GigaVUE Administration Guide

GigaVUE-FM and GigaVUE-OS

Product Version: 5.10

Document Version: 2.2

(See Change Notes for document updates.)

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
1.1	02/11/2021	Revised the Common Criteria topic to reference the NIAP CCEVS site instead of listing specific supported versions and hardware: Common Criteria
2.2	02/11/2021	Revised the Common Criteria topic to reference the NIAP CCEVS site instead of listing specific supported versions and hardware: Common Criteria
2.1	10/13/2020	Doc Updates: - Upgrade GigaVUE-FM Virtual Machines in GigaVUE-FM HA Environment (version 5.9.xx to 5.10.00)–Refer to GigaVUE-FM High Availability - Added information about how to access GigaVUE-FM due to failure in authentication–Refer to Authentication Type - Updated configuration behavior changes based on release–Refer to Overview of Authentication. - Updated AAA information in GigaVUE-OS section–Refer to Configure AAA Authentication Options
2.0	08/28/2020	Added the following new features and enhancements: - GigaVUE-FM Scale Enhancements—Refer to the following topics: - SNMP Traps - Backup and Restore - RBAC Enhancements for Events, and Audit Logs—Refer to the following topics: - All Audit Logs - Events - Alarms for Inline Network and GigaSMART Operations - Alarms
1.0	08/14/2020	Original release of this document with 5.10.00 GA.

Contents

GigaVUE-FM and GigaVUE-OS Administration

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

Featured Content:

- Administer GigaVUE-FM
- Administer GigaVUE Nodes
- Software Licensing Reference
- Related Commands

Administer GigaVUE-FM

Featured topics:

- Authentication
- Tags
- Alarms
- Events
- All Audit Logs
- Tasks
- Reports
- System
- Roles and Users

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
- User Management
- RBAC
- Single Sign-on
- Authentication Type
- RADIUS
- TACACS+
- LDAP
- Grant Roles 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. Click ⚙ on the right side of the top navigation bar.
2. On the left navigation pane, click **Authentication**.

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

Page	Description
User Management	Manage local user accounts. From here, you can add new accounts, edit existing accounts, or delete users. Refer to User Management for details.
RBAC	Controls RBAC mode to decide if the user's privileges are controlled by GigaVUE-FM or the managed device. Refer to RBAC for details.
Authentication Type (Local, RADIUS, TACACS+, LDAP, Third Party)	Use to configure authentication methods. GigaVUE-FM can authenticate users against the local user database configured in the User Management or against the external authentication server (LDAP, RADIUS, or TACACS+) or the third party (that is, external organization IdP). Refer to Authentication Type for more details.

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

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

User Management

The 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

Users

The Users page lets you manage the GigaVUE-FM and GigaVUE-OS FM users. You can also configure user's role and user groups to control the access privileges of the user in GigaVUE-FM. 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 users configured in GigaVUE-FM. For more information about adding users, refer to the Add Users section in the Roles and Users.

User Groups

The User Groups page lists the user groups available in GigaVUE-FM. Refer to the Create User Groups for more details to associate a group to a user.

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.

Change Your Password

Users authenticated against GigaVUE-FM's local user database can always change their own passwords. GigaVUE-FM passwords must conform to the following minimum standards:

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

> NOTE: Users authenticated against an external authentication server cannot change their password using this link. External passwords must be changed in the external authentication server itself.

The following are the steps for changing your password:

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

The Change Password page displays.

2. On the Change Password page, do the following:

   - Enter your current password in the **Current Password** field.
   - Enter the new password in the **New Password** and **Confirm Password** fields.

3. Click **Save**.

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

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

RBAC

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

- Data on managed devices or
- Data in GigaVUE-FM.

For more information about RBAC, refer to Roles and Users.

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:

- **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

ADFS is the only external IdP that has been qualified to be operational with GigaVUE-FM. To configure ADFS as external IdP you must perform the following:

1. 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 ADFS in GigaVUE-FM for details.
3. Install IdP signing certificates (ADFS) 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 ADFS). You must then log in using the external IdP user name and password for logging in to GigaVUE-FM.

Refer to the following figure:

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 sp metadata file to configure in IDP.

To configure GigaVUE-FM in ADFS as Relying Party:

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

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

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

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

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

7. Review the data available in preview section and add the relying party.
8. Open **Edit Claim rules** to grant user access:

a. Add a New claim rule to transform UserPrincipalName as 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.

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:

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:

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

Authentication Type

Use the **Authentication > Authentication Type** to configure how user logins are authenticated. GigaVUE-FM supports and authenticates users against the following authentication methods:

- Local database configured in the User Management
- External authentication server (LDAP, RADIUS, or TACACS+)
- Third Party, which is the 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.

> **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.
> However, in case of remote authentication mechanisms, 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 is tried and so on.

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.

To configure Default User Group in GigaVUE-FM:

1. Click ⚙ on the right side of the top navigation bar.
2. On the left navigation pane, select **Authentication** > **Authentication Type**. In the authentication type page that appears:

  a. Select the required **Authentication Type.**
  b. Set the **Default User Group** to one of the options:
    - Super Admin Group
    - Admin Group
    - User Group

3. Click **Save**.

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:

Auth Method	Logged in User	Map Default UserGroup	Remote Roles/ Group Base DN (if configured)	Expected Group	Assigned Group	Notes
Local	test	-	-	fm_user	fm_user	The authMethod is 'LOCAL'. Therefore,

Auth Method	Logged in User	Map Default UserGroup	Remote Roles/ Group Base DN (if configured)	Expected Group	Assigned Group	Notes
						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 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

Auth Method	Logged in User	Map Default UserGroup	Remote Roles/ Group Base DN (if configured)	Expected Group	Assigned Group	Notes
						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 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.
LDAP	ldapuser1	-	CN=FMQA-SSO,DC=hqdevtest,DC=com	fm_admin	fm_admin	The mapped group for the provided Group Base DN will be assigned to the logged in user.
LDAP	ldapuser2	-	CN=FMQA-SSO,DC=hqdev,DC=com	-	-	If there are no group mapped to the provided/associated

Auth Method	Logged in User	Map Default UserGroup	Remote Roles/ Group Base DN (if configured)	Expected Group	Assigned Group	Notes
						GROUP BASE DN, then GigaVUE-FM will reject the user and will not allow the user to log in as well.
LDAP	ldapuser2	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	ldapuser3	-	-	-	-	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	ldapuser3	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 whether **Default User Group** has been configured; If so, it will assign the same and allow the user to log in to GigaVUE-FM.

External Authentication Server Group Assignments

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

Remote Server	In GigaVUE-FM Release 5.7 and earlier (Role Mapping)	In GigaVUE-FM Release 5.8 and further (User Group Mapping)	Example
TACACS+	<mapping_local_ user>[:role-<mapping_local_ role_1> [role-<mapping_local_ role_2>[...]]]	gigamon:groups=<comma separated FM groups>	gigamon:groups=Super Admin Group,Admin Group
RADIUS	<mapping_local_ user>[:role-<mapping_local_ role_1> [role-<mapping_local_ role_2>[...]]]	Class=<comma separated FM groups>	Class=Super Admin Group,Admin Group

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

Assign User Groups in External Authentication Servers

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

RADIUS

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

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

Figure 1 *Adding 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 Server section has four buttons that allow you to manage the information that appears in the table. **Add**, **Edit**, **Delete**, and **Default Settings**.

Controls	Description
Add	Allows you to add a new RADIUS Server to the list. See Add a New RADIUS Server for details.
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.
Edit Default	Allows you to set default **Key**, **Timeout**, and **Retransmit** options for RADIUS Servers. When you add a new RADIUS Server to the list, you have the option of accepting these default settings or providing custom values. See Set Default Key, Timeout, and Retransmit Options for RADIUS Servers for details.

Add a New RADIUS Server

You can add a new RADIUS Server to GigaVUE-FM. Click the **Add** button and set the options shown in Figure 2 Adding Radius Server.

Figure 2   *Adding Radius Server*

The following table describes the settings on the Add Radius Server page.

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 **Key**, **Timeout**, and **Retransmit** options configured by clicking the **Edit Default** button at the top of the **RADIUS** page.

Setting	Description
	Alternatively, you can leave this box unchecked and set custom values for the **Key**, **Timeout**, and **Retransmit** options using the respective fields.
SharedSecret	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 open the Edit Radius Default Settings page shown in the following figure. Use this page to set default **Key**, **Timeout**, and **Retransmit** options available for use with all new RADIUS server entries.

The following table describes the settings.

Setting	Description
Key	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 Type > TACACS+** to add entries to GigaVUE-FM's list of available TACACS+ authentication servers.

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

Figure 3 *TACACS+ Page*

> NOTE: If you are deploying GigaVUE-FM inside AWS, make sure to provide the private IP address of GigaVUE-FM to the TACACS+ server for authentication and not its public IP address. 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 four buttons that allow you to manage the information that appears in the table. **Add**, **Edit**, **Delete**, **Default Settings**.

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

Controls	Description	
Delete	Allows you to delete a TACACS+ Server entry.	
Default Settings	Allows you to set default **Key**, **Timeout**, **Retransmit**, **Service** and **Extra Roles** 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.	

The following are the fields in the TACACS+ server section:

Field	Description
Server IP/DNS Name	The IPv4/IPv6 address or the DNS name configured for this TACACS+ Server entry.
Auth Port	The UDP port number configured for this TACACS+ server entry. The default TACACS+ port number is 49.
Timeout	Indicates how long GigaVUE-FM will wait for a response from the TACACS+ server to an authentication request before declaring a timeout failure.
Retransmit	Indicates the number of times GigaVUE-FM will attempt to authenticate with this TACACS+ server before moving on to the next authentication server or method.
Enabled	Indicates whether this server is currently enabled for use with authentication requests.

Add a New TACACS+ Server

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

Figure 4   *Adding TACACS+ Server Settings*

The following table describes the settings.

Setting	Description
Enabled	Specifies whether this server is currently enabled for use with authentication requests
Server IP/DNS Name	Specifies the IP address of the TACACS+ server. The same IP address can be used for more than one TACACS+ server as long as they use different **Auth Port** values.
Auth Port	Specify 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.
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.
Key	Specifies a shared secret string to be used for encryption of authentication packets sent 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 Type > LDAP** section to add entries to GigaVUE-FM's list of available LDAP authentication servers.

Figure 5   *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 has been 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 select SSL or TLS as mode. To enable LDAP over SSL:

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

LDAP Server Section: Controls and Fields

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

Controls	Description
Add	Allows you to add a new LDAP Server to the list. See Add a New LDAP Server for details.
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 Type > LDAP** and click **Add**. The Add LDAP Server page is displayed. Refer to Add a New LDAP Server. Enter the following details and click **Save**:

- Server IP/DNS Name
- Priority

A new LDAP Server is added to the GigaVUE-FM's list.

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.

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

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.

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

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

7. Click the **Add** button [Add ∧] to add this attribute to the authorization profile.

8. Assign this authorization profile to a group and populate it with GigaVUE-FM users.

Figure 6 Supplying the Class Field for RADIUS (ACS 5.x) shows these settings in a CiscoSecure ACS 5.x authorization profile.

Figure 6   *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

4. Click the **Add** button to add this attribute to the shell profile.

5. Click **Submit** to finalize this shell profile.

6. Create Service Selection Rules that will assign this shell profile to desired GigaVUE-FM and GigaVUE-OS users.

Figure 7 Supplying local-user-name and groups in ACS 5.x for TACACS+ shows the an example of a shell profile for TACACS+ in ACS 5.x with the local-user-name attribute supplied.

Figure 7   *Supplying local-user-name and groups in ACS 5.x for TACACS+*

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 hundreds of clusters and thousands of 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 **admin** or **super_admin_role** or 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

Notes and Rules

Refer to the following notes and rules 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.
- **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
- GigaVUE-FM does not allow you to create or delete any tag 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 object, then all the objects at the lower level inherit the tag ID. This 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

To view the tags, click ⚙ on the top navigation bar. On the left navigation pane, select **Tags**. The existing tags are displayed in the Tags page.

Figure 8   *Tags Home Page*

The following buttons are displayed in the Tags page.

Field	Description
Filter	Filters the tags available in the Tags page. For more information, refer to Filter Tags.
New	Creates a new tag. For more information, refer to Create a Site and Create User-defined Tag.
Edit	Edits an existing tag. For more information, refer to Edit Tags.
Delete	Deletes an existing tag.

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

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 right side of the top navigation bar, click ⚙.

2. On the left navigation pane, select **Tags**.

3. In the Tag page, click **New**.

Figure 9 *New Tag Creation*

4. 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**.

5. Click **OK**. 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**.

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.

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 right side of the top navigation bar, click ⚙.
2. On the left navigation pane, select **Tags**.
3. In the Tags page, select a tag you want to edit and click **Edit**.
4. In the Edit Tag page, you can edit the following:
   - Description
   - Multi Valued
   - Tag Type
   - Hierarchy
   - Values
5. Click **OK** to save the changes.

> NOTE: You cannot edit the name of the tag.

Filter Tags

To filter the tags:

1. On the right side of the top navigation bar, click ⚙.

2. On the left navigation pane, select **Tags**.

3. In the Tags page, click **Filter** to filter the tags. The Filter quick view is displayed. Refer to Figure 10 Tag Filters.

Figure 10   *Tag Filters*

4. From the **Names** drop-down list, select the name of the tag that you want to search. You can select multiple tags. The respective tag key will be displayed in the drop-down list.

5. From the **Values** drop-down list, select the name of the tag value. The results matching the filter criteria is displayed in the Tags page.

Delete Tags

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

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 Create Roles 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 Create User Groups for more details on defining user roles.

RBAC mode: RBAC mode is used to apply further restriction on user's tasks or operation.

GigaVUE-FM provides the following two RBAC modes:

- Device RBAC
- GigaVUE-FM RBAC

> NOTE: Users are authorized to perform a task or operation based on the definition of their role in GigaVUE-FM.

Device RBAC mode

Once the users are authorized, GigaVUE-FM in the device RBAC mode does the following:

- Leverages the RBAC settings defined for the user on the managed device to further control the user's access privileges.
- Uses the user's login credentials to execute the task or operation on the managed device.

If the user does not have the necessary privileges defined on the managed device, the user will not be allowed to perform the task or operation. Therefore, user's login credentials in GigaVUE-FM should match the user's login credentials in the managed device.

It is recommended that both GigaVUE-FM and the managed device validate user credentials against a common authentication service (such as LDAP, RADIUS, or TACACS+).

GigaVUE-FM RBAC

Once the users are authorized, GigaVUE-FM in this mode, does the following:

- Uses the node credentials to execute the task or operation on the managed device. Node credential is the credential used while adding a node in GigaVUE-FM.

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

Set RBAC Mode

To set the RBAC mode in GigaVUE-FM:

1. On the right side of the top navigation bar, click ⚙.

2. On the left navigation pane, select **Authentication** > **RBAC**. The RBAC page is displayed as shown in Figure 11 Enabling or Disabling RBAC Mode on GigaVUE-FM.

Figure 11 *Enabling or Disabling RBAC Mode on GigaVUE-FM*

3. To set the RBAC mode, select or clear the checkbox as required:

- Select the checkbox to use GigaVUE-FM RBAC mode. You will get a confirmation message stating that the RBAC mode cannot be reverted. Select **OK** to continue.

   GigaVUE-FM RBAC is the default RBAC mode.
- Leave the checkbox unchecked to use device RBAC mode. If the number of nodes and/or devices is large, it is recommended that LDAP or similar mechanism is used to ease user credential management. When in this mode, ensure that users are added to the local GigaVUE-FM or central server (LDAP, RADIUS, or TACACS+) with the same node credential as the device.

> NOTE: Starting in software version 5.7, device RBAC is not supported in GigaVUE-FM. But, if you are already using device RBAC and upgrade to GigaVUE-FM version 5.7, then GigaVUE-FM supports device RBAC and provides an option to migrate to GigaVUE-FM RBAC.

4. Click **Save** to set the mode.

In both the RBAC modes, GigaVUE-FM RBAC is enforced. For example, a GigaVUE-FM user with the role fm_user will not be able to modify anything on the node even if the user's login credential matches the credential on the managed node and has all the necessary privileges.

> NOTE: Selecting or clearing the checkbox has no impact on the following operations performed by GigaVUE-FM:

- Rediscovery
- Configuration sync
- Statistics collection

In any RBAC mode in GigaVUE-FM, a user with **fm_super_admin**/ **fm_admin** role or a user with write access to Physical Device Infrastructure Management category can add a node to GigaVUE-FM. However, when adding the node credentials, if the node credentials do not match the admin privileges on the node, the node cannot be managed in GigaVUE-FM.

Configure Role-Based Access and Set Permissions

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

- Add Users
- Create Roles
- Create User Groups

Add Users

This section provides the steps for adding users. You can add users only if you are a user with **fm_super_admin role** or a user with either read/write access to the 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 right side of the top navigation bar, click ⚙.

2. On the left navigation pane, select **Authentication** > **User Management > Users**. The **User Management** page is displayed.

User Management	Users	Roles	User Groups				
						Add	Actions ▾
							Expand All Collapse All
☐	Username	Name	Email	Roles	Resources	Member of Groups	⊕
☐	› admin	System Administrator		1	1 show all	1	⋮
☐	› user1	user1		1	2 show all	1	⋮
☐	› user2	user2		1	2 show all	1	⋮
☐	› user3	user3		1	2 show all	1	⋮
☐	› user4	user4		2	1 show all	2	⋮
☐	› user6	user6		1	2 show all	1	⋮

Figure 12   *FM Users Page*

3. Click **Add**. In the Create User wizard that appears perform the following steps. Click **Continue** to progress forward and click **Back** to navigate backward and change details.

Create User ✖

Name — Name
Username — Username
Email — Email
Password — Password   ❓
Confirm Password — Confirm Password

Cancel   Save

Figure 13   *Create User*

a. In the **User Information** tab, enter the following details:

- **Name:** User's actual name
- **User Name**: User name
- **Email**: Email ID of the user
- **Password/Confirm Password**: Password for the user.

b. Click **Save**.

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. For the steps to create roles, refer to Create Roles. For the steps to create groups, refer to 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:

- **Edit:** Edit the user details.
- **Delete:** Delete a user.
- **View Details:** View the user details.

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.

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, whitelist and so on.

> NOTE: Custom roles are available to users with prime package license. If you do not have a prime license, then GigaVUE-FM supports only the default roles mentioned above.

Refer to the following table for the various categories and the associated resources:

> **NOTE:** Hover your mouse over the resource categories in the Roles page to view the description of the resources in detail.

Category	Associated Resources
All	Manages all resources • A user with fm_super_admin role has both read and write access to all the resource categories. • A user with fm_user role has only read access to all the resource categories.
Infrastructure Management	Manages resources such as devices, cards, ports and cloud resources. You can add or delete a device in GigaVUE-FM, enable or disable cards, modify port parameters, set leaf-spine topology. The following resources belong to this category: • **Physical resources:** Chassis, slots, cards ports, port groups, port pairs, cluster config, nodes and so on • **GigaVUE-FM inventory resources:** Nodes, node credentials • **Device backup/restore:** Device and cluster configuration • **Device license configuration:** Device/cluster licensing • **Statistics:** Device, port • **Tags**: Events, historical trending • **Device security**: SystemTime, System EventNotification, SystemLocalUser, System Security Policy Settings, AAA Authentication Settings,Device User Roles, LDAP Servers, RADIUS Servers, TACACS+ Servers • **Device maintenance**: Sys Dump, Syslog • **Cloud Infrastructure resources**: Cloud Connections, Cloud Proxy Server, Cloud Fabric Deployment, Cloud Configurations, Sys Dump, Syslog, Cloud licenses, Cloud Inventory. > **NOTE:** Cloud APIs are also RBAC enabled.
Traffic Control Management	Manages inline resources, flow maps, GigaSMART applications, second level maps, map chains, map groups. The following resources belong to this category: • **Infrastructure resources**: IP interfaces, circuit tunnels, tunnel endpoints, tunnel load balancing endpoints, ARP entries

Category	Associated Resources
	• Intent Based Orchestration resources: Policies, rules • **GigaSMART resources:** GigaSMART, GSgroups, vPorts, Netflow exporters • **Map resources**: Fabric, fabric resources, flow maps, maps, map chains, map groups, map templates • **Application intelligence resources**: Application visibility, Metadata, application filter resources • **Tag**: Flow manipulation - Netflow operations, Statistics - device port • Active visibility • **Inline resources**: Inline networks, Inline network groups, Inline tools, Inline tool groups, Inline serial tools, Inline heartbeat profile • **Cloud operation resources**: Monitoring session, stats, map library, tunnel library, tools library, inclusion/exclusion maps. **NOTE:** Cloud APIs are also RBAC enabled.
FM Security Management	Ensures secure GigaVUE-FM environment. Users in this category can manage user and roles, AAA services and other security operations.
System Management	Controls system administration activities of GigaVUE-FM. User in this category are allowed to perform operations such as backup/restore of GigaVUE-FM and devices, and upgrade of GigaVUE-FM. The following GigaVUE-FM resources belong to this category: • Backup/restore • Archive server • License • Storage management • Image repo config • Notification target/email

Category	Associated Resources
Whitelist/CUPS Management	Manages the whitelist configuration. The following resources belong to this category: • GTP whitelists • SIP whitelists • Diameter whitelists
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.

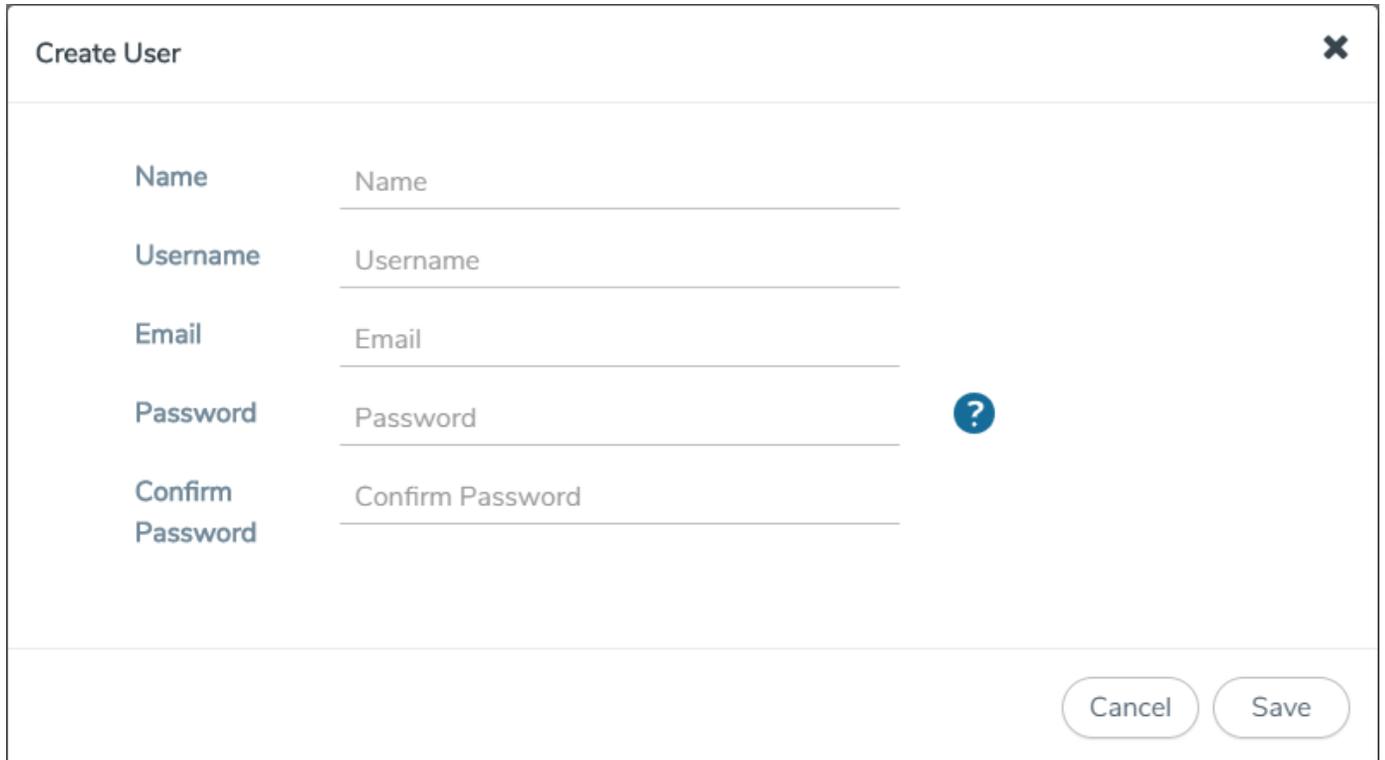To create a role,:

1. On the right side of the top navigation bar, click .

2. On the left navigation pane, select **Authentication > User Management > Roles**.

3. Click **Create**. In the Wizard that appears, perform the following steps. Click **Continue** to progress forward and click **Back** to navigate backward and change details.

Create Role ✖

Figure 14   *Create Roles*

a. In the **Name Role** tab enter the following:

- **Name:** Name of the role.
- **Description:** Description for the role.

b. In the **Select Permissions** tab:

- Select the required resources. Hover your mouse over the resource category to get a glimpse of the resource.
- Select the required read and write permissions for the resources selected.

c. In the **Review** tab, review the role created. Click **Save** to create the role.

The new role is added to the summary list view.

The following tables describes how access control is applied to a user who has the required role to access the resources based on:

- RBAC settings in the device
- RBAC mode selected in GigaVUE-FM

Table 1: Access control for a user who has the required role in GigaVUE-FM to access the resources.

RBAC Settings on the Managed Devices	RBAC Mode in GigaVUE-FM	Access control
Allows user to access its resource	Device RBAC	Allow user to access GigaVUE- FM resources
		Allow user to access managed device resources
	GigaVUE-FM RBAC (node credentials has admin privileges)	Allow user to access GigaVUE- FM resources
		Allow user to access managed device resources
Disallows user to access its resource	Device RBAC	Allow user to access GigaVUE- FM resources
		Disallow user to access managed device resources
	GigaVUE-FM RBAC (Node credential has admin privileges)	Allow user to access GigaVUE- FM resources
		Allow user to access managed device resources

NOTE: Refer to the following notes:

- For users who do not have the necessary role to access the resources, the access controls mentioned above are disallowed irrespective of the RBAC settings on the managed devices and the RBAC mode in GigaVUE-FM.

- For users authenticated using the remote authentication servers such as LDAP or TACACS+, user groups will be assigned to the user based on the mapped-user group configuration. Refer to Authentication for more details about role-mapping in LDAP and TACACS+ based authentication.

Create User Groups

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

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

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

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

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

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

To create a group:

1. On the right side of the top navigation bar, click ⚙.

2. On the left navigation pane, select **Authentication > User Management > User Groups**.

3. Click **Create**. In the Wizard that appears, perform the following steps. Click **Continue** to progress forward and click **Back** to navigate backward and change details.

Create Group

Figure 15   *Create Group*

a. In the **Name Group** tab enter the following:

- **Group Name:** Name of the group.
- **Description:** Description for the group.

b. In the **Assign Roles** tab, select the required role.

c. In the **Assign Tags** tab, select the required tags Id and tag value. Only access control tags will be available for selection.

> **NOTE:** Select the **Override User** option to allow the user to access the resources for which the tag key of the resource does not match the tag key of the user.

d. Select the required users (this step is optional).

e. In the **Review** tab, review the group created. Click **Save** to create the group.

The new group is added to the summary list view. Click on the ellipses to perform the following operations:

- **View Details:** View the details of the group such as the Group Name, Description, Role associated to the group, Tag associated to the group.
- **Assign Users:** Assign groups to users if this step was skipped at the time of creating the group.
- **Remove Users**: Remove existing users from the group.
- **Edit:** Edit an existing group.
- **Delete:** Delete an existing user.

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
- Manage Alarms
- Manage Multiple Alarms
- Alarm Correlation
- Filter Alarms
- Events

NOTE: The alarm management feature is available only to users with prime package license.

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.

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.
-

View Alarms

To view the alarms triggered in GigaVUE-FM:

1. Click **Alarms** on the top navigation bar. The Alarm page appears. Widgets for the following alarm categories appear on the top of the page

   - Unacknowledged
   - Acknowledged
   - Critical
   - Major
   - Minor
   - Warning
   - Information

> **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.

Figure 16   *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.

Permission Level	Description
Comment	Comment added/updated by the user for the alarm.
Status	The status of the alarm. Can be: • Acknowledged. You can hover your mouse to view the details of the user who acknowledged the alarm and the last acknowledged time. • Unacknowledged
Cluster ID	Cluster Id
Host Name	Host name
Alias	Alias name
Last Acknowleged By	User who acknowledged the alarm.
Acknowledged Time	Time the alarm was acknowledged.

3. Select an alarm and click the ellipsis to:

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

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

   • **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.

Alarms for Fabric Maps

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.

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.

Orchestrated Policies	Fabric Maps	Cluster Level Maps	Ports
Policy_1	Fabric_map_1	Map_1	Port_11 Port_12
		Map_2	Port_21 Port_22

	Fabric_map_2	Map_3	Port_31
			Port_32
		Map_2	Port_21
			Port_22
Policy 2	Fabric_map_4	Map_4	Port_41
			Port_42
		Map_5	Port_51
			Port_52

Refer to the following notes:

- If the health status of Port_21 (circuit port) turns red, then the following alarms are generated:
  - One port level alarm for the circuit port Port_21.
  - One cluster map level alarm for Map_2.
  - Two fabric map level alarms for Fabric_map_1 and Fabric_map_2.
  - One policy level alarm for Policy_1.
- If the health status of Port_51 (stack port) turns red, then the following alarms are generated:
  - One port level for the stack port Port_51
  - One cluster map level alarm for Map_5
  - One fabric map level alarms for Fabric_map_4
  - One policy level alarm for Policy_2

Alarms for Inline Networks

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 configuration 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.

Manage Alarms

Use the Manage Alarms button to configure the following:

- Enable Exclusion Rules
- Configure Threshold Values for Memory and CPU Status

Enable 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 top 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.

Configure 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. Click **Alarms** on the top navigation bar.

2. Select the alarms that you want to acknowledge.

3. Click 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

3. Click **Apply Filter** to apply the filter.

4. Click **Clear** to clear the filter.

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

Alarm Correlation

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

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

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

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

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.

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 Persmissions
- Filter Events
- Archive or Purge Event Records

Overview of Events

The Events page display the events generated from GigaVUE-FM and GigaVUE-OS 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.

Table 2: Event Parameters describes the parameters recording for each event. You can also use filters to narrow down the results. Refer to Filter Events.

Table 2: Event Parameters

Controls/ Parameters	Description
Filter	Opens the Filter quick view for narrowing down the events to view the desired results.
Manage	Opens the Manage Event page for exporting and selecting records for archiving or purging. For more information, refer to Filter Events.
	NOTE: This option is not available in the Physical and Virtual Events page.
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 H Series or GigaVUE-FM and GigaVUE-OS 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

Controls/ Parameters	Description
	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.
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.
Event Type	The type of event that generated the events. The type of events can be CPU utilization high, cluster updated, device discovery failed, fan tray changed, netflow statistics, and so on.
Tags	Tags associated with the event
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.
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).
Device IP	The IP address of the device.
Host Name	The host name of the device.

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-FM User's Guide*.

View Events based on User's RBAC Persmissions

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 to see events from resource that are permitted as per your role definitions and events from the devices that he 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.

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.
Start Date End Date	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).
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).
Tags	Tags associated with the event

To filter the event:

1. Click **Filter**.

   The Filter quick view appears.

2. Specify the filter criteria, then click **Apply 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.

Archive Event Records

To archive the events records, do the following:

1. Select **Events** in the navigation pane.

2. Click **Manage**.

3. Click the Calendar icon and select a date. Records older than this date will be exported.

4. Select **Export Records** and specify the following:

   - The address of the SFTP Server to which the logs will be exported.
   - The user name and password for the SFTP server.
   - The file path on the server where the files will be archived. The file should be in the .zip format.

5. Click **OK** to export to the records to the SFTP server.

Purge Events Records

The events data continues to grow over time. You can purge the records, by doing the following:

1. Select **Events** in the navigation pane.

2. Click **Manage**.

3. Click the Calendar icon and select a date. Records older than this date will be purged.

4. Select **Purge Selected Records**.

5. Click **OK** to purge the records.

Archive and Purge Events Records

Audit log records can be exported and purged at the same time by doing the following:

1. Select **Events** in the navigation pane.

2. Click **Manage**.

3. Click the **Calendar** icon and select a date. Records older than this date will be exported.

4. Select **Export Records** and specify:

   • 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. The file should be in the .zip format.

5. Select **Purge Selected Records**.

6. Click **OK** to export the records to the SFTP server, and then purge the records.

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
   • 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 have the following parameters:

Parameters	Description
Time	Provides the timestamp on the log entries.
User	Provides the logged user information.
Operation Type	Provides specific entries that are logged by the system such as: • Log in and Log out based on users. • Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.
Entity type	Name of the resource type that the audit log is associated to such as port, port group, user, host name, device IP.
Source	Provides details on whether the user was in 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:

- When—display logs that occurred within a specified time range.
- Who—display logs related a specific user or users.
- What—display logs for one or more operations, such as Create, Read, Update, and so on.
- Entity Type—display logs for resource types that the audit log is associated to.
- Result—display logs for success or failure.

To filter the audit logs, do the following:

1. Click **Filter**.

   The quick view for Audit Log Filters displays.

2. Specify any or all of the following:

- **Start Date** and **End Date** to display logs within a specific time range.
- **Who** limits the scope of what displays on the Audit Logs page to a specific user or users.
- **What** narrows the logs to the types of operation that the log is related to. You can select multiple operations. Select **All Operations** to apply all operation types as part of the filter criteria.
- **Entity Type** allows you to select the required entity type such as host name, device ip and so on.
- **Result** narrows the logs related to failures or successes. Select All Results to apply both success and failure to the filter criteria.
- **Tags** associated to the audit logs which are acquired from a resource object

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

Archive or Purge Audit Log Records

Audit logs are saved to the 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.

| All Audit Logs | | | | | | | | Filter | Manage |

Filter : **none**

Time	User	Operation Type	Entity Type	Source	Device IP	Hostname	Status	Description	Tags

No Records Found

> **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.

Archive Audit Logs

To archive the audit log records, do the following:

1. On the right side of the top navigation bar, click ⚙.

2. On the left navigation pane, select **All Audit Logs** in the navigation pane.

3. Click **Manage**.

4. Click the **Calendar** icon and select a date. Records older than this date will be exported.

5. Select **Export Records** and specify:

   - 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.

6. Click **OK** to exported to the records to the SFTP server.

Purge Audit Log Records

The audit log data continues to grow over time. You can purge the audit log records, by doing the following:

1. On the right side of the top navigation bar, click ⚙.

2. On the left navigation pane, select **All Audit Logs** in the navigation pane.

3. Click **Manage**.

4. Click the **Calendar** icon and select a date. Records older than this date will be purged.

5. Select **Purge Selected Records**.

6. Click **OK** to purge the records.

Archive and Purge Audit Log Records

Audit log records can be exported and purged at the same time by doing the following:

1. Select **Audit Logs** in the navigation pane.

2. Click **Manage**.

3. Click the Calendar icon and select a date. Records older than this date will be exported.

4. Select **Export Records** and specify:

   - 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.

5. Select **Purge Selected Records**.

6. Click **OK** to exported the records to the SFTP server, and then purge the records.

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.

To view the **Admin Tasks**, click ⚙ on the top navigation bar. On the left navigation pane, click Tasks.

	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	-	-	

Admin Tasks — Total Tasks : **2**   Filtered By : **none** — Delete | Filter

Figure 17 *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.

Parameters	Description
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.

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 right side of the top navigation bar, click ⚙.

2. On the left navigation pane, select **Tasks**.

3. In the Admin Tasks page, click the Detail link in the Node Summary column. Refer to Admin Tasks.

4. 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 right side of the top navigation bar, click ⚙.

2. On the left navigation pane, select **Tasks**.

3. From the Admin Tasks page, select a task from the list.

4. Click **Delete**.

   The task is unscheduled and stopped the task 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-FM and GigaVUE-OS nodes upgrade, and GigaVUE-FM configuration data.

Figure 18 *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 right side of the top navigation bar, click ⚙.

2. On the left navigation pane, select **Tasks > Scheduled Task**.

3. 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).

4. Click **Delete**.

   Clicking Delete unschedules and stops the task from happening.

Reports

The Reports page lists different templates that you can use to generate reports. This section covers the following topics:

- Overview of Reports
- Report Templates
- NetFlow Format Support on Exporters

Overview of Reports

The reports can be downloaded 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 page is available based on the GigaVUE-FM and GigaVUE-VM licenses installed on the system. See the *Licensing* section for more details.

- Reports can be stored or deleted on the 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, click ⚙ on the top navigation bar. On the left navigation pane, select **Reports**. Click **Generate New**.

Figure 19   *Reports Page View*

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

After the report is generated, if you wish to view it, the browser will try to open a new window. However, if you have a pop-up blocker enabled, you will need to disable the pop-up blocker to view the pages.

Report Templates

This section describes the report templates available for generating reports:

- Template 1: Visibility Fabric Performance Report provides traffic analysis information.

- Template 2: Visibility Fabric Node Details Report provides specific details relating to the physical nodes (includes H Series, G Series and TA Series).

- Template 3: GigaVUE-VM Report provides for GigaVUE-VM traffic analysis information.

- Template 4: Visibility Fabric Inventory Report provides a summary of all physical inventory (includes H Series, G Series and TA Series) that is visible on GigaVUE-FM.
- Template 5: GigaSMART Performance Report summary on GigaSMART performance for all H Series nodes with GigaSMART functionality.

Template 1: Visibility Fabric Performance Report

This multi-page template 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 20 Visibility Fabric Performance Report shows an example of a report for Visibility Fabric Performance.

Figure 20   *Visibility Fabric Performance Report*

Template 2: Visibility Fabric Node Details Report

This multi-page template 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 21 Inventory Details Report shows an example of a report for Visibility Fabric Node Details.

Figure 21   *Inventory Details Report*

Template 3: GigaVUE-VM Report

This multi-page template 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 22 Report Pages Available for GigaVUE-VM show an example of a report for GigaVUE-VM.

Figure 22   *Report Pages Available for GigaVUE-VM*

Template 4: Visibility Fabric Inventory Report

This multi-page template 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 23 Inventory Summary Report show an example of a report for Visibility Fabric Inventory.

Figure 23 *Inventory Summary Report*

Template 5: GigaSMART Performance Report

This template 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 24 Report for GigaSMART Performance Indicators show an example of a report for GigaSMART Performance.

Figure 24   *Report for GigaSMART Performance Indicators*

NetFlow Format Support on Exporters

NetFlow Exporters support versions IPFIX, v5, and v9. Starting in software version 5.3, the Common Event Format (CEF) version 23 is also supported. CEF is a standard format used by event collection/correlation Security Information and Event Management (SIEM) vendors. SIEMs such as Arcsight, Splunk, and QRadar accept CEF format. By supporting CEF, NetFlow metadata can integrate with and use a variety of SIEMs.

CEF is a logging format that uses the syslog message as a transport mechanism, meaning that the CEF message (header and payload) is included within the syslog message. The transport protocol that is supported is UDP and the default port number is 514.

Metadata that is generated by NetFlow can be exported in the supported formats to one or more collectors. Each exporter must have the same export type (v5, v9, IPFIX, or CEF). One CEF message is sent out per record per flow.

Also, starting in software version 5.3, IP fragmentation is supported. CEF does not allow a message to be split over multiple CEF payloads. Since CEF messages are verbose, they can be larger than the MTU.

To support CEF messages that exceed the MTU, a single IP datagram containing a CEF message will be broken up into multiple packets of smaller sizes. The reassembly of the datagram will occur at the receiving end (at the SIEMs).

For details on the CEF message format, refer to CEF Message Format.

CEF Message Format

An example of the CEF message format is as follows:

```
Fri Feb 23 02:25:37 2018 9/3/e1
CEF:23|Gigamon|metadata|5.3.00|4|metadatageneration|6| src=68.94.156.1
GigamonMdataDnsAdditionalType=41GigamonMdataDnsAdditionalTypeText=OPT
```

In the example CEF message, there is a syslog header, a CEF header, and an extension that contains the CEF payload. The fields are delimited with a vertical bar (|).

The syslog header contains the following:

- timestamp—Fri Feb 23 02:25:37 2018
- host name identifier—9/3/e1

NOTE: The host name identifier has the format <box ID>/<slot ID>/<engine ID>.For example, 9/3/e1 means 9 is the box ID, 3 is the slot ID, and e1 is the engine ID.

The CEF header contains the following:

- version—CEF:23
- device vendor—Gigamon
- device product—metadata
- device version—5.3.00
- signature identifier—4
- name—metadata generation
- severity—6

The CEF extension contains key-value pairs delimited with a space. In the example CEF message, the following is the CEF payload, in plaintext:

- src=68.94.156.1
- GigamonMdataDnsAdditionalType=41
- GigamonMdataDnsAdditionalTypeText=OPT

The CEF standard specifies key-value pairs. There are some predefined 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=31373031303633030303030305a
GigamonMdataSslSerialNo=0118ee3c2167b99e1b718c6eadb8fb4d00000000
GigamonMdataSslValidNotAfter=32303031313533132303030305a
GigamonMdataSslCertSigAlgo=2a864886f70d01010b
GigamonMdataSslCertSubAlgo=2a864886f70d010101
GigamonMdataSslCertSubKeySize=270 GigamonMdataSslServerVersion=771
GigamonMdataSslCertSubAltName=*.stickyadstv.com
GigamonMdataSslServerCompressionMethod=192 GigamonMdataSslServerCipher=49199
GigamonMdataSslServerVersionText=TLSv1.2 GigamonMdataSslServerSessionId=63
GigamonMdataSslIssuer=2f433d55532f4f3d44696769643657272420496e632f4f553d7777772e6469
676963
6572742e636f6d2f434e3d446967676943657274205348413220486967682041737375726e636
52053657276 6572204341 GigamonMdataSslCertSubCommonName=*.stickyadstv.com
GigamonMdataSslSub=2f433d55532f53543d4e657720596f726b2f4c3d4e657720596f726b2f4f3d4
672656
```

5776865656c204d6564696120496e632f4f553d46726565776865656c2f434e3d2a2e737469636b796164737 4762e636f6d dst=10.50.22.59 src=38.106.34.118

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.

To access the system pages, click the gear icon ⚙ on the top navigation bar. On the left navigation pane, click **System**.

System provides access to the following pages:

- Preferences
- Node Details
- NAT Configuration
- Backup/Restore
- Bulk Configuration
- Images
- Trust Store
- Notifications
- Email Servers
- Licenses
- System Logs
- Storage Management
- SNMP Traps

Preferences

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

Figure 25   *Preferences for GigaVUE-FM*

To change the GigaVUE-FM preferences:

1. On the right side of the top navigation bar, click ⚙.

2. On the left navigation pane, go to **System** > **Preferences**.

3. Click **Edit**.

4. In the Edit Preferences page, you can perform the following:

   - 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.)
   - Under **Display**, 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

  - You can configure the following using the **Session** option:

- 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)** option, the maximum duration GigaVUE-FM can be inactive before it is logged out automatically. By default, the auto-logout time is set to 30 minutes. You can set the auto-logout time to a maximum of 350 minutes, only if the **NOC View Mode** is set to off.

- Select the number of items to be displayed on a page by entering a value in the **Items displayed per page** field.
- 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-FM User's Guide"*.
- Configure a pre-login banner which states the security policy of your company or organization in the Login Banner box. For more information about configuring a custom banner, refer to the *"Configure a Custom Banner"* section in the *"GigaVUE-FM User's 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.

Node Details

The **Node Details** page includes the details of every node managed by GigaVUE-FM. Figure 26 Credentials for Physical Nodes. shows an example. For each node, you need to provide a user name and password that allow administrator privileges on the node.

To access **Node Details**, click ⚙ on the top navigation bar. On the left navigation pane, go to **System** > **Node Details**.

Figure 26   *Credentials for Physical Nodes.*

> NOTE: To ensure that users have the same privileges whether using GigaVUE-FM or H-VUE, it is advised that you use a centralized authentication server such as LDAP, instead of storing the user name and password locally.

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-FM and GigaVUE-OS 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 Page Controls and Fields

Node Details table has following buttons that allow you to manage the information that appears in the table, **Add**, **Edit**, **and Delete**. To Edit or Delete a Node, click on the check box to the left of the IP address that needs to be modified.

Controls	Description
Add	Allows you to add a node and its login credentials. • Clicking **Add** opens a dialog where you specify the node IP address, a User name, and a Password. • Only one node can be added each time. • The user name and password you provide must have administrator privileges on the node.
Edit	Allows you to change the credentials for a node. • Select a node and click Edit to open a dialog where you make the changes. • Multiple IP addresses cannot be selected for editing. > NOTE: If you have changed the HTTPS port number of a device using CLI, then you must update the same in GigaVUE-FM using the Edit option. Failure to do so will terminate the communication between GigaVUE-FM and the device.
Delete	Allows you to delete a node and its credentials. • The Delete Option will have a validation option to select as a pop-up prior to deleting a node. • Multiple IP addresses can be selected for deletion.

NAT Configuration

The NAT Configuration page allows you to configure the following:

- DNS Servers and Default Search Domains
- Interface Settings

Refer to the following sections for details:

- IP Resolver
- Interface Settings

IP Resolver

GigaVUE-FM must be configured with DNS server and default search domains in order to add and manage the nodes by their FQDN. This configuration may not be mandatory to manage normal nodes/clusters but it is mandatory to manage the clusters behind NAT.

The reason is 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 as follows:

1. On the right side of the top navigation bar, click ⚙.

2. On the left navigation pane, select **System > NAT Configuration > IP Resolver.**

3. Enter the following details, as required. Use the +/- icon to add the additional servers.

Field	Description
DNS Server	Domain name server
Default Search Domain	Default search domain

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

Interface 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 Interface Settings page you can configure any other interface as the default interface. To do this:

1. On the right side of the top navigation bar, click ⚙.

2. On the left navigation pane, select **System > NAT Configuration > Interface Settings**.

3. Enter the following details:

Field	Description
Management Interface	Management interface
Data Interface	Data interface

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

4. 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.
- 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.

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 and GigaVUE-OS FM Appliance.**

3. Click **Backup**.

4. Select **Immediate**.

5. Select the archive server for the backup file. Refer to Figure 27 Immediate Backup to an Archive Server.

   To add an archive server, refer to Add an Archive Server.

6. Click **OK**.

Figure 27   *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 and GigaVUE-OS 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 28 Scheduled Backup for GigaVUE-FM shows an example scheduled backup. In this example, the weekly backup to archive server Archive Server 1 starts on March 17 and occurs every Saturday at 9:00 pm until March 31.

Figure 28   *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 twice 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.

Figure 29   *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-FM and GigaVUE-OS 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 master 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 master 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 Master of the cluster (and new API that will be provided same as 7 above).

10. Cluster master 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.

Bulk Configuration

The Bulk Configuration page allows you upload and send a configuration file to one or more G Series nodes or clusters at the same time, replicating the configuration on each node or cluster. Bulk Configuration is not supported on H Series nodes.

The configuration file is a text-based file. This means that you can create a custom configuration file and upload it, or you can make a backup of a node and then edit the backup file to create a new configuration.

Bulk configuration is only supported on G Series models GV2404 and GV420. GV212 and GV216 are not supported. If unsupported device models are in a G Series stack, the entire stack is disregarded for configuration.

Important: GigaVUE-FM does not validate the configuration file before pushing it to the specified node or nodes during bulk configuration. If any errors occur, they are logged in the configuration log files.

Replicate Configuration Files

Use the following steps to replicate a configuration across nodes and clusters. If you are creating a new configuration file for bulk configuration, go directly to step 3.

1. Create a backup file.

   a. Click **Physical** on the top navigation bar.

  b. On the Physical Nodes page, select a node.

  c. Go to **Actions > Backup**.

  d. On the Backup page, select **Immediate**.

  e. Click **OK**.

2. Download the backup file created in Step 1.

  a. On the right side of the top navigation bar, click ⚙.

  b. Select **Backup/Restore > Physical Nodes**.

  c. Select the backup file of the node you want to replicate.

  d. Select **Actions > Download**.

  e. Select **Immediate**.

  f. Click **OK** and then save the file.

   GigaVUE-FM downloads the configuration as a text file.

3. Open the configuration file in a text editor to make any needed changes to the configuration.

 The configuration file is expected to have header information that is based on the device type. If you are creating a configuration file from scratch, you need to provide the correct header. Table 3: Headers for G Series Configuration Files provides the headers for each device type that is supported. In the header, version is the software version and file is the filename of the device image.

4. Upload the configuration file:

  a. Select **System > Bulk Configuration**.

   The Bulk Configuration Files page displays. An example is shown in the following figure.

  b. Select **Actions > Upload**.

   The Upload Configuration File page displays. The page is shown in the following figure.

  c. Click **Choose File** to upload the file downloaded and edited in Step 2.

  d. (Optional) Enter a comment about the file in the **Comment** field.

  e. For **Series**, select G Series. (Only G Series nodes are supported in the current release.)

  f. Click **OK**.

   The uploaded file appears on the Configuration File page.

5. Replicate the file on the node or cluster.

  a. On the Bulk Configuration page, select the file uploaded in Step 4.

  b. Select **Actions > Replicate**.

The Replicate Configuration File page displays. The page shows the selected configuration file, comment entered on the Upload Configuration File page, and the list of nodes that you can select for replication. Replicate Configuration Files shows an example.

When **Autosave Backup Configuration** is selected, GigaVUE-FM takes a backup prior to applying the configuration changes. Configuration changes are not be applied if backup fails.

    c.   Select the nodes to which you want to replicate the configuration file

    d.   Click **OK**.

6.   To view the progress of the configuration, select **All Alarms/Event** in the left navigation pane.

Table 3: Headers for G Series Configuration Files

Device	Header
GigaVUE-FM and GigaVUE-OS-420	#=== #Platform: GigaVUE-FM and GigaVUE-OS-420 #Software version/file: 8.6.10/gvb86.01_07 #===
GigaVUE-FM and GigaVUE-OS-2404	#=== #Platform: GigaVUE-FM and GigaVUE-OS-2404 #Software version/file: 8.6.10/gvc86.11_04 #===

View Configuration Log Files

When a configuration file is applied to a physical node, the node returns response messages that are recorded in a log file. These log files are useful for identifying any errors if the configuration fails. The log file is a text field that contains the list of CLI commands applied in during the configuration and the results.

The log file for a configuration file applied to a node has the following format:

```
<config-filename>_<device-ip>_<date>_<time>.txt
```

For example, if the configuration log file is named GseriesConfig__10.10.10.10_20160621_203610.txt, the filename is interpreted as follows:

- Configuration filename: GseriesConfig.txt
- Applied to device IP: 10.10.10.10
- Date Applied: 20160521 (May 21, 2016)
- Time applied (FM server time): 203610

To view a log for a configuration file, do the following:

1.   On the right side of the top navigation bar, click ⚙.

2.   On the left navigation pane, select **System > Bulk Configuration**.

The Bulk Configuration Files page displays. An example is shown in the following figure.

3. Under **Configuration Logs**, click the Configuration Log File link for the configuration file log you want to view.

   The Configuration Logs page displays.

4. Select the configuration file, and then click **Download**. In the following figure, the file selected for download is 10.115.200.4__2010621_202902_10.115.200.4_20160521_203610.txt.

5. Open the downloaded configuration file in a text editor to review the contents.

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.

To access Images, click ⚙ on the top navigation bar. On the left navigation pane, 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. Figure 30 Image File Uploaded shows an image file for a Gigamon-HC2 node selected for uploading. To upload the file, click **OK**.

Figure 30 *Image File Uploaded*

After the uploading has completed, the image file is shown on the Internal Image Files page as shown in Figure 31 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.

	Images	Internal Image Files	External Servers			

Upload | Download | Delete

	Model	Filename	Version	Date	Size	⊕
☐	GIGAVUE-HC2	image-GigaVUE-OS-ppc-gv...	5.8.00	2019-11-15	607 MB	
☐	GIGAVUE-HC3	image-GigaVUE-OS-x86_6...	5.8.00	2019-11-17	620 MB	

|< | < | Go to page: 1 ▾ of 1 | > | >| | Total Records: **2**

Figure 31   *Internal Image Files Page*

External Servers

If you use an external server for the image files, the files used to upgrade the physical nodes or GigaVUE-FM to the latest software version are stored on an external Image servers. To access the External Servers page, go to **System > Images > External Servers**. The External Servers page has buttons used to set up and manage external image servers. These buttons are described in Table 4: 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-FM User's Guide*.

Table 4: Controls on External Servers Page

Controls	Description
Add	Allows you to specify where server images will be stored. The page is shown in External Servers. Clicking **Add** opens the Image Server Details dialog, where you specify: • **Alias** — A name to identify the server. • **Server Address** — The IP address of the server. • **Base Image Directory** — The base path where image files are stored. Images can be placed in subdirectories of this base directory. **NOTE:** Images can be updated using SCP, FTP or TFTP. • **Username and Password** —The user name and password that will be used to log into the server to store the image file. **NOTE:** A username and password are not required if using TFTP or SCP.
Edit	Select a server and click **Edit** to open the Image Server Details dialog, where you can modify the values specified

Controls	Description
	for the server. Same options are to be filled as noted for **Add**.
Delete	Select a server and click **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. • Multiple IP addresses can be selected for deletion.

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.

The Trust Store page lets you toggle between enabling and disabling security:

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

Use the `crypto` CLI command for adding the keys and certificates. Refer to the *GigaVUE-OS-CLI Reference Guide* for detailed information.

To access the Trust Store Page, click ⚙ 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 **OK**.

The certificate is added to the list view.

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 you have immediate visibility of events affecting node health.

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

To access the Notifications page, click ⚙.

Some of these events are detected by GigaVUE-FM and GigaVUE-OS H Series, TA Series, and G Series nodes, 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*.

Configure the Email Notifications

To configure the automatic email notifications:

1. On the right side of the top navigation bar, click ⚙.

2. On the left navigation pane, select **System > Notifications**

3. Select the required notification from the Notifications list table and click on **Actions**.

4. From the drop-down options click on ,

   - Configure- To set the automatic email notification to a single event. Enter the email addresses of the recipient or recipients in the Recipient(s) field and click on **Save**
   - Unconfigure- To remove the configuration for a specific recipient. Select the notification and click on the Unconfigure ,the configuration will be removed.

Controls	Description
Configure	Allows you to add recipients to the selected notification(s).
	Select a notification from the Description list and then click **Configure** to open the Configure Notification page, where you specify the recipient or recipients in the **Recipient (s)** field for that notification.
Unconfigure	Allows you to remove recipients from all selected notification(s). Click **Unconfigure** to delete the email notification for a recipient or recipients

Controls	Description
Notifications	The list of notifications that can be emailed to recipients as alerts. Table 5: GigaVUE-FM Notifications provides more information about these notifications. You can toggle notifications to display in descending or ascending order by clicking the label.
Email Recipients	Email addresses of the people to be notified. Each email address should be separated by a comma. You can toggle the order of the email recipients to display in descending or ascending order by clicking the label.

The following table describes all GigaVUE-FM notifications.

Table 5: GigaVUE-FM Notifications

Notifications	Description	Node Series
Apply Device Configuration	The configuration was applied to a managed node.	H Series
Authentication failure	A user login attempt failed on the indicated GigaVUE-FM and GigaVUE-OS G Series node.	G Series
AWS License Expire	The AWS license is close to expiry.	
Battery level changed	The battery charge in a G-TAP A-TX21 tap changed. Traps are generated at 25% increments as the available battery charge falls - 75%, 50%, and 25%. Traps are also generated when the available battery charge falls to 15% and the system closes the tap relays, falling back to passive mode.	A Series
BPS Failover	An inline bypass failover has occurred.	H Series
Buffer usage exceeds configured threshold notification is the Edge/Level Triggered Event	Buffer threshold can be set by going to **Node IP > Ports > Ports > Configure**. When using the drop down on Configure, you can set the buffer threshold for each port.	H Series
GigaSMART CPU Temperature	GigaSMART CPU temperature is above an acceptable level	H_Series
Cluster added	A cluster is added to the GigaVUE-FM instance.	H Series TA Series
Cluster creation failed	The cluster failed to form successfully.	H Series TA Series
Cluster creation started	The cluster creation has started.	H Series TA Series
Cluster image install finished	Installation of a new image on the indicated cluster of nodes began.	H Series TA Series
Cluster image install started	Installation of a new image on the indicated cluster of nodes began.	H Series TA Series
Cluster reboot finished	A reboot of the specified cluster completed.	H Series TA Series
Cluster reboot started	A reboot of the specified cluster was initiated.	H Series TA Series
Cluster Removed	The indicated cluster of nodes was removed from GigaVUE-FM.	H Series

Notifications	Description	Node Series
		TA Series
Cluster Updated	The indicated cluster of nodes was updated in GigaVUE-FM.	H Series TA Series
Configuration saved	The configuration of a node was saved to local storage (for example, by using the **write memory** command).	Any
CPU Temperature	The CPU temperature is above the threshold limit.	
CPU utilization is high	CPU utilization on the indicated node exceeded a hard-coded threshold.	Any
Device config backup	GigaVUE-FM performed a configuration backup for the indicated node(s).	GigaVUE-FM
Device config deleted	GigaVUE-FM deleted a backed-up configuration file for the indicated node(s).	GigaVUE-FM
Device config restore	GigaVUE-FM restored a configuration file to the indicated node(s).	GigaVUE-FM
Device Health changed	The health status of the device is changed based on the health status of ports, cards, fan tray, power module, memory utilization, and CPU utilization.	H Series TA Series
Device image install failed	Installation of a new image on the indicated node failed.	Any
Device image install finished	Installation of a new image on the indicated node completed at the indicated time.	Any
Device image install started	Installation of a new image on the specified node began at the indicated time.	Any
Device Operational mode changed	The cluster or standalone node is in Safe or Limited mode.	H Series
Device reboot finished	Reboot of the specified node began at the indicated time.	Any
Device reboot started	Reboot of the specified node finished at the indicated time.	Any
Disk space low	The available disk space on the indicated node fell below a hard-coded threshold.	Any
Evaluation License Expire	The evaluation license for GigaVUE-FM has expired.	GigaVUE-FM
Exhaust Temperature	Exhaust temperature is above the acceptable level.	H Series
Fabric Node Down	The GigaVUE-FM and GigaVUE-OS V Series node is down	
Fabric Node Reboot Failed	The GigaVUE-FM and GigaVUE-OS V Series node has failed to reboot.	
Fabric Node Rebooted	The GigaVUE-FM and GigaVUE-OS V Series node is rebooted.	
Fabric Node Replacement Launch Failed	The GigaVUE-FM and GigaVUE-OS V Series node upgrade failed to launch the new version.	
Fabric Node Replacement Launched	The new version of GigaVUE-FM and GigaVUE-OS V Series node is launched and the old version is removed.	
Fabric Node Restart Failed	The GigaVUE-FM and GigaVUE-OS V Series node failed to restart.	
Fabric Node Restarted	The GigaVUE-FM and GigaVUE-OS V Series node restarted.	
Fabric Node Unreachable	The GigaVUE-FM and GigaVUE-OS V Series node is unreachable.	
Fabric Node Up	The GigaVUE-FM and GigaVUE-OS V Series node is up.	
Fan tray changed	The Fan Tray in GigaVUE-FM and GigaVUE-OS H Series node was removed and reinserted.	H Series
Firmware changed	The system booted and detected that its firmware has been updated from the previous boot.	G Series

Notifications	Description	Node Series
FM image install Finished	Installation of the image file for GigaVUE-FM completed installation	GigaVUE-FM
FM Image Upgrade Completed	GigaVUE-FM was successfully upgraded from the installed image.	GigaVUE-FM
FM Image Upgrade Failed	Upgrade of GigaVUE-FM from the installed image failed.	GigaVUE-FM
FM Image Upgrade Started	An upgrade of GigaVUE-FM has started.	GigaVUE-FM
FM Server config backup	Backup of GigaVUE-FM has completed.	GigaVUE-FM
Gigamon Discovery	An email notification is sent to all configured destinations each time a new Gigamon discovery neighbor is discovered or Gigamon discovery information for an existing neighbor is changed or expired.	
GigaSMART Application Core Crash	A GigaSMART application core crash occurs due to a back trace trigger or a soft reset being initiated.	H_Series
GigaSMART CPU Utilization	GigaSMART CPU utilization is above the rising threshold.	H_Series
GigaSMART Packet Drop	A packet drop was detected by GigaSMART.	H_Series
GigaVUE-VM came online	The indicated GigaVUE-VM node came online and was detected by GigaVUE-FM.	GigaVUE-VM
GigaVUE-VM for Datacenter install completed	A bulk deploy of GigaVUE-VM nodes from GigaVUE-FM completed.	GigaVUE-VM
GigaVUE-VM for Datacenter install interrupted	A bulk deploy of GigaVUE-VM nodes was interrupted before the installation completed.	GigaVUE-VM
GigaVUE-VM for Datacenter install started	A bulk deploy of GigaVUE-VM nodes from GigaVUE-FM began.	GigaVUE-VM
GigaVUE-VM install completed	Installation of the indicated GigaVUE-VM node completed.	GigaVUE-VM
GigaVUE-VM install started	Installation of the indicated GigaVUE-VM node began.	GigaVUE-VM
GigaVUE-VM pinned to host	GigaVUE-VM was pinned to the host.	GigaVUE-VM
GigaVUE-VM unpinned from host	GigaVUE-VM is no longer pinned to the host.	GigaVUE-VM
Inline Bypass State Change	Forwarding state changed on an inline network.	H Series
Inline Tool Recovery	An inline tool recovered from failover.	H Series
Link state changed	An GigaVUE H Series node detected that either: • A port's link status has changed from up to down or vice-versa. • A port's speed has changed. **NOTE:** This trap is **not** sent when the Management port's link status changes. **NOTE:** The link state polling interval is 1 second. If a link state change is detected during the poll, a trap is generated.	H Series
Manual link added	A link was added to the Topology manually.	GigaVUE-FM
Manual link removed	A manually added link was removed from the Topology.	GigaVUE-FM
Manual link updated	A manually added link in the Topology was changed.	GigaVUE-FM

Notifications	Description	Node Series
Manual node added	A node was added to the Topology manually.	GigaVUE-FM
Manual node removed	A manually added node was removed from the Topology.	GigaVUE-FM
Manual node updated	A manually added node in the Topology was changed.	GigaVUE-FM
Module changed	A GigaVUE-FM and GigaVUE-OS node has detected a change in line card/module type from the last polling interval. This typically happens when a line card/module is pulled from a slot or inserted in an empty slot.	G Series H Series
Node added	A new physical node was added to GigaVUE-FM.	GigaVUE-FM
Node cold start	A GigaVUE-FM and GigaVUE-OS node restarted with a possible configuration change.	Any
Node failed to join cluster	The nodes failed to join the cluster.	
Node failed to remove from cluster	The nodes failed to leave the cluster.	
Node joined to cluster	The nodes joined the cluster.	
Node Link down	The link status on the indicated port changed from up to down.	Any
Node Link up	The link status on the indicated port changed from up to down.	Any
Node removed	A physical node was removed from GigaVUE-FM.	GigaVUE-FM
Node removed from cluster	The nodes are removed from the cluster.	
Node state changed	The status of a physical node in GigaVUE-FM changed from up to down (or vice-versa).	Any
Node warm start	A node restarted without changing its configuration.	Any
Packets dropped	A node detected dropped packets on the indicated port.	Any
Port link changed	A G Series node detected that a port's link status changed from up to down or vice-versa. **NOTE:** The **portlinkchange** trap is **not** sent when the Management port's link status changes. **NOTE:** The link state polling interval is 1 second. If a link state change is detected during the poll, a trap is generated.	G Series
Port Optics Temperature	Port optics temperature is above the acceptable level.	H Series
Port utilization below threshold Change	The utilization of the port is below the threshold limit.	
Power module changed	A G Series node detected either: • One of the two power supplies was powered on or off. • Power was lost or restored to one of the two power supplies.	G Series
Power source changed	The power source used by an A Series tap changed (for example, from Primary AC to Battery).	A Series
Process CPU utilization is high	An email notification is sent to all configured destinations each time the control card CPU utilization exceeds the pre-configured process threshold values.	H Series TA Series
Process Memory utilization is high	An email notification is sent to all configured destinations each time the control card memory utilization exceeds the pre-configured process threshold	H Series TA Series

Notifications	Description	Node Series
	values.	
System CPU utilization is high	An email notification is sent to all configured destinations each time the control card CPU utilization exceeds the pre-configured system threshold values.	H Series TA Series
System Memory utilization is high	An email notification is sent to all configured destinations each time the control card memory utilization exceeds the pre-configured system threshold values.	H Series TA Series
Resource Extreme High Usage Problem Cleared	An email notification is sent to all configured destinations each time the disk usage percentage falls below the extreme high usage threshold.	GigaVUE-FM
Resource Extreme High Usage Problem Detected	An email notification is sent to all configured destinations each time the disk usage percentage exceeds the extreme high usage threshold.	GigaVUE-FM
Resource High Usage Problem Cleared	An email notification is sent to all configured destinations each time the CPU and memory utilization falls below the high usage threshold.	GigaVUE-FM
Resource High Usage Problem Detected	An email notification is sent to all configured destinations each time the CPU and memory utilization exceeds the high usage threshold over the period of 2 minutes.	GigaVUE-FM
Scheduled task [%s] created	Any new task that is created under **All Nodes > Inventory > More Actions**, will trigger a notification.	H Series
Secondary Flash Boot	A boot partition next operation has occurred.	GigaVUE-FM
Service Status Down Detected	A service monitored by GigaVUE-FM is down.	GigaVUE-FM
Service Status Up Detected	A service monitored by GigaVUE-FM is up.	GigaVUE-FM
Stack image install finished	Install complete of a new image on the indicated stack of G Series nodes.	G Series
Stack image install started	Install start of a new image on the indicated stack of G Series nodes.	G Series
Stack reboot finished	A reboot of the specified stack of G Series nodes completed.	G Series
Stack reboot started	A reboot of the specified stack of G Series nodes was initiated.	G Series
Switch CPU Temperature	The switch CPU temperature is over the threshold limit.	
System Reset	A node has started, either as a result of cycling the power or a soft reset initiated by the **reload** command (H Series) or the **reset system** command (G Series).	Any
System Reset by Watchdog timer	A node detected that the watchdog monitor had to reset a failed process on the system.	H Series
TAP Relay changed	A G Series node detected a GigaTAP-Tx module's relays switched from active to passive or passive to active, as a result of the **config port-params taptx** command.	G Series
Thresholds exceeded	The utilization threshold configured for a port was exceeded: • **GigaVUE-FM and GigaVUE-OS G Series** – The threshold configured with **config port-alarm** was exceeded for five consecutive seconds. • **GigaVUE-FM and GigaVUE-OS H Series** – The threshold configured with **port <Port list> alarm utilization-threshold <percentage>** was exceeded for six consecutive seconds.	G Series H Series

Notifications	Description	Node Series
Transmit / Receive error	G Series node received one of the following physical errors on a data port: • Undersize error • Fragment • Jabber • CRC or Alignment errors • Unknown errors	G Series
Unexpected shutdown	A H Series node shut down unexpectedly (for example, because power was lost and subsequently restored).	H Series
User authentication failed	A user login has failed on a H Series node.	H Series
VM Instance Running	A VM instance is running	
VM Instance Stopped	A VM instance is stopped.	
VM Instance Terminated	A VM instance is terminated	
Vmm Error	An error related to VMware ESXi inventory occurred.	GigaVUE-VM

Email Servers

The Email Servers page displays email hosts currently configured used for to send notifications and the email address for the From filed in email notifications.

To access the Email Servers page, click ⚙ on the top navigation bar. On the left navigation pane, select **System > Email Servers**.

Figure 32   *Setting Email Addresses for Alarm/Event Notifications*

Click the Configure button on the Email Server page to open the configuration page. Table 6: Configure Email Server Fields describes the field on the Configure Email Server page.

Table 6: Configure Email Server Fields

Field	Description
Enable SMTP Authentication	The user's credentials are used for SMTP authentication when this option is select. 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 you want to have show up in the From field of the notification emails.

Licenses

The **Licenses** page lets you review and apply licenses for the following components:

- GigaVUE-FM and GigaVUE-VM nodes using the **Fabric Manager/Cloud** tab
- Devices managed by GigaVUE-FM using the **Node View** tab
- Card assignments for the licenses can be viewed in the **Activation View** tab

This section describes how to use the GigaVUE-FM licensing interface to manage your GigaVUE-FM licenses and your node-application license assignments.

In this section:

- Activate a GigaVUE-FM License
- Add a GigaVUE-FM License
- Delete a GigaVUE-FM License
- Activate a SMART License
- Assign a Node License

> NOTE: For information about GigaVUE-FM licensing options, refer to GigaVUE-FM Licensing. For information about GigaSMART licensing options, refer to GigaSMART Licensing.

GigaVUE-FM License

To access the GigaVUE-FM license(s) page:

Starting from the top navigation, click ⚙System > Licenses > Fabric Manager/Cloud Licenses.

You can activate and delete GigaVUE-FM licenses from this page.

Figure 33 *GigaVUE-FM Licenses Page*

NOTE: If you use the GigaVUE-FM CLI command **show license**, the command may show an active Prime license as unrecognized.

Activate a GigaVUE-FM License

To activate the license, do the following:

1. Get the MAC address for your instance of GigaVUE-FM. To get the MAC address, click the gear icon ⚙ on right side of the top navigation bar. On the left navigation pane, click **About**. The address is in the **MAC Address** field. Note the address for the next steps.

2. Go to **System > Licenses > Fabric Manager/Cloud Licenses** and click **Activate License**.

3. Follow the instructions on the screen to activate your licenses. In these next steps you will:

    • Download the fabric inventory (.json) file from GigaVUE-FM.

- Go to the Gigamon license portal and find license you want to activate and complete the three screens to activate your license. On the second screen, you will be prompted to upload the fabric inventory (.json) file.
- After activating the license, record the license key or keys.
- Return to GigaVUE-FM and add the additional GigaVUE-FM licenses.

> NOTE: To access the Gigamon license portal, directly, you can go to Licensing Portal.

Figure 34 *Gigamon Licensing Portal*

4. Use the filter options on the Gigamon license portal to find the license

   To find already purchased but inactive licenses, select "inactive" under the **View by** filter, and then enter any known value in any of the filters at the top of each column, such as the EID or SKU.

   The last three columns are frozen so they will always be visible even when you resize the page: Quantity, Status, and License Key.

   > NOTE: To view licenses for GigaVUE-FM and GigaVUE-OS TA Series port enablement or clustering, or for GigaSMART licenses for GigaVUE-FM and GigaVUE-OS H Series nodes, click the **Licenses > Node View** tab. You can also still log in to the H-VUE or CLI for that node to apply the licenses.

5. After you have obtained the license key, follow the steps described in Add a GigaVUE-FM License.

Add a GigaVUE-FM License

To add a license to GigaVUE-FM, do the following:

1. Activate a license key as described in Activate a GigaVUE-FM License.

2. In GigaVUE-FM, click the gear icon ⚙ on right side of the top navigation bar.

3. Go to **System > Licenses > Fabric Manager/Cloud**.

4. Click **Activate License**.

5. Click the "Add FM License" link. The Add License page is displayed.

6. Enter the license key in the License Key field.

   To add more than one license, click the **+** button to add additional License Key field.

7. Click **Save**.

   The license and its description is added to the Licenses page.

Delete a GigaVUE-FM License

To delete a license, do the following:

1. In GigaVUE-FM, click the gear icon ⚙ on right side of the top navigation bar.

2. Go to **System > Licenses > Fabric Manager/Cloud**.

3. On the Licenses page, select the license key for the license you want to delete.

4. Click **Delete** to remove the license.

Activate a SMART License

To activate or find the license or licenses, do the following:

1. In GigaVUE-FM, click the gear icon ⚙ on right side of the top navigation bar.

2. Go to **System > Licenses > Activation View**.

   You can use this page to access the Gigamon license portal where you can activate licenses. You can then use this page to assign the active licenses to the devices

3. Click **Activate Licenses > With License Portal**:

4. Follow the instructions on the screen to activate your licenses.

   In these next steps you will:
   - Download the fabric inventory (.json) file from GigaVUE-FM.
   - Go to the Gigamon license portal and find license you want to activate and complete the three screens to activate your license. On the second screen, you will be prompted to upload the fabric inventory (.json) file.
   - After activating the license, you can download the license (.lic) files or record the license key or keys.
   - Return to GigaVUE-FM to assign the licenses to specific nodes.

5. Click **Download Inventory** to download your GigaVUE-FM inventory (in a *.json file). Note the location. You will upload this file to the license portal in a subsequent step.

6. Click the **Gigamon Licensing portal** link).

> NOTE: To access the Gigamon license portal, directly, you can go to the Licensing Portal at https://licensing.gigamon.com.

Figure 35   *Filtering in Gigamon Licensing Portal*

7. Use the filter options on the Gigamon license portal to find the license

Filter for the licenses you wish to activate using the **View by** options and entering a value in any of the filter boxes at the top of each column. For example:

To find purchased but inactive licenses, for example, select "inactive" under the **View by** filter, and then enter any known value in any of the filters at the top of each column, such as the EID or SKU.

The last three columns are frozen so they will always be visible even when you resize the page: Quantity, Status, and License Key.

8. Click the **Activate** link in the Lic. Key the license activation file (.lic). You can follow the on-screen instruction to complete the forms.

Activation Method:
-   When asked if you use GigaVUE-FM, select **Yes**. The option to upload your Fabric Inventory will appear.
-   Click **Choose File** to upload the Fabric Inventory (.json) file that you just downloaded from GigaVUE-FM.
-   Details about the uploaded file will appear. Click **Continue**.

Activation Quantity:
Complete the relevant fields in each row. When the form is complete, click Review to proceed.
-   **Type**: select Node-Locked or Floating
    -   *Node-Locked* is for licenses that are locked to a specific node. All pre-5.7 licenses are node-locked.
    -   *Floating* licenses allow you to move licenses from one node to another as needed to support your network configuration. Floating licenses are newly available with GigaVUE-FM and GigaVUE-OS-5.7.
-   **Version**: The portal supports licenses that were purchased pre-5.7 and post-5.7.
-   **Device Locked to**:
    -   If your license is locked to a device, enter the device IP here.
    -   If your license is floating, enter the Challenge MAC address for your GigaVUE-FM here.
-   **Qty**: specify the quantity of this license that you wish to activate
-   **Action**: Use the +/- action buttons to add or remove items.

Review:

- Review the licenses you are about to activate.
- When ready, click Activate to complete the activation.
- When done, click All Licenses to return to the main view of the licensing portal.

Licenses:
- From the Licenses main view, click the **Download** link under the Lic. Key column on the row of an activated license to download the active license.
- **Limitation**: This license file download only works for post-GigaVUE-FM-5.7 licenses.

9. Return to GigaVUE-FM, log in as an administrator, and return to the license activation screen.

- Click the gear icon, then navigate to **System > Licenses Activation View > With License Portal** and complete the activation by importing the downloaded License (.lic) files.
- Or, navigate to **System > Licenses Activation View > With License Key** and complete the activation by entering the license key.

10. Click **Import license** (.lic) and use your file explorer to find and open the license file.

> NOTE: Please contact technical support team for assistance.

Assign a Node License

To assign a license to the device:

1. Generate the license as described in section Activate a SMART License.

2. In GigaVUE-FM, click the gear icon in the top navigation, then select **System > Licenses > Activation View.**

3. Click the quantity link in the **# of Available Seats** column. The Available Seats page appears.

4. Select the required Cluster ID and Slot ID.

5. Click **Assign**. Repeat this for each assignment.

6. Click **Save.**

> **NOTE:** You can also use the **Import CSV** option on this page to perform a bulk assignment. To learn the syntax required, download the example CSV file from inside the Import window:

To view node assignments, go to the Node View under **Licenses > Node View**.

Node View

To access the node license(s) page, select **System > Licenses > Node View**. This is a view only page showing the node and cluster details along with the license expiry information.

> NOTE: When you login to GigaVUE-FM, a notification is displayed on the top of the page with license expiry details for the nodes which have validity less than 30 days. Click the **Go To Licenses** option to go to the **Licenses** page.

The **Expires** option indicates the status of the license:

- **Never**: License is a life time license and will never expire
- **Expired:** License has already expired
- **Exact date:** Date when the license will expire (for example Oct 12, 2019)

Licenses   Fabric Manager/Cloud   Node View   Activation View

Cluster ID	Host name	Serial# (chassis or card)	Slot ID	Features	Expires
10.115.39.243	FMHC1-39...	1D60-0329	1	Add Header	Never
10.115.39.243	FMHC1-39...	1D60-0329	1	Adaptive Packet Filtering	Never
10.115.39.243	FMHC1-39...	1D60-0329	1	Application Session Filtering	Never
10.115.39.243	FMHC1-39...	1D60-0329	1	De-duplication	Never
10.115.39.243	FMHC1-39...	1D60-0329	1	ERSPAN	Never
10.115.39.243	FMHC1-39...	1D60-0329	1	Flow Sampling	Never
10.115.39.243	FMHC1-39...	1D60-0329	1	Header Stripping	Never
10.115.39.243	FMHC1-39...	1D60-0329	1	Masking	Never

|<   <   Go to page: 1 ▼ of **16**   >   >| Total Records: **125**

Figure 36   *Node Licenses Page*

> NOTE: Refer to the Release Notes v5.7.00 and *GigaVUE-FM User's Guide* for additional information about the new floating license options.

System Logs

You can generate log files that contain information about the system. Gigamon support can use these files for root cause analysis. Click the **Download** button to download the compressed files.

To access Logs, click the gear icon ⚙ on the top navigation bar. On the left navigation pane, select **System > Logs**.

Create a Log file

To create a log file that Gigamon can use for analysis, do the following:

1. Select **System > Logs**.

   The Logs page displays, which shows a list of log files.

Logs

	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 37   *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 **Delete**.

Storage Management

The Storage Management page shows the available and used storage space shown under /var file system of the GigaVUE-FM appliance. Figure 38Storage Management Page shows that 2588MB of storage is used and 25750MB is available only 9 percent full. This information is pulled from the same file system irrespective of the virtual environment where the appliance is installed.

This information is useful when collecting NetFlow records for reports, and audit logs because the appliance may run out of storage and there might be a degradation in performance. Generally, if everything is functioning well, the NetFlow records would be transferred to /config file system and this issue may never arise.

GigaVUE-FM Storage Management allows you to define how the stored logs are managed. You can specify a schedule for purging old device logs. You can also specify an SFTP server to export the log records prior to purging. Storage Management is used for all storage settings, including device logs, alarm/event notifications, and statistics. Refer to Alarms and Events.

To access Storage Management, click ⚙ on the top navigation bar. On the left navigation pane, select **System > Storage Management**.

Figure 38 *Storage Management Page*

If needed, you can free the used storage older than a specified date by doing the following:

1. On the right side of the top navigation bar, click ⚙.

2. Navigate to **System > Storage Management**. The Storage Management page is displayed.

3. Click **Edit** to edit the settings. The Edit Storage Management page appears.

4. Specify the Storage Management settings for each type of record:

Setting		Description
Statistics		
	Delete stats older than	Click the Calendar icon to select a date. This will specify a cut off date for deleting statistics. Statistics prior to the specified date will be deleted, immediately, when you click **OK**. **Important**: If a date is specified, the records will be

Setting	Description
	immediately and permanently deleted from the database when you click **OK**.
Export Records To	
Remote directory	If the "automatically export" check box is selected under Alarm/Events or Device Logs, the records will be exported to a CSV file at the specified interval.
	Use this field to specify the ftp/sftp location to send the export records.
	For example:
	`sftp://username@121.0.0.1/path/directory`
Password	Specify a password for accessing the remote server.
Alarm/Events	
Automatically delete records period	Specify how often to delete Alarm/Event records. Options are 7 days, 30 days, 60 days or custom (in days). (7 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 Alarms/Events page.
	Click the **Automatically export** check box to enable exporting the records to the specified location on a periodic basis. (It is enabled by default.) When selected, records will be exported once before the immediate purge, and then again in the number of days specified in the records period. Records will continue to be exported once every set period of days.
Device Logs	
Automatically delete records period	Specify how often to delete Device Log records. Options are 7 days, 30 days, 60 days or custom (in days). (7 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.
	Click the **Automatically export** check box to enable exporting the records to the specified location on a periodic basis. (It is enabled by default.) When selected, records will be exported once before the immediate purge, and then again in the number of days specified in the records period. Records will continue to be exported once every set period of days.

a. To permanently remove the records from the database based on the specified settings, click OK.

> **Caution**: There is no undo. Statistics records prior to the date specified will be immediately and permanently deleted from the database when you click **OK**. Alarm/Event records will be permanently deleted from the database at the specified scheduled interval.

SNMP Traps

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

- • SNMP Traps
- • SNMP Throttling
- • Port Utilization Threshold

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 that GigaVUE-FM instance. When the GigaVUE-FM instance starts, the following SNMP traps are enabled by default (for all the devices):

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

Starting in software version 5.10.01, traffic health state of the ports and devices is computed based on the SNMP traps. Therefore, in addition to the above traps, the following SNMP traps which are used to determine the health status of the ports and devices are also enabled by default:

- Packet Drop
- GigaSMART Packet Drop
- Packet Error
- Port Utilization
- Low Port Utilization
- GigaSMART Port Utilization
- GigaSMART Port Low Utilization
- System Memory Threshold
- Process Memory Threshold

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.

> **NOTE:**
> - 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

To access SNMP Traps, click ⚙ on the top navigation bar. On the left navigation pane, select **System > SNMP Traps**.

Figure 39 *SNMP Traps Page*

The SNMP Traps page allows you to configure the following:

- Enable/disable all the traps for all the devices using the **Enable All** and **Disable All** options.
- Enable/disable specific traps for all the devices using the **Enable** and **Disable** options for each of the traps.

- Retain device settings for all the traps using the **Retain Device Settings for All Traps** option.

To configure the SNMP traps:

1. Click the **Edit** button on the top right corner.

2. Configure the required setting. For example, to retain the individual device level setting for all traps, select the **Retain Device Setting for All Traps** checkbox.

> **NOTE:** You can also retain the device settings for specific traps by selecting the **Retain Device Setting** checkbox against the required traps.

3. Click **Save**

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**.

   > **NOTE:** The **SNMP Throttling** option that was available under **Thresholds** is now included under **SNMP Traps**.

3. The **SNMP Throttling** page is displayed.

Figure 40 *SNMP Throttle Settings Page*

4. Click **Edit** to configure the following throttling settings for the traps:

- **Disable Throttle**: Allows you to disable the throttle for the required traps. If you select the **Disable Throttle** checkbox in the header, then throttling is disabled for all the traps.

- **Interval**: Allows you to configure the throttling interval. The throttling interval is configured by default for some of the traps (which is displayed in the page).

- **Report Threshold**: Allows you to 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.

5. Click **Save**.

> NOTE: SNMP throttling is available for all traps for all devices running version 5.5 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		Events to the particular cluster will be throttled
Summary	Dashboard, Physical nodes	2 events per 5 second	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. Click ⚙ on the top navigation bar.
2. On the left navigation pane, select **System > SNMP Traps** > **Port Utilization Threshold**.
3. Click **Create**

4. Enter the upper and lower threshold values and click **Save.**

5. Click **Edit** to edit the port utilization threshold values.
6. Click **Apply All** to apply the configuration to all the devices. The configured port utilization threshold values will be applied for devices running software version 5.10 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.

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
- Configure GigaVUE-FM High Availability
- Failover Mechanism
- Troubleshoot GigaVUE-FM High Availability Issues
- Upgrade GigaVUE-FM Virtual Machines in HA Environment (version 5.8.xx to 5.9)

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 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.

Get Started

To configure the GigaVUE-FM HA feature, you must have access to three authenticated GigaVUE-FM instances that reside on a trusted network. All three GigaVUE-FM instances must run the same software version. The ports in the GigaVUE-FM instances must be up and must be assigned IPv4 addresses. You can also choose to assign DNS host names.

> NOTE: You can configure the GigaVUE-FM HA feature only if you have administrative privileges.

Hostname Setups

The three GigaVUE-FM instances are not required to be in the same subnet, but still must be able to communicate with each other. However, if you plan to configure Virtual IP, the three GigaVUE-FM instances must be in the same subnet.

In addition, ensure that the three instances have uniques host names. You must be able to ping a GigaVUE-FM instance from the other two instances using the hostname or the IP address.

To add a GigaVUE-FM instance to a GigaVUE-FM HA group, one of the following conditions must be met:

- The host names of the GigaVUE-FM instances must be resolvable through a DNS server.

- The host names of the GigaVUE-FM instances must be mapped to the respective IP addresses. Refer to the *"fmctl"* section in the *GigaVUE-FM Installation and Migration Guide*.
- The IP addresses of the GigaVUE-FM instances must be reachable to each other.

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-FM and GigaVUE-OS-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

Rules and Notes

Keep in mind the following rules and notes when you configure the GigaVUE-FM HA feature:

- Load-balancing in an Active-Active model is not supported. In the GigaVUE-FM HA group, only one instance is active at a given time.
- You can deploy the three GigaVUE-FM HA virtual machines on a WAN link with a maximum latency of 200 ms.
- Sharing of a Virtual IP Address by the three GigaVUE-FM HA virtual machines is not supported.
- If you plan to configure Virtual IP, the three GigaVUE-FM instances must be in the same subnet and the Virtual IP addresses must be static in the same subnet. Only one Virtual IP address is allowed per direction (northbound or southbound).
- Upgrading to software version 5.8.00 using the GUI or CLI of the previous version is not supported. Also, orchestrated upgrade from active GigaVUE-FM is not supported. You must disassemble or break down the HA group and then upgrade each of the GigaVUE-FM instances separately. For more information, refer to Upgrade GigaVUE-FM Virtual Machines in HA Environment (version 5.8.xx to 5.9).

  > NOTE: When you break down the HA group, the three GigaVUE-FM instances will be restored to the default configuration database and their existing database will be deleted.

- No support for IPv6 addresses, or GigaVUE-FM behind a NAT.
- You cannot add a GigaVUE-FM Hardware Appliance and a GigaVUE-FM virtual machine in the same HA group.

- The three GigaVUE-FM instances 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.

Configure GigaVUE-FM High Availability

To enable GigaVUE-FM HA, create a HA group with the three GigaVUE-FM instances.

Before you proceed to create the HA group, ensure that you meet the following prerequisites:

- You have the IP addresses or DNS names of the three GigaVUE-FM instances.
- All the three GigaVUE-FM instances are running the same software versions.

To create a HA group:

1. Log in to one of the GigaVUE-FM instance. This instance will be the Active instance after you have created the HA group.
2. On the top navigation bar, click ⚙.
3. From the left navigation pane, select **High Availability**.
4. Click **Create**. The High Availability wizard appears.
5. In the **Group Name** field, enter a unique name for the HA group, and then click **Continue**.
6. In the Define Virtual IP Addresses VIP page, you can choose to configure the Virtual IP addresses to minimize service interruptions upon failovers. Complete the following fields:

   a. In the **VIP Name** field, enter a unique name.

   b. In the **Type** field, select the **Direct** option to configure direct Virtual IP address.

   c. In the **Direction** field, select one of the following options:

      - **Northbound**—The Virtual IP address will be configured on the northbound facing GigaVUE-FM.
      - **Southbound**—The Virtual IP address will be configured on the southbound facing GigaVUE-FM.
      - **Dualbound**—The Virtual IP address will be configured for both northbound and southbound directions. If you choose this option, you cannot configure another Virtual IP address.

   d. From the **Interface** drop-down list, select the required management interface.

   e. Enter the IP address and the subnet mask in the respective fields.

   f. You can choose to configure another Virtual IP address or click **Continue**.

Figure 41 *Configure Virtual IP Address*

7. Click **Continue**. The Add Devices section appears with the first GigaVUE-FM instance (the instance that you are logged-in) added to the HA group. The details of the instance such as **Status**, **IP Address**, **Software Version**, **System Uptime**, and **Reachable** status appear as shown in Figure 42 Add GigaVUE-FM Instances to the HA Group.

Figure 42 *Add GigaVUE-FM Instances to the HA Group*

8. Click "**+**" to add the second GigaVUE-FM instance.

9. In the **Add FM Instance** dialog box, enter the following details for the second GigaVUE-FM instance:

    • IP Address—IP Address or Domain Name Server (DNS) name of the second GigaVUE-FM instance

- Username
- Password
- Entity ID—A unique identifier for the GigaVUE-FM nodes that are part of the HA group.

10. Click **Add**. The second GigaVUE-FM instance is added to the HA group.

11. Click "**+**" to add the third GigaVUE-FM instance. Refer to Step 9 for details.

12. Click **Add**. The third GigaVUE-FM instance is added to the HA group.

13. Click **Continue**. You can view information such as the Group Name and details of the three GigaVUE-FM instances that are added.

14. Click **Submit** to create the GigaVUE-FM HA Group. GigaVUE-FM takes some time to create the group. Refer to Figure 43 GigaVUE-FM HA Group Created.

Figure 43 *GigaVUE-FM HA Group Created*

Important Recommendations

- Do not close the GigaVUE-FM tab until the GigaVUE-FM HA group is created. Open a new tab to simultaneously perform other tasks.

- Do not make any changes to the two standby instances while creating the HA group. This is because, the database of the two standby GigaVUE-FM instances are overwritten with the contents of the active GigaVUE-FM instance's database after the formation of the HA group.

The first instance becomes the active instance of the HA group. The second and third GigaVUE-FM instances are in standby mode. When the active instance of the GigaVUE-FM fails, one of the other two instances becomes the active instance. You can view the health state of the HA group after the creation of the GigaVUE-FM HA group.

A standby instance allows you to:

- reboot the other standby instances or active instance in case of failures.
- view the High Availability page and the Events page.

> NOTE: A standby instance does not allow you to edit or remove any other instance from the HA group.

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.

1. On the top navigation bar, click ⚙.

2. From the left navigation pane, 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 44 Disabling GigaVUE-FM Instance.

Figure 44 *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 top navigation bar, click ⚙.

3. From the left navigation pane, select **High Availability**.

4. Click the ellipsis on the GigaVUE-FM instance widget in the High Availability page.

5. 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 not only disassembles the GigaVUE-FM HA group, but will also revert the standalone GigaVUE-FM instances to their default database. All managed devices will be removed and GigaVUE-FM settings will be reset to the default values.

GigaVUE-FM High Availability States

The GigaVUE-FM HA state depends on the status of the three GigaVUE-FM instances. The following table lists the various states of the GigaVUE-FM HA group. You can view the HA group state from **Administration** > **High Availability** in the GigaVUE-FM GUI.

Table 7: High Availability States

State	Number of GigaVUE-FM Instances	Description
Healthy	Three GigaVUE-FM instances are up and running	One GigaVUE-FM instance is in active state. Other two instances are in standby state.
At Risk	Two GigaVUE-FM instances are up and running	One GigaVUE-FM instance is in active state. Another GigaVUE-FM instance is in standby state. The third GigaVUE-FM instance has either not joined the HA group or has left the HA group.
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 45   *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.

Refer to the following table for the various failover reasons:

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 top navigation bar, click ⚙, and then from the left navigation pane, 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. • The GigaVUE-FM GUI of the standby instances will only have the Events and High Availability page.
What happens to the GigaVUE-FM instances that were previously in standby state?	• One of the standby GigaVUE-FM instances changes to the active state • The other standby GigaVUE-FM instance remains in the standby state.
What happens to the embedded devices when a new Active instance takes over?	There are no changes to the devices except that they are being managed by the new active GigaVUE-FM instance.
How do you trigger a failover?	Click on the 'Reboot' option on the current active GigaVUE-FM instance to trigger a failover.

Troubleshoot GigaVUE-FM High Availability Issues

Use the following table to troubleshoot issues that you might encounter while working with the HA feature.

Problem	Solution
Unable to add a license to GigaVUE-FM HA group after a failover **Reason:** Using the MAC Address in the **About** page to generate the license	Always use the **Challenge MAC Address** in the **Licenses** page of the active GigaVUE-FM instance to generate licenses. Add the licenses to the HA group.

Problem	Solution
Unable to join the GigaVUE-FM HA group after changing the password **Reason:** Not logging out of GigaVUE-FM after changing the password and before joining the HA group	Always logout of GigaVUE-FM after changing the password and login again with the new password before joining the HA group.

Upgrade GigaVUE-FM Virtual Machines in HA Environment (version 5.8.xx to 5.9)

When you try to upgrade the GigaVUE-FM instances that are part of the HA group, it will trigger the orchestrated upgrade, however, the orchestrated upgrade is not supported from version 5.8.xx to 5.9. You must disassemble the HA group and then upgrade each of the GigaVUE-FM instances separately. To do this, perform the following tasks:

1. Take a backup of the GigaVUE-FM instance that is in the active state.

   > NOTE: This backup will not have the HA configuration and statistics.

2. Disassemble the HA group.

   > NOTE: When you disassemble the HA group, the three GigaVUE-FM instances will be restored to the default configuration database and their existing database will be deleted.

3. Upgrade the two GigaVUE-FM instances that you want to set as the standby instances. For instructions, refer to the *GigaVUE-FM Installation and Migration Guide*.

4. Restore the backed-up configurations on the GigaVUE-FM instance that you want to set as the active instance, and then upgrade the instance.

   > NOTE: Ensure to restore the configurations before you upgrade the instance. Also, you must reinstall the Prime license to reconfigure the HA group.

5. Reconfigure the HA group.

Upgrade GigaVUE-FM Virtual Machines in HA Environment (version 5.9.xx to 5.10)

Orchestrated upgrade is not supported from version 5.9.xx to 5.10. Therefore, use the `fmctl` command to upgrade each of the GigaVUE-FM instances in the HA group. Refer to the following steps:

1. Upgrade the first standby GigaVUE-FM instance (GigaVUE-FM 2) using the following commands:

   `fmctl image fetch <image-url-path>`
   `fmctl image install <image-name> location <next-boot-location-id>`
   `fmctl image boot <next-boot-location-id>`

   The first standby GigaVUE-FM instance is upgraded to 5.10.00 version. However, GigaVUE-FM GUI will not be up for this standby instance.

2. Upgrade the second standby GigaVUE-FM instance (GigaVUE-FM 3) using the same commands. The second standby instance is upgraded to 5.10.00 version, but GigaVUE-FM GUI will not be up for this standby instance, as well.

3. Upgrade the active GigaVUE-FM instance (GigaVUE-FM 1) using the same commands. The active instance is upgraded to 5.10.00 version and the GigaVUE-FM GUI will be up for this instance.

4. Reboot the first and the second standby (GigaVUE-FM 2 and GigaVUE-FM 3) instances for the GigaVUE-FM GUI to come up:

   `Go to fm cli`
   `sudo su`
   `reboot`

Administer GigaVUE Nodes

Featured topics:

- Introducing the GigaVUE Nodes
- Access Nodes From GigaVUE-FM
- GigaVUE-OS Overview
- Get Started with GigaVUE-FM and GigaVUE-OS Nodes
- Configure Security Options
- License GigaVUE-FM and GigaVUE-OS 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 H 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-FM and GigaVUE-OS H Series and TA Series
- GigaVUE H Series Features and Benefits

About the GigaVUE-FM and GigaVUE-OS H Series and TA Series

The GigaVUE-FM and GigaVUE-OS H 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 (H-VUE) 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-FM and GigaVUE-OS H Series and TA Series include the following models that run GigaVUE-OS:

- GigaVUE-HC1

- GigaVUE-HC2
- GigaVUE-HC3
- GigaVUE-FM and GigaVUE-OS-TA10
- GigaVUE-FM and GigaVUE-OS-TA40
- GigaVUE-FM and GigaVUE-OS-TA100
- GigaVUE-FM and GigaVUE-OS-TA100-CXP
- GigaVUE-FM and GigaVUE-OS-TA200
- Certified Traffic Aggregation White Box

NOTE: This document describes how to configure and operate the GigaVUE-OS for GigaVUE-FM and GigaVUE-OS H Series and TA Series nodes.

GigaVUE-HC1	• **1RU Footprint** • **Built-in GigaSMART functionality** • **Standard GigaVUE-OS CLI and H-VUE GUI** • **Cluster with GigaVUE-FM and GigaVUE-OS H Series and GigaVUE-FM and GigaVUE-OS 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 H-VUE GUI** • **Cluster with GigaVUE-FM and GigaVUE-OS H Series and**	

	GigaVUE-FM and GigaVUE-OS 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 H-VUE GUI** • **Supports all GigaVUE-HC3 Modules** • **Cluster with GigaVUE-FM and GigaVUE-OS H Series and GigaVUE-FM and GigaVUE-OS TA Series Nodes**	
GigaVUE-FM and GigaVUE-OS-TA10	• **1RU Footprint** • **Flexible 10Gb/40Gb Modes for 40Gb Ports** • **Standard GigaVUE-OS CLI and H-VUE GUI** • **Cluster with GigaVUE-FM and GigaVUE-OS H Series and GigaVUE-FM and GigaVUE-OS TA Series Nodes**	
GigaVUE-FM and GigaVUE-OS-TA40	• **1RU Footprint** • **Flexible 10Gb/40Gb Modes for 40Gb**	

	Ports • Standard GigaVUE-OS CLI and H-VUE GUI • Cluster with GigaVUE-FM and GigaVUE-OS H Series and GigaVUE-FM and GigaVUE-OS TA Series Nodes	
GigaVUE-FM and GigaVUE-OS-TA100	• 1RU Footprint • 32 x 100Gb/40Gb Ports • Standard GigaVUE-OS CLI and H-VUE GUI • Cluster with GigaVUE-FM and GigaVUE-OS H Series and GigaVUE-FM and GigaVUE-OS TA Series Nodes	
GigaVUE-FM and GigaVUE-OS-TA100 CXP	• 1RU Footprint • 20 100Gb CXP Ports, 8 100Gb QSFP28 Ports • Standard GigaVUE-OS CLI and H-VUE GUI	
GigaVUE-FM and GigaVUE-OS-TA200	• 2RU Footprint • 64x 100Gb/40Gb Ports • Standard GigaVUE-OS CLI and H-VUE GUI • Cluster with GigaVUE-FM and GigaVUE-OS H	

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

Notes on TA Series Nodes

- A twenty-four (24) port GigaVUE-FM and GigaVUE-OS-TA10 version, called the GigaVUE-FM and GigaVUE-OS-TA10A is available with only the first 24 1Gb/10Gb ports enabled. A license is needed to expand a GigaVUE-FM and GigaVUE-OS-TA10A to include all 48 1Gb/10Gb ports as well as the four (4) 40Gb ports.
- On the GigaVUE-FM and GigaVUE-OS-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-FM and GigaVUE-OS-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-FM and GigaVUE-OS-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 H Series Features and Benefits

Capable of port-to-port full line rate performance with minimal packet latency, the GigaVUE-FM and GigaVUE-OS H Series uses patented Flow Mapping® techniques to aggregate, replicate, and direct traffic flows, providing dynamic connectivity for 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-FM and GigaVUE-OS H 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-FM and GigaVUE-OS 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 1 The Gigamon Visibility Platform summarizes these features.

Figure 1   *The Gigamon Visibility Platform*

Features and Benefits

The following table lists the major features and benefits of the GigaVUE-FM and GigaVUE-OS H Series:

Benefit	Descriptions
Web-Based Management	Manage the operations of the GigaVUE-FM and GigaVUE-OS H Series node using H-VUE, Gigamon's simple but powerful Web-based interface for the GigaVUE-FM and GigaVUE-OS H Series nodes. H-VUE makes it easy to set up flow mapping, allowing you to see at a glance which network ports are delivering which packets to individual tool ports. Reconfigure flow mapping on the fly, selecting the packets you need when you need them.
CLI Management	Configure the operations of the GigaVUE-FM and GigaVUE-OS H 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.

Benefit	Descriptions
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-FM and GigaVUE-OS H Series node evolves with network speeds, including line cards with 40Gb and 100Gb support for data centers and service providers.
Cluster Support	Connect multiple GigaVUE-FM and GigaVUE-OS H Series nodes in a self-healing, intelligent cluster. When you create a cluster of GigaVUE-FM and GigaVUE-OS H 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-FM and GigaVUE-OS H 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-FM and GigaVUE-OS H Series Flow Mapping® features let 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-FM and GigaVUE-OS H Series, GigaVUE-FM and GigaVUE-OS TA Series, and G Series nodes. The GigaVUE-FM and GigaVUE-OS H 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-FM and GigaVUE-OS H 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.
Email Notifications	Use email alerts for proactive notification of a wide variety of GigaVUE-FM and GigaVUE-OS 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-FM and GigaVUE-OS H 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. From the top navigation menu, select **Physical**.

2. From the left navigation pane, select **Physical Nodes**. This displays the list of Devices/Cluster Nodes managed by this instance of GigaVUE-FM.

3. 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-FM and GigaVUE-OS node.

- Manage Roles and Users–GigaVUE-OS to manage roles and users in H-VUE and to assign access permissions.

- Reboot and Upgrade Options to upload and upgrade images on the GigaVUE-FM and GigaVUE-OS node.

- Backup and Restore to learn how to back up and restore the configuration of the GigaVUE-FM and GigaVUE-OS node.

- Use SNMP to learn how to use the SNMP features on the GigaVUE-FM and GigaVUE-OS node.

Get Started with GigaVUE-FM and GigaVUE-OS 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 Internet Explorer for Use with H-VUE

Configure the Host Name

It is generally a good idea to configure the GigaVUE-FM and 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 2 Hostname Page.

To set the host name, do the following:

1. Select **Settings > Global Settings > Host Name**.

2. Click **Edit**.

3. Enter a name in the **Hostname** field.

4. Click **Save**.

| Global Settings | Security | Web | SNMP | SNMP v3 Users | SNMP Traps | SSH | TELNET | Hostname | Logging | Event Notification |

Email Notifications   ARP/NDP

Edit

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-FM and GigaVUE-OS node includes a variety of features for setting the time. By default, the GigaVUE-FM and GigaVUE-OS H Series node is configured to use its local clock, as configured with on 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-FM and GigaVUE-OS node's time is manually from the Date and Time page, which is shown in the following figure.

Date and Time   Date and Time   NTP   NTP Keys   PTP   Timestamp

(Edit)

Settings

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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS node's list and enable the use of NTP.

1. Select **Settings > Date and Time > NTP**.

2. Click **Add**. The Add NTP Server page displays.

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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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**.

Configure Logging

GigaVUE-FM and GigaVUE-OS H 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-FM and GigaVUE-OS H Series node's logging output. When an external syslog server is specified, the GigaVUE-FM and GigaVUE-OS H 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 H-VUE, 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.

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 master/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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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-FM and 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-FM and GigaVUE-OS node, do the following:

1. 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.

2. Click **Server Settings**. The Edit Email Server Settings page displays.

Figure 3   *Email Server Settings*

3. Enter the information about the email server on the settings page.

4. Click **OK**.

5. 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-FM and GigaVUE-OS node, do the following:

1. Select **Settings > Global Settings > Email Notifications**

2. Click **Event Settings**. The Edit Email Event Settings page displays, which provides a list of events that you can select for email notifications.

Figure 4   *Email Event Settings*

3. Select the event or events about which the email recipient should be notified.

4. Click **OK**.

5. 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-FM and GigaVUE-OS node, do the following:

1. Select **Settings > Global Settings > Email Notifications,** and then click **Add**.

2. 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.

3. 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.

4. Click **OK**.

Use a Custom Banner

The GigaVUE-FM and GigaVUE-OS 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**.

View Information About the Node

GigaVUE-OS H-VUE provides pages that provide specific information about the node. The About page provides product and version information that you can use when contacting customer support. The Interface page provides information about current settings for the interface. The DNS page lists the IP addresses for Domain Name Services.

About

To view the About page (refer to Figure 5 About Page), select **About** in the main navigation pane. The About provides the following information: GigaVUE Administration Guide

- 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 on which H-VUE is running. 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 5   *About Page*

Interface

The Interface page (refer to Figure 6 Interface Page) shows status information about the various interfaces. To access the interface page, select **Settings > interface > Interface**. The page provides the following information:

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

- Ethernet status information(eth0, eth1, eth1, eth2, or eth2.11). The number of interfaces depends on the node model. The following information is provided about the interface:
  - Admin Status
  - Link Status
  - Duplex
  - MTU
  - ifsource
  - Autconf enable
  - Auoconf privacy
  - IPv6 addresses
  - Dhcp enabled
  - Speed
  - IP address
  - Netmask
  - Type
  - ifindex
  - IPv6 enabled
  - Autoconf route

- DCHCPv6 running
- 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

Interface   Interface   DNS   Protocol Configuration

Admin Status	—	Speed	-
Link Status	—	IP address	-
Duplex	-	Netmask	-
MTU	-	Type	-
HW addr	-	Ifindex	-
ifSource	-	IPv6 enabled	yes
Autoconf enabled	no	Autoconf route	yes
Autoconf privacy	no	DHCPv6 running	no
IPv6 addresses	-	IPv6 address	-
Dhcp enabled	no	Comment	-

eth0

Admin Status	✓	Speed	1000Mb/s (auto)
Link Status	✓	IP address	10.115.54.6
Duplex	full (auto)	Netmask	/21
MTU	1500	Type	ethernet
HW addr	00:0C:29:40:38:C0	Ifindex	2
ifSource	physical	IPv6 enabled	no
Autoconf enabled	no	Autoconf route	no
Autoconf privacy	no	DHCPv6 running	no
IPv6 addresses	1	IPv6 address	fe80::20c:29ff:fe40:38c0/64
Dhcp enabled	yes	Comment	-

Figure 6   *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

Starting in software version 4.7, safe and limited modes are introduced to 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 master if the current master 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 non-master nodes in the cluster do not process any incoming traffic configuration from the cluster master.

- 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 master enters safe mode, the SNMP trap will be sent and the master 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 master 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 master. The following is an example of the CLI console message:

```
hc2 [default-cluster:master] (config) #
! Box-ID 4: System has entered into safe mode!!
hc2 [default-cluster:master] (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 H-VUE screen captures
- SNMP captures

To contact technical support, refer to Contact Technical Support on page 345.

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 H 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 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 H-VUE or 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

Security Tools	Description
	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-FM and GigaVUE-OS H 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 logins 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-FM and GigaVUE-OS 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 7 Role-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 7 Role-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 7   *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 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.

Step	Description
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 8 Sharing Locks

Figure 8   *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 H 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 logins to the GigaVUE-FM and GigaVUE-OS 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 logins to the GigaVUE-FM and GigaVUE-OS H 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
    - TACACS+
    - RADIUS
    - 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 H 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 9 Local 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.

Figure 9 *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 H 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-FM and GigaVUE-OS 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 H 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS H Series node), or by using the **local-only** option to map all externally authenticated users to a specific account on the GigaVUE-FM and GigaVUE-OS node.

Use AAA Server Role Assignments

In this model, you configure the GigaVUE-FM and GigaVUE-OS 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-FM and GigaVUE-OS node. In this case, the roles are fully assigned in the AAA server and there are no matching accounts on the GigaVUE-FM and GigaVUE-OS node.

Use Combination of Local and AAA Role Assignments

In this model, you configure the GigaVUE-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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

👤 **gmota**: local-user-name=mcain:role-IT

👤 **bposey**: local-user-name=psandoval

Local Account Database

👤 **mcain**: roles Security, IT

👤 **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-FM and GigaVUE-OS 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.

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

gmota

bposey:local-user-name=psandoval

atorres

mcain

Local Account Database

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

gmota

bposey:local-user-name=psandoval

atorres ⊘

mcain ⊘

Local Account Database

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

gmota

bposey:local-user-name=psandoval

atorres

mcain

Local Account Database

gmota

bposey

aaa authorization map default-user catchall

Figure 10   *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 H 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-FM and GigaVUE-OS node and the external server itself:

Figure 11 *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 12 Adding 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**.

Figure 12 *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 13 Adding a TACACS Server

4. Click **Save**.

Add TACACS Server		OK	Cancel
Enabled:	Yes		
Server IP:	IP Address		
Auth Port:	49		
Auth Type:	pap		
	☑ Use defaults for following		
Key:	********		
Timeout:	3		
Retransmit:	1		

Figure 13 *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. 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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 **Secure Cryptography** (refer to Configure Secure 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-FM and GigaVUE-OS nodes, including how to include a local user mapping attribute that the GigaVUE-FM and GigaVUE-OS node can use to assign roles to an externally-authenticated user. Refer to the following sections for details:

• Grant Roles with External Authentication Servers

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

Configure Cisco ACS: RADIUS Authentication

Use the following steps to configure Cisco ACS 5.x (RADIUS) to grant extra roles to externally authenticated users on the GigaVUE-FM and GigaVUE-OS H Series node.

Enable Extra Roles for RADIUS on the GigaVUE-FM and GigaVUE-OS Node

1. Go to **Settings > Authentication > RADIUS > Default Settings** to enable the GigaVUE-FM and GigaVUE-OS 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-FM and GigaVUE-OS H Series node/cluster.

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

2. Navigate to **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles** and click **Create** to add a new authorization profile.

3. Give the profile a name and description and click on the **RADIUS Attributes** tab.

4. Leave **Dictionary Type** set to **RADIUS-IETF** and click the **Select** button adjacent to the **RADIUS Attribute** field.

5. Select the **Class** attribute from the dialog that appears and click **OK**.

6. Leave the **Attribute Type** and **Attribute Value** fields at their default value (**String** and **Static**, respectively).

7. Supply the local user mapping and optional roles, as shown in the following figure:

8. Click the **Add** button to add this attribute to the authorization profile.

9. Assign this authorization profile to a group and populate it with GigaVUE-FM and GigaVUE-OS users.

Figure 14 Supplying the Class Field for RADIUS (ACS 5.x) shows these settings in a CiscoSecure ACS 5.x authorization profile.

Figure 14 *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 grant extra roles to externally authenticated users on the GigaVUE-FM and GigaVUE-OS H Series node.

Enable Extra Roles for TACACS+ on the GigaVUE-FM and GigaVUE-OS H Series Node

1. Go to **Settings > Authentication > TACACS > Default Settings** to enable the GigaVUE-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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** and click **Create** to add a new shell profile.

3. Give the profile a name and description in the **General** tab.

4. Click on the **Custom Attributes** tab.

5. Set the Attribute field to local-user-name.

6. Leave the **Requirement** and **Attribute Value** fields at their default value (**Mandatory** and **Static**, respectively).

7. Supply the local user mapping and optional roles, as shown in the following figure:

8. Click the **Add** to add this attribute to the shell profile.

9. Click **Submit** to finalize this shell profile.

10. Create Service Selection rules that will assign this shell profile to desired GigaVUE-FM and GigaVUE-OS users.

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-FM and GigaVUE-OS H Series node.

1. Enable Extra Roles for LDAP on the GigaVUE-FM and GigaVUE-OS H Series.

   To enable the GigaVUE-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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>[...]]]
   ```

   Figure 15 Adding the employeeType Attribute shows an example.

Figure 15   *Adding the employeeType Attribute*

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

NOTE: Refer to the GigaVUE-FM and GigaVUE-OS Release Notes for the latest browser support information.

Default Ports

The following default ports are normally open on GigaVUE-FM and GigaVUE-OS nodes:

Table 4: Open Default Ports

Port Number	Protocol	Description	Service/Server
22	TCP	SSH	OpenSSH 6.2
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-FM and GigaVUE-OS nodes, unless configured:

Table 5: Default Ports, Normally Closed

Port Number	Description
20	FTP
49	TACACS+
123	NTP
162	SNMP host
389	LDAP
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-FM and GigaVUE-OS 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 1.0.2l.

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.

The device will reload once FIPS is enabled.

For communications with the GigaVUE-FM and GigaVUE-OS 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-FM and GigaVUE-OS node. For example, if a client attempts to connect to the GigaVUE-FM and GigaVUE-OS Ethernet management port using blowfish, the following error message will be displayed: *No matching cipher found.*

UC APL Compliance

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

UC APL certification ensures that the GigaVUE-FM and GigaVUE-OS H 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS H 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-FM and GigaVUE-OS H Series products are as follows:

- httpd 2.4.29
- 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.

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-FM and GigaVUE-OS node certified with Common Criteria, the following configuration steps are required:

- enable secure cryptography mode. Refer to Configure Secure 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 Secure Cryptography Mode

A GigaVUE-FM and GigaVUE-OS node can be put into secure cryptography mode to improve the security of the management interface. In secure cryptography mode, weak encryption/decryption and hashing algorithms, used for accessing data and generating keys, are disabled. The secure cryptography mode limits the cryptographic algorithms, hashing algorithms, and SSH transport protocols, that are available for use on a GigaVUE-FM and GigaVUE-OS node.

Initially, the secure cryptography mode is disabled. There are two steps to enabling 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-FM and GigaVUE-OS Release Notes for the latest browser support information for Secure Cryptography Mode.

Enable Secure Cryptography Mode

To enable secure cryptography mode from the GigaVUE-FM and GigaVUE-OS H-VUE, do the following:

1. Select **Settings > Global Settings > Security**.
2. Click **Edit**.
3. On the **Edit Security Settings** page, select **Secure Cryptography**.
4. Click **Save**.

   The system displays the following notification:

   > Security settings updated successfully. Please reboot the device for the settings to take effect.

   For the secure cryptography mode to take effect the node needs to be reloaded.

   a. Select **Settings > Reboot and Upgrade**.

   b. Click **Reboot**.

When a GigaVUE-FM and GigaVUE-OS node is in secure cryptography mode, a status is displayed when you log in. For more information, refer to Status of Secure Cryptography Mode.

IMPORTANT: TLS version 1.2 is required for secure cryptography mode. When enabling secure cryptography mode, TLS version 1.2 is enabled by default. If you disable secure cryptography mode and want to change the TLS version, useGigaVUE-OSCLI command:`web server ssl min-version tls<version>`. Refer to the *GigaVUE-OS-CLI Reference Guide* for CLI guidance.

Disable Secure Cryptography Mode

By default, the secure cryptography mode is disabled. If it has been enabled, use the following steps to disabling it:

1. Select **Settings > Global Settings > Security**.
2. Click **Edit**.
3. On the Edit Security Settings page, clear **Secure Cryptography**.
4. Click **Save**.

   The system displays the following notification:
   `Security settings updated successfully. Please reboot the device for the settings to take effect.`

For the secure cryptography mode to take effect the node needs to be reloaded.

   a. Select **Settings > Reboot and Upgrade**.

   b. Click **Reboot**.

Enable Enhanced Cryptography Mode

To enable enhanced cryptography mode from the GigaVUE-FM and GigaVUE-OSH-VUE, 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 Secure Cryptography Mode

Use the following ciphers with secure cryptography mode:

Secure Cryptography Mode All Platforms
AES128-CBC
AES256-CBC

NOTE: Refer to the GigaVUE-FM and GigaVUE-OS 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 secure 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 Secure Cryptography Mode

If the secure cryptography mode is configured on a GigaVUE-FM and GigaVUE-OS 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 Cryptography and 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 30 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 competing the account details, click **Save**.

Manage Blank Passwords

Starting in software version 5.1, you can manage user accounts with blank passwords. By default, login with a blank password is allowed. However, you can also disallow login with a blank password to enhance security on the node.

The upgrade to software version 5.1 will go smoothly and all user accounts with blank passwords will remain intact and active. Disallowing login with a blank password will disable all user accounts with blank passwords. An **admin** user must take explicit action to re-enable those accounts.

An **admin** user will be able to re-allow login with blank passwords. However, this action will not automatically enable those user accounts that were previously disabled when login with a blank password was disallowed.

H-VUE options and error messages have been added to manage blank passwords. They are for local authentication only.

Refer to the following sections for details on managing blank passwords:

- Disallow Login with a Blank Password
- Allow Login with a Blank Password

Disallow Login with a Blank Password

When upgrading from a software version prior to 5.1, by default, login with a blank password is allowed. However, there are new CLI command options to disallow login with a blank password. This enhances security on the node.

When logging in is not allowed without a password, a user will not be able to login if their user account does not have a password configured. When the user logs in, they will be prompted for a password as if one has been configured, but login attempts will fail.

To manually disallow logging into a system with a blank password:

1. Go to **Settings > Global Settings > Security**. The **Allow Blank Passwords** field should be Disabled.

2. If it is enabled, click **Edit** and uncheck the **Allow Blank Passwords** check box.

The following messages can be displayed when logging in is not allowed without a password:

- a warning message if there are any user accounts in the system with a blank password

- an error message if the **admin** user account has a blank password

- an error message if the currently logged in user has a blank password

- an error message if there is an attempt to configure a blank password for a user

Allow Login with a Blank Password

An **admin** user can configure a setting to allow logging into a system without a password. Keep in mind that this is less secure.

When logging in is allowed without a password, a user will be able to login if their user account does not have a password configured, in other words, if their password is blank.

To allow logging into a system with a blank password:

1. Go to **Settings > Global Settings > Security**.

2. Click **Edit**. Select the **Allow Blank Passwords** check box.

3. Click **OK**.

Encrypt Syslog Audit Data

Syslog audit data, such as messages and traps, are usually sent unencrypted between a GigaVUE-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS node

- generate a public key to allow authentication between the GigaVUE-FM and GigaVUE-OS 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 **rsa1** 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. In GigaVUE-FM and GigaVUE-OS H-VUE, 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-FM and GigaVUE-OS 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 16 Logging Page shows an example.

Figure 16   *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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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 Telnet is Not Supported
- 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 Secure Cryptography Mode to Run Scans is Recommended
- Change the Password on admin Account
- Best Practices for Passwords

Use of Telnet is Not Supported

Using Telnet for remote connections over the Mgmt port is not recommended because Telnet is a non-secure protocol. By default, the Telnet server in GigaVUE-OS is disabled.

The status of the Telnet server is displayed on Telnet page in GigaVUE-FM and GigaVUE-OS-H-VUE. Select **Settings > Global Settings > TELNET** to verify that the Telnet server is disabled.

Using SSH is recommended. To set the SSH server settings, select **Settings > Global Settings SSH**. Click **Settings** and use the Edit SSH Server Settings page to generate host keys and enable/disable the SSH server.

IMPORTANT: Telnet server functionality is no longer supported as of GigaVUE-OS 5.7.00.

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-FM and GigaVUE-OS nodes.

Use of Secure Cryptography Mode to Run Scans is Recommended

Using secure cryptography mode to run scans is recommended.

Refer to Configure Secure 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

Starting in software version 4.7, the password on the default **admin** account must be changed to a non-default password. The default password (admin123A!) on the admin account is no longer allowed. If you are using the default password on this account the best practice is to change it to a non-default password before you upgrade to 4.7.xx or higher release.

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 *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 starting in software version 4.7.

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 to from GigaVUE-FM and the default password is in use, the first time you log in to GigaVUE-FM and GigaVUE-OS-HVUE after the upgrade, you are required to changed the default admin password through the CLI. GigaVUE-FM and GigaVUE-OS-HVUE 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 H 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 and GigaVUE-OS H-VUE 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 and GigaVUE-OS H-VUE 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 Disallow Login with a Blank Password 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-FM and GigaVUE-OS TA Series

This section describes the perpetual licenses for GigaVUE-FM and GigaVUE-OS TA series and how to apply licenses to GigaVUE-FM and GigaVUE-OS-TA series nodes.

- Perpetual GigaVUE-FM and GigaVUE-OS TA Series Licenses
- Apply Licenses for GigaVUE-FM and GigaVUE-OS TA Series

Perpetual GigaVUE-FM and GigaVUE-OS TA Series Licenses

Table 9: GigaVUE TA Series License Types lists perpetual licenses available on GigaVUE-FM and GigaVUE-OS TA Series nodes.

Table 9: GigaVUE TA Series License Types

Port License	
GigaVUE-OS	To enable ports on a white box after installing GigaVUE-OS, the appropriate license needs to be installed on the whitebox. The license can be purchased by calling the Gigamon representative. The initial key sent to the user is the Gigamon Installation Key.
	Using the digital footprint and serial number of the white box along with the EID, the license key can be obtained from the Gigamon licensing portal. After obtaining the license key, install it directly on the white box from either the CLI or H-VUE.
	This enables all ports on the white box.
GigaVUE-FM and GigaVUE-OS-TA1	GigaVUE-FM and GigaVUE-OS-TA1 requires port licensing to enable ports x25-x48 and the 4 additional 40G ports. For details, refer to the *GigaVUE-FM and GigaVUE-OS-TA1 Hardware Installation Guide*.
GigaVUE-FM and GigaVUE-OS-TA10	The GigaVUE-FM and GigaVUE-OS-TA10 has all forty-eight 1Gb/10Gb ports and four 40Gb ports enabled and does not require a port license. For details, refer to the *GigaVUE TA Series Hardware Installation Guide*.
GigaVUE-FM and GigaVUE-OS-TA10A	The GigaVUE-FM and GigaVUE-OS-TA10A has the first twenty-four 1Gb/10Gb ports enabled. A port license is needed to expand the GigaVUE-FM and GigaVUE-OS-TA10A to include all forty-eight 1Gb/10Gb ports as well as the four 40Gb ports. For details, refer to the *GigaVUE TA Series Hardware Installation Guide*.
GigaVUE-FM and GigaVUE-OS-TA100	On the GigaVUE-FM and GigaVUE-OS-TA100, only the first 16 out of 32 ports are enabled. Two port licenses are available to enable an additional 8 or 16 ports to expand to 24 or 32 ports. For details, refer to the *GigaVUE TA Series Hardware Installation Guide*.
GigaVUE-FM and GigaVUE-OS-TA100-CXP	On the GigaVUE-FM and GigaVUE-OS-TA100-CXP, all ports are enabled.
GigaVUE-FM and GigaVUE-OS-TA200	On the GigaVUE-FM and GigaVUE-OS-TA200, only the first 32 out of 64 ports are enabled. A port license is available to enable an additional 32 ports.
Advanced Features License	
GigaVUE-FM and GigaVUE-OS-TA1 / GigaVUE-FM and GigaVUE-OS-TA10 / GigaVUE-FM and GigaVUE-OS-TA10A / GigaVUE-FM and GigaVUE-OS-TA100 / GigaVUE-FM and GigaVUE-OS-TA200 / GigaVUE-OS	To enable clustering feature on all GigaVUE-FM and GigaVUE-OS TA Series nodes including the white box, installation of the specific Advanced Features License key on each TA node in a cluster is important. The license key needs to be enabled prior to joining the cluster.
	This applies to the white box with GigaVUE-OS as well.
	Any TA Series node can be added to a cluster however it cannot take the role of a master or a standby. It can only join as a normal. There can be more than one TA node in a cluster, however each node requires its own Advanced Features License to join a cluster.

Apply Licenses for GigaVUE-FM and GigaVUE-OS TA Series

Ports on GigaVUE-FM and GigaVUE-OS-TA1, GigaVUE-FM and GigaVUE-OS-TA10, GigaVUE-FM and GigaVUE-OS-TA100, and on a white box with GigaVUE-OS are enabled using Gigamon license keys. To enable clustering Contact your Sales Representative for information on obtaining a license key to enable ports or

clustering.

The GigaVUE-FM and GigaVUE-OS-TA10 has all forty-eight (48) 1Gb/10Gb ports and four (4) 40Gb ports enabled and does not require a port license.

A twenty-four (24) port GigaVUE-FM and GigaVUE-OS-TA10 version, called the GigaVUE-FM and GigaVUE-OS-TA10A is available with only the first 24 1Gb/10Gb ports enabled. A license is available to expand a GigaVUE-FM and GigaVUE-OS TA10A to include all 48 1Gb/10Gb ports as well all four (4) 40Gb ports.

On the GigaVUE-FM and GigaVUE-OS-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 to 24 ports or from 16 ports to 24 ports and then to 32 ports.

On the GigaVUE-FM and GigaVUE-OS-TA200, only the first 32 out of 64 ports are enabled. A port license is available to enable an additional 32 ports.

To view all licenses assigned to a TA Series node, select **Settings > Config and Licenses,** from the navigation pane. Advanced Features Licenses will start with ADV while Ports licenses will have PRT in the license key. For all licenses, the **Expiration Date** column has the word Never to indicate that there is no expiration date. Evaluation licenses are currently not available for GigaVUE-FM and GigaVUE-OS TA Series.

To view serial numbers, select **Chassis** from the Navigation pane, and then click **Table View**. The serial number is displayed in the **Serial Number** column under **Properties**.

To install licenses, select **Settings > Config and Licenses > Licenses**, and then click **Install**. Enter the license key in the License Key field and select the **Box ID** of the chassis to which to apply the license. For standalone nodes, there will be only one Box ID available.

Move a License between GigaVUE-FM and GigaVUE-OS TA Series

Ports Licenses and Advanced Features Licenses for GigaVUE-FM and GigaVUE-OS TA Series are connected to the serial number of the chassis. Licenses can be removed from these nodes and they will disable the functionality on the node. However licenses cannot be re-installed on a different node. To install a license on a new serial number, contact Gigamon representative or the support line.

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-FM and GigaVUE-OS-TA10 or GigaVUE-FM and GigaVUE-OS-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 17 Chassis View. Chassis View includes two types of views. Port View and Transceiver View. Transceiver View is the default view.

Figure 17   *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 18 Chassis View of Node in a Cluster shows an example.

Figure 18   *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-FM and GigaVUE-OS-TA1, you will only see one card allocation because these are non-modular nodes.

Figure 19 Chassis View—HC2 and Chassis View show some examples of chassis displayed on the Chassis page.

Figure 19   *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 Chassis View page. This view shows you the H 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 20 Chassis + Transceiver View shows an example of a Chassis + Transceiver View.

Figure 20   *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-FM and GigaVUE-OS-TA100. When fanout is used, the fanout is displayed on the Chassis page as shown in Figure 21 Chassis + Transceiver View with Fanout Ports.

Figure 21   *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 20 Chassis + 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 22 *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 (and H-VUE) uses lowercase notation to refer to ports (for example, c1, q1, x4, and g1).

When displaying ports in Chassis View (and H-VUE), 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 H 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 23 Chassis Table View for a Gigamon HC2 CCv2 shows an example of the Table View. For GigaVUE-FM and GigaVUE-OS-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.

Figure 23   *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, Hardware Type, Mode, Hardware Revision, Product Code, and Serial Number. 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 Gigamon HC-2 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 RMP of the 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 Advance 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-FM and GigaVUE-OS-TA1, GigaVUE-FM and GigaVUE-OS-TA10, or GigaVUE-FM and GigaVUE-OS-TA40 node. For more details, refer to Change 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-FM and GigaVUE-OS-TA1, GigaVUE-FM and GigaVUE-OS-TA10 and GigaVUE-FM and GigaVUE-OS-TA40 nodes. On the GigaVUE-FM and GigaVUE-OS-TA1, GigaVUE-FM and GigaVUE-OS-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-FM and GigaVUE-OS-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-FM and GigaVUE-OS-TA10 or GigaVUE-FM and GigaVUE-OS-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-FM and GigaVUE-OS-TA1 or GigaVUE-FM and GigaVUE-OS-TA10

The following card modes are available for the GigaVUE-FM and GigaVUE-OS-TA1 and GigaVUE-FM and GigaVUE-OS-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-FM and GigaVUE-OS-TA1 or GigaVUE-FM and GigaVUE-OS-TA10:

   a. Select **Actions > Change Mode**

   b. For **Mode**, select 48x, 56x, or 64x.

   The settings for each available mode are summarized in Table 10: 40Gb Port Settings by Card Mode on GigaVUE-FM and GigaVUE-OS-TA10 .

   c. Click **Save**.

3. Configure the card by selecting **Actions > Configure**.

Table 10: 40Gb Port Settings by Card Mode on GigaVUE-FM and GigaVUE-OS-TA10

Card Mode	Physical 40Gb Interface on GigaVUE-FM and GigaVUE-OS-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-FM and GigaVUE-OS-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-FM and GigaVUE-OS-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-FM and GigaVUE-OS-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 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS-TA40, GigaVUE-FM and GigaVUE-OS-TA100, GigaVUE-FM and GigaVUE-OS-TA200, GigaVUE-FM and GigaVUE-OS-TA100-CXP, the PRT-HD0-C06X24 line card on GigaVUE-FM and GigaVUE-OS 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-FM and GigaVUE-OS-TA40 supports 4x10G breakout at port level. Port breakout mode in GigaVUE-FM and GigaVUE-OS-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-FM and GigaVUE-OS-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-FM and GigaVUE-OS-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-FM and GigaVUE-OS 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 24 Port 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 24   *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-FM and GigaVUE-OS-TA100, the fanout ports are displayed in the chassis view as shown in Figure 25 Breakouts Displayed on a GigaVUE-FM and GigaVUE-OS-TA100 Chassis. In Figure 25 Breakouts Displayed on a GigaVUE-FM and GigaVUE-OS-TA100 Chassis, the ports that are set to **4x10G** show four additional ports.

Figure 25   *Breakouts Displayed on a GigaVUE-FM and GigaVUE-OS-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-FM and GigaVUE-OS-HC series devices and GigaVUE-FM and GigaVUE-OS-TA series devices.

Advance 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 Advance Hashing

Fabric Advance Hashing is used to enable advanced fabric hashing on a chassis in GigaStream stack links and GigaSMART groups. The Fabric Advance 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-FM and GigaVUE-OS-HC2+
- GigaVUE-HC3-v1
- GigaVUE-HC3-v2
- GigaVUE-FM and GigaVUE-OS-TA40
- GigaVUE-FM and GigaVUE-OS-TA100
- GigaVUE-FM and GigaVUE-OS-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 Advance 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 Advance Hash** is already configured, click the **Box-ID** field to view the Fabric Advance 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-FM and GigaVUE-OS Nodes

About Role-Based Access

GigaVUE H Series nodes use role-based access to manage access to the Gigamon Visibility Platform. Through H-VUE, 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.

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-FM and GigaVUE-OS nodes have three built-in roles for specifying which users have access to a given port. These roles are:

- Admin

---

[1]Requires Level 2 or Level 3 access, based on the user's role membership.

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 H-VUE. 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.

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.

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 Role-Based Access and Setting Permissions in GigaVUE-FM and GigaVUE-OS Nodes

Configuring RBAC in H-VUE 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 describes provides the steps for adding users to GigaVUE-FM and GigaVUE-OS nodes. Users are also assigned to roles that set there access permissions. For the step to create roles, refer to Create Roles.

To add users, do the following:

1. Select **Roles and Users > Users.** The **User Setup** page displays.

User Setup					Add	Edit	Delete
	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		

I< < 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, do the following:

   - 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.
   - 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**.

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 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,

Permission Level	Description
	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.

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 in H-VUE are:

- 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-FM and GigaVUE-OS nodes. For more detailed instructions on the upgrade paths available, refer to the *GigaVUE-FM and GigaVUE-OS H Series Upgrade Guide* and *GigaVUE-FM and GigaVUE-OS 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 H-VUE for the node to reboot.

2. Select **Settings > Reboot and Upgrade > Reboot**. The Reboot page displays as shown in Figure 26 Reboot Page.

Reboot and Upgrade   Reboot

Reboot   Reboot the system. This operation may take several minutes.
Please wait before attempting to access configuration pages or logging in.

Shutdown   Shutdown the system. This operation will not reboot until it is power-cycled.

Figure 26 *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 Figure 27 Reboot Dialog appears. Click **OK** to reboot the node.

REBOOT

WARNING: This action will reboot this node. Are you sure you want to proceed?

OK   Cancel

Figure 27 *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 Figure 28 Save and Reboot. 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.

Save and Reboot   Reboot   Cancel

Figure 28 *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-FM and GigaVUE-OS node.

In a cluster configuration, if you try to update the software through H-VUE, 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 H Series nodes when in a cluster.
```

Important: Starting in GigaVUE-OS 4.7.00, the default password admin123A! is no longer allowed on the admin account. If the node is upgraded to through the **configuration-jumpstart** command, the password for the admin user is required to be set, which will be the password when the admin user logs into H-VUE after the upgrade. If the node is upgraded through GigaVUE-FM, H-VUE does require the default password to be reset. However, you should change the admin default password after upgrading.

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.

> **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-FM and GigaVUE-OS 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 29 Active 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 29   *Active Images Page Showing Both Partitions*

3. Remove all the currently uploaded images.

   a. As shown in Figure 30 All 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 30   *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 31 Install 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 31   *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-FM and GigaVUE-OS-TA1, or GigaVUE-HC2).

    In Figure 32 Local 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 32   *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-FM and GigaVUE-OS 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 33 Configuration Files Page.

Figure 33 *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-FM and GigaVUE-OS node. To upload a configuration file, do the following:

1. Select **Actions > Upload**. The Upload dialog displays as follows:

Upload

Upload local binary file:

[Choose File] No file chosen

(To be saved as separate file with its original name)

[Upload Configuration] [Cancel]

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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS H Series Nodes

Nodes and Cluster Backup

This section describes how to backup H 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 master only.

You can schedule node or nodes and node clusters for immediately backup or schedule 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 Master node 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 34 SNMP Trap Configuration Save Enabled.

Figure 34   *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 35 Nodes 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.

Figure 35 *Nodes Selected for Scheduled Backups*

5. From the **Recurrence** drop-down list, select one of the following:

Table 11: 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. Set an end date to determine until when the backup must recur.

Option	Description
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 master node 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 either the CLI or H-VUE, are also available for restoring from the GigaVUE-FM.

- In the Device Restore process, master preferences for the cluster are only updated to the master node after restoring; they are not propagated to any of the standby nodes.

Restore Nodes and Clusters

To restore nodes or clusters, do the following:

1 Click **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.

   2 Select **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-FM and GigaVUE-OS 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-FM and GigaVUE-OS H Series node's current systems to the active configuration file.

   You can also save the GigaVUE-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS H Series nodes, you configure SNMP hosts and notification events from the master/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 master/VIP address.

In addition, you browse each individual clustered node's MIB separately, not over the VIP/master.

NOTE: A GigaVUE-FM and GigaVUE-OS TA Series node can never assume the role of a master node in a clustered environment.

Configure SNMP Notifications

GigaVUE-FM and GigaVUE-OS 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:

Figure 36   *Configuring SNMP Notifications*

Configure the SNMP Server and Notification Destinations

The SNMP server on the GigaVUE-FM and GigaVUE-OS 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-FM and GigaVUE-OS H Series or GigaVUE-FM and GigaVUE-OS 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 40 Edit SNMP Settings Page displays.

Figure 37 *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-FM and GigaVUE-OS 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 38 SNMP Settings Page.

Figure 38 *SNMP Settings Page*

The GigaVUE-FM and GigaVUE-OS H Series and GigaVUE-FM and GigaVUE-OS 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-FM and GigaVUE-OS H Series and GigaVUE-FM and GigaVUE-OS 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 39 Notification 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 39 *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-FM and GigaVUE-OS H Series node's MIB is available for download from the Gigamon Customer Portal. 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 12: Log messages Associated with SNMP Event

SNMP Event	Description	Log Message
2ndflashboot	Secondary flash boot notification (for GigaVUE-FM and GigaVUE-OS-TA100, GigaVUE-FM and GigaVUE-OS-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-FM and GigaVUE-OS-TA100, GigaVUE-FM and GigaVUE-OS-TA100-CXP, GigaVUE-HC1, and GigaVUE-HC3)	/gv/snmp/events/CPUTemp
eporttemp	GigaSMART CPU (e1/e2 port) temperature notification (for GigaVUE-HC3)	/gv/snmp/events/EPortTemp
evallicensereminder	Evaluation license expiration notification	/gv/snmp/events/EvalLicenseReminder
exhausttemp	Exhaust temperature notification (for GigaVUE-FM and GigaVUE-OS-TA100, GigaVUE-FM and GigaVUE-OS-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

SNMP Event	Description	Log Message
modulechange	Module change notification	/gv/snmp/events/ModuleChange
operationmode	Operational mode change notification	/gv/snmp/events/SystemModeChange
opticstemp	Optics (transceiver) temperature notification (for GigaVUE-FM and GigaVUE-OS-TA100, GigaVUE-FM and GigaVUE-OS-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 (TX) error	/gv/snmp/events/RxTxError
switchcputemp	Switch CPU temperature notification (for GigaVUE-FM and GigaVUE-OS-TA100, GigaVUE-FM and GigaVUE-OS-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-FM and GigaVUE-OS H Series or GigaVUE-FM and GigaVUE-OS 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-FM and GigaVUE-OS H Series and GigaVUE-FM and GigaVUE-OS TA Series supports public MIBs, including partial MIB-II (ifTable and ifXTable).

The GigaVUE-FM and GigaVUE-OS H Series and GigaVUE-FM and GigaVUE-OS 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-FM and GigaVUE-OS H Series and GigaVUE-FM and GigaVUE-OS 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 40 Edit SNMP Settings Page

Figure 40   *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-FM and GigaVUE-OS H Series and GigaVUE-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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 OID	Value for a PRT-H00-X12G04 in Slots 1/2
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.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-FM and GigaVUE-OS H Series and GigaVUE-FM and GigaVUE-OS 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 13: Statistics for CPU Utilization describes the statistics for CPU utilization:

Table 13: 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 14: 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.
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 .

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, or USB.

`(config) # show diag detail upload <upload URL>`

Work with Port Utilization Measurements

The GigaVUE-FM and GigaVUE-OS H Series and GigaVUE-FM and GigaVUE-OS 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	**port <port list> alarm low-utilization-threshold <percentage>**

Feature	CLI Command
the GigaVUE-FM and GigaVUE-OS 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 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-FM and GigaVUE-OS H Series or GigaVUE-FM and GigaVUE-OS 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.

Port	Type	Speed (Mb/s)	Utilization		Threshold		Last time threshold triggered	
			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-FM and GigaVUE-OS 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-FM and GigaVUE-OS H Series node will log an alarm for the specified ports. The threshold must be exceeded for at least a 5-second interval. 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.

Requirement	Description
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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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-FM and GigaVUE-OS 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**
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/A
12/1/x6    39      N/A       2014/07/01 17:30:07.378  N/A                  32         N/A
12/1/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:  35
     Last Time Exceeding:  2014/07/01 17:30:07.384
      12/1/x5 counters     value
      --------------------------
                    RX:  41
                    TX:  0
             RX Config:  30
             TX Config:  0
     Last Time Exceeding:  0
      12/1/x6 counters     value
      --------------------------
                    RX:  39
                    TX:  0
             RX Config:  32
             TX Config:  0
     Last 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.

Software Licensing Reference

Reference Topics:

- GigaVUE-FM Licensing
- GigaSMART Licensing

GigaVUE-FM Licensing

This section describes how to obtain and apply licenses for GigaVUE-FM. It consists of the following main sections:

- Licensing GigaVUE-FM describes the licenses available and how to obtain and apply them.
- GigaVUE-FM License Types lists the available licenses and features available with each license type.
- Applying Licenses describes the process to apply the licenses.
- Upgrading and Downgrading License Packages covers the best practices when upgrading or downgrading license packages.

> NOTE: For information about GigaVUE-VM licensing, refer to the GigaVUE Cloud Suite for VMware Configuration Guide.

Licensing GigaVUE-FM

GigaVUE-FM is provisioned by default with a Base License that lets you add one physical node and one virtual node. To manage additional physical or virtual nodes, you must obtain and apply licenses, as described in this section.

> NOTE: To run only GigaVUE-VM, there is no requirement to purchase additional licenses for GigaVUE-FM. For information about GigaVUE-VM licensing, refer to the *GigaVUE Cloud Suite for VMware Configuration Guide*.

Obtaining a New License

Contact your Sales representative to obtain a new license for GigaVUE-FM Nodes (see Contact Sales for the contact information).

Retrieving a Lost License

If you lost an existing license, contact Gigamon Technical Support for assistance. For the contact information, refer to *Contact Technical Support*.

GigaVUE-FM License Types

GigaVUE-FM are available in multiple tiered options along with optional Add-On Features which are also available as a special license (add-on are included with the Prime Package as free-of-charge). All GigaVUE-FM are available with base option and with base feature of 1 free physical node and 1 free virtual node and 10 virtual tap points for OpenStack, AWS and Azure. No licenses are required to activate this option.

> NOTE: For information about GigaVUE-VM licensing, refer to the *GigaVUE-VM Configuration Guide*.

Additional GigaVUE-FM licenses are available for purchase. The following tables summarizes the available packages and support features with each package.

Table 1: GigaVUE-FM Evaluation License Packages

License Types	Physical Nodes	Virtual Nodes	OpenStack/AWS/Azure	Features available	Notes
GigaVUE-FM Evaluation	Up to 200	1 (included as Base)	10 Virtual TAP Points	All features available with Prime for the evaluation period.	License automatically expires after 45 days.

> NOTE: Evaluation licenses are not recommended for deployment in production environment. At the end of the evaluation period, if the license is not upgraded to a fully licensed version, the features are disabled automatically. For an evaluation license, contact your Gigamon representative.

GigaVUE-FM License Packages

The following table summarizes the GigaVUE-FM License packages.

Table 2: GigaVUE-FM License Packages

Features	Base (Free-of-charge)	5-Pack	10-Pack	Prime
Physical Node Count	1	Up to 5	Up to 10	Up to 200
Rest API	Yes	Yes	Yes	Yes
Audit, Events Logs	Yes	Yes	Yes	Yes
Firmware Upgrade	Yes	Yes	Yes	Yes
Configuration Backup	Yes	Yes	Yes	Yes
Dashboard	Only the following Static Widgets are displayed:	Customizable	Customizable	Customizable

Features	Base (Free-of-charge)	5-Pack	10-Pack	Prime
	• Top 10 Network Ports by Traffic • Top 10 Tool Ports by Traffic • Top 10 Maps by Traffic • Audit Logs By Result • Events By Severity • Ports Link Status Summary • Unhealthy Maps Status Summary • Unhealthy Flows			
Reports	No	Yes	Yes	Yes
Trending Data	1 Day	1 Week	1 Month	1 Month

There are also upgrade packages for GigaVUE-FM available for customers that have already purchased GigaVUE-FM. The packages allow users to upgrade from a 5-pack option to a 10-pack or a Prime package. There is also an option to upgrade from a 10-pack to a Prime package. To find out more about the upgrade purchase, contact your Gigamon Sales representative.

For upgrade option, your GigaVUE-FM information should match what is in the record for MAC address and customer information.

Applying Licenses

Use the following procedure to license your products on the **License** page.

To obtain and apply the GigaVUE-FM license:

1. Locate the email sent to you by Gigamon containing the licensing information for your installation. This email contains one or more **EID** (Entitlement ID) values. You will use these EIDs to generate License Keys on the Gigamon Licensing Website.

2. Locate the Challenge MAC address of the virtual network adapter associated with the GigaVUE-FM installation.

   a. To locate the address, starting from the top navigation, click the gear icon, then click **System > Licenses**.

   The Fabric Manager/Cloud Licenses are listed by default.

   Note the Challenge MAC address.

Figure 1 *Locate the MAC Address*

Refer to the Challenge MAC displayed in the Licenses page. The license is only valid with the corresponding MAC address. If GigaVUE-FM is deleted or re-installed, contact Gigamon Support.

3. GigaVUE-FM licenses can be activated by clicking **Activate License** and following the on-screen advice. The instructions provide a link directly to the Gigamon License Portal at

   https://licensing.gigamon.com

   > **NOTE:** Gigamon Community credentials are required to access the License Portal. When prompted, click **Allow** to grant access to the licensing portal.

4. Enter the MAC address and EIDs of the purchased licenses in the portal. Multiple EIDs can be entered by clicking the **+** button. Once all the information is entered and submitted, the license key(s) are displayed on the screen.

   1Download the (.lic) files or record the license key or keys.

5. Login to GigaVUE-FM as an administrator and return to the license activation screen.

   - Click the gear icon, then navigate to **System > Licenses Activation View > With License Portal** and complete the activation by importing the downloaded .lic files.
   - Or, navigate to **System > Licenses Activation View > With License Key** and complete the activation by entering the license key.

Upgrading and Downgrading License Packages

- Upgrading of license packages is available at all times.
- To purchase a new license, please contact Gigamon Sales Representative.
- All licenses are perpetual therefore they carry in to any software upgrades without re-applying the licenses, except evaluation licenses are set for expiration. Software upgrades can be managed during valid evaluation period.
- Licenses can be upgraded from Base to either a 45 day evaluation or to paid version.

- If an evaluation license is upgraded to Express or Advanced version, the Add-on features are automatically disabled. To retain the Add-On features, please purchase the license, or upgