Update Failed
AnyCloudInventoryUpdateStarted	AnyCloud Inventory Update started

GigaVUE-FM Event	Description
AnyCloudInventoryUpdateCompleted	AnyCloud Inventory Update Completed
KubernetesConnectionStateChanged	Kubernetes Connection Status Changed
KubernetesConnTriggeredInvUpdateStarted	Kubernetes Connection Triggered Inventory Update Started
KubernetesConnTriggeredInvUpdateCompleted	Kubernetes Connection Triggered Inventory Update Completed
KubernetesConnTriggeredInvUpdateFailed	Kubernetes Connection Triggered Inventory Update Failed
NutanixConnectionStateChanged	Nutanix Connection Status Changed
NutanixConnTriggeredInvUpdateStarted	Nutanix Connection Triggered Inventory Update Started
NutanixConnTriggeredInvUpdateCompleted	Nutanix Connection Triggered Inventory Update Completed
NutanixConnTriggeredInvUpdateFailed	Nutanix Connection Triggered Inventory Update Failed
NutanixInventoryUpdateStarted	Nutanix Inventory Update started
NutanixInventoryUpdateCompleted	Nutanix Inventory Update Completed
VcenterConnectionStateChanged	vCenter Connection Status Changed
VmwareConnectionTriggeredInventoryUpdateCompleted	VMware Connection Triggered Inventory Update Completed
VmwareConnectionTriggeredInventoryUpdateFailed	VMware Connection Triggered Inventory

GigaVUE-FM Event	Description
	Update Failed
VmwareInventoryUpdateCompleted	VMware Inventory Update Completed
VmwareVmInventoryUpdateFailed	VMware VM Inventory Update Failed
VmwareFabricDeploymentInventoryUpdateFailed	VMware Fabric Deployment Inventory Update Failed
VmwareVmPinToHost	GigaVUE-VM pinned to host
VmwareVmUnPinFromHost	GigaVUE-VM unpinned from host
VmwareNsxtNodeDeploymentStarted	VMWare NSX-T Node Deployment started
VmwareNsxtNodeDeploymentSuccess	VMWare NSX-T Node Deployment successful
VmwareNsxtNodeDeploymentFailed	VMWare NSX-T Node Deployment failed
VmwareNsxtNodeDeploymentCompleted	VMWare NSX-T Node Deployment completed
VmwareNsxtNodeUndeploymentStarted	VMWare NSX-T Node Undeployment started
VmwareNsxtNodeUndeploymentSuccess	VMWare NSX-T Node Undeployment successful
VmwareNsxtNodeUndeploymentFailed	VMWare NSX-T Node Undeployment failed
VmwareNsxtNodeUndeploymentCompleted	VMWare NSX-T Node Undeployment completed
GvtapAgentInventoryUpdateCompleted	G-vTAP Agent Inventory Update Completed
NoCompatibleGvtapController	No compatible G-vTAP controller exists for G-vTAP Agent version
GcbRegistered	GCB Registered

GigaVUE-FM Event	Description
GcbDeregistered	GCB Deregistered
InstanceRunning	VM Instance Running
InstanceStopped	VM Instance Stopped
InstanceTerminated	VM Instance Terminated

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

GigaVUE-FM Event	Description
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
DeviceRebootStarted	Device reboot started
DeviceConfigBackedUp	Device configuration backup
DeviceConfigDeleted	Device configuration deleted
DeviceConfigRestored	Device configuration restore
ApplyDeviceConfig	Apply device configuration
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
GigaVUE-FM Event Name	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
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

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

Inline Bypass Solution

The following table lists the events related to Inline Bypass solution.

GigaVUE-FM Event	Description
InlineToolStateChange	Inline Tool State Change
InlineToolGroupStateChange	Inline Tool Group State Change
InlineNetworkStateChange	Inline Network State Change
InlineNetworkLagStateChange	Inline Network Lag State Change
InlineStateChange	Inline State Change

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
LicensesinGrace (applicable for floating and node-locked licenses)	Licenses in grace period (licenses for which grace period is applicable)
LicensesExpired (applicable for floating and node-locked licenses)	Licenses expired
VolumeUsageAlertThresholdExceeded	Volume Usage alert threshold exceeded
VolumeUsageReportEmailSendFailed	Volume Usage report email send failed

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
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 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

Manage 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 a not-reachable member node rejoins the cluster after it comes online.
ClusterMemberNotReachable	This event is triggered when a node in a cluster is not-reachable.

GigaVUE-FM Events

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	Description
gigamonFMServerConfigBackupCompletionStatusNotification	.1.3.6.1.4.1.26866.6.1.1	FMServerConfigBackupCompletionStatus	GigaVUE-FM sends a notification to the external servers whenever the server backup configuration operation is completed.
gigamonFMServerConfigRestoreCompletionStatusNotification	.1.3.6.1.4.1.26866.6.1.2	ServerConfigRestoreCompletionStatus	GigaVUE-FM sends a notification to the external servers when the server restoration is complete.
gigamonFMImageUpgradeStartedNotification	.1.3.6.1.4.1.26866.6.1.3	ImageUpgradeStarted	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	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	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	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	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	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	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-FMs license is about to expire in 15 days.
gigamonFMLicensesExpiredNotification	.1.3.6.1.4.1.26866.6.1.10	LicensesExpired	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	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	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	GigaVUE-FM sends a notification 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	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 allowance of the base bundle as well as the add-on packages volume allowance.
gigamonFMVolumeUsageReportEmailSendFailedNotification	.1.3.6.1.4.1.26866.6.1.15	VolumeUsageReportEmailSendFailed	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	GigaVUE-FM sends a notification to the external server when any unexpected error occurs while computing the flow.
igamonFMSFlowHealthStateChangedNotification	.1.3.6.1.4.1.26866.6.1.17	FlowHealthStateChanged	GigaVUE-FM sends a

			notification to the external server whenever there is a change in the health status.
gigamonFMSyslogOverThresholdNotification	.1.3.6.1.4.1.26866.6.1.18	SyslogOverThreshold	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: 1. For 16GB- 100 logs per minute 2. For 32GB- 1000 logs per minute

			3. For more than 32GB-5000 logs per minute
gigamonFMHighAvailabilityNotification	.1.3.6.1.4.1.26866.6.1.23	HighAvailability	GigaVUE-FM sends a notification to the external servers when a state change happens in GigaVUE-FM High availability.
gigamonFMDiskReclaimEventNotification	.1.3.6.1.4.1.26866.6.1.24	DiskReclaimEvent	GigaVUE-FM sends a notification to the external servers when configuration directory occupies more than 70% of the memory.

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's link is down.
- The port's traffic is unhealthy based on the configured parameters.

Corrective Action

1. Check whether the connections are enabled at the port.
2. Check the port's hardware status.
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

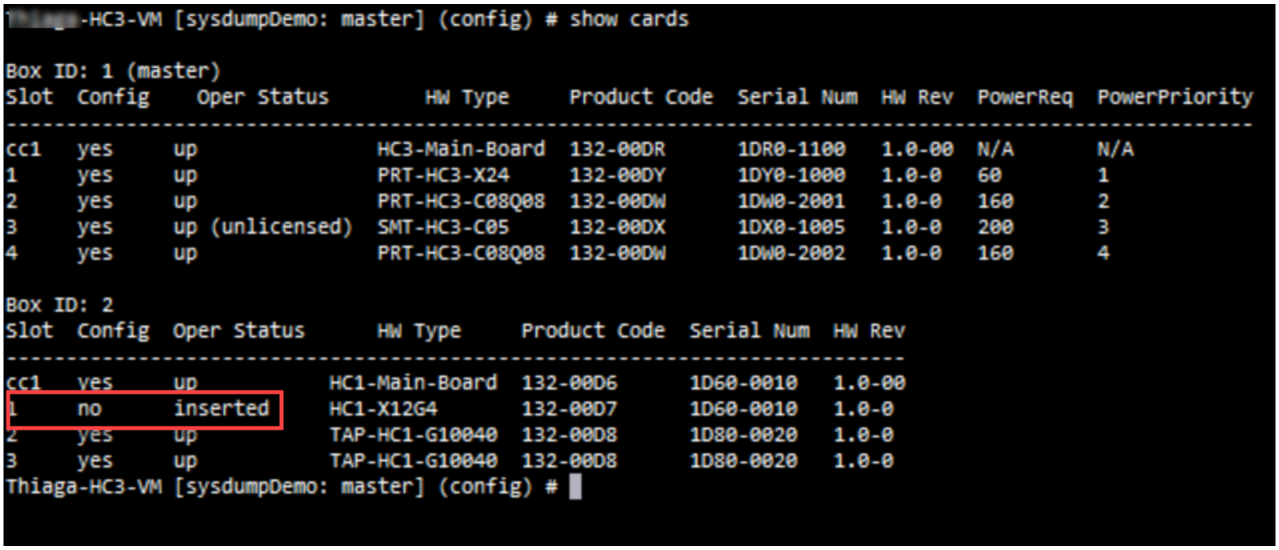
This alarm is generated due to various reasons. Most common scenarios are:

- 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.

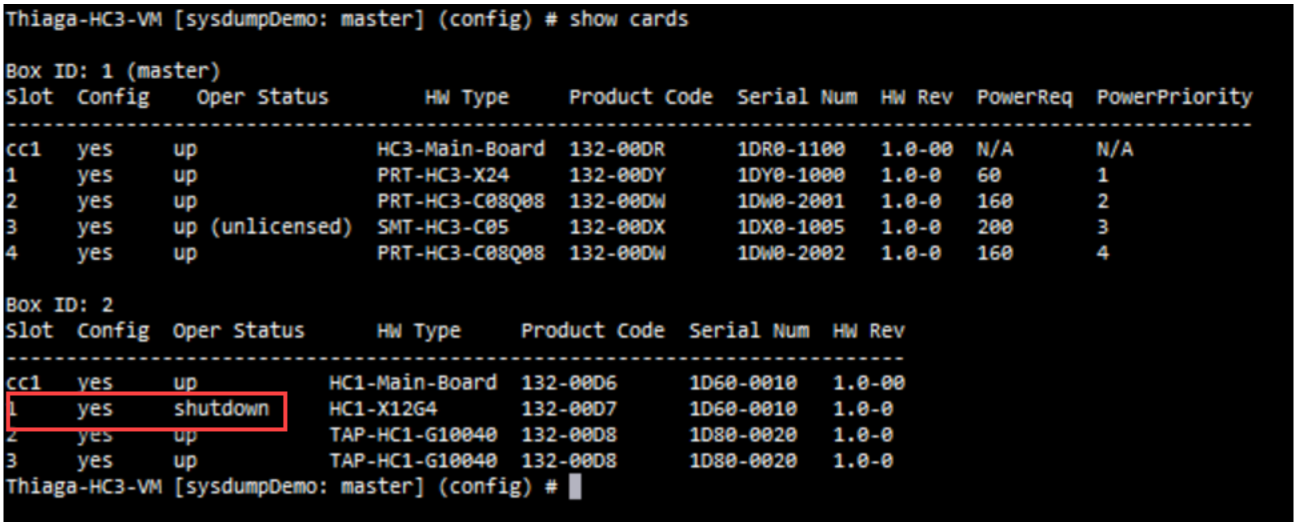


```
[redacted]-HC3-VM [sysdumpDemo: master] (config) # show cards

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
Thiaga-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.



```
Thiaga-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
Thiaga-HC3-VM [sysdumpDemo: master] (config) #
```

Abnormal Fan Operation

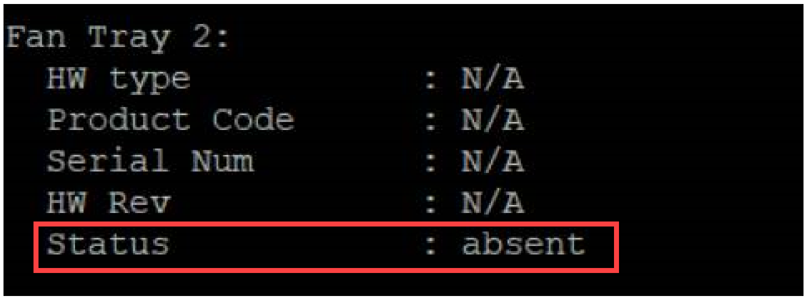
Description

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

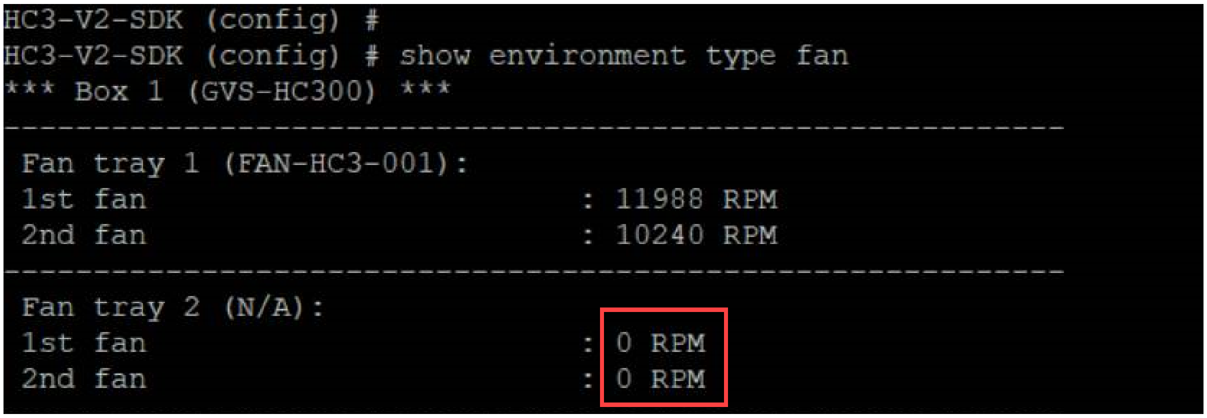
Perform the following tasks to troubleshoot this issue:

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.

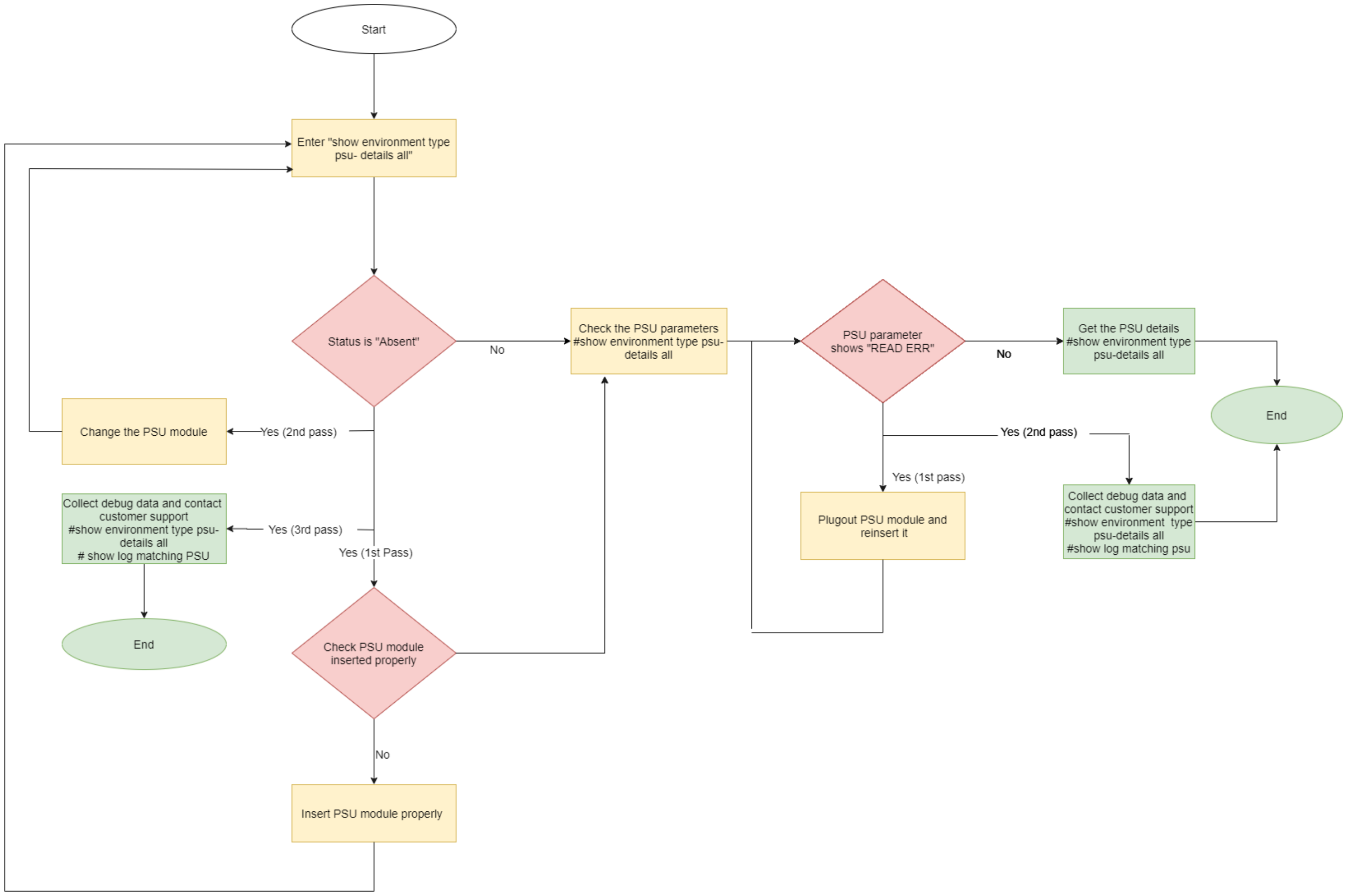
Faulty Power Module

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.


Start
Enter "show environment type psu- details all"
Status is "Absent"
No
Check the PSU parameters #show environment type psu-details all
PSU parameter shows "READ ERR"
No
Get the PSU details #show environment type psu-details all
End
Yes (2nd pass)
Yes (1st pass)
Plugout PSU module and reinsert it
Collect debug data and contact customer support #show environment type psu-details all #show log matching psu
Change the PSU module
Yes (2nd pass)
Collect debug data and contact customer support #show environment type psu-details all # show log matching PSU
Yes (3rd pass)
Yes (1st Pass)
End
Check PSU module inserted properly
No
Insert PSU module properly

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 IfInPktDrops. 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 gsgrp command to determine the GigaSMART group to which the GSOP is associated with.
2. Refer to Gsgroup Unhealthy

Additional Sources of Information

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

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

Documentation

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

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

Table 1: Documentation Set for Gigamon Products

GigaVUE 6.3 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE devices; reference information and specifications for the respective GigaVUE devices
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide
GigaVUE-TA200 Hardware Installation Guide

GigaVUE 6.3 Hardware and Software Guides
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-TA100 Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE-Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
***GigaVUE V Series Applications Guide**
GigaVUE V Series Quick Start Guide
GigaVUE Cloud Suite for AWS–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for Azure–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for OpenStack–GigaVUE V Series 2 Guide
***GigaVUE Cloud Suite for Nutanix Guide—GigaVUE V Series 2 Guide**
GigaVUE Cloud Suite for VMware—GigaVUE V Series Guide
***GigaVUE Cloud Suite for Third Party Orchestration**
GigaVUE Cloud Suite for AnyCloud Guide
Universal Container Tap Guide
Gigamon Containerized Broker Guide

GigaVUE 6.3 Hardware and Software Guides

GigaVUE Cloud Suite for AWS–GigaVUE V Series 1 Guide

GigaVUE Cloud Suite for Azure–GigaVUE V Series 1 Guide

GigaVUE Cloud Suite for OpenStack–GigaVUE V Series 1 Guide

GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide

GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide

GigaVUE Cloud Suite for AWS Secret Regions Guide

Reference Guides

GigaVUE-OS CLI Reference Guide

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

GigaVUE-OS Security Hardening Guide

GigaVUE Firewall and Security Guide

GigaVUE Licensing Guide

GigaVUE-OS Cabling Quick Reference Guide

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

GigaVUE-OS Compatibility and Interoperability Matrix

compatibility information and interoperability requirements for Gigamon devices

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

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

Release Notes

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

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

important notes regarding installing and upgrading to this release

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

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

In-Product Help

GigaVUE-FM Online Help

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

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

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

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The VÜE Community

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

Visit the VÜE site to:

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

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

Register today at community.gigamon.com

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

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

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

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

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

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)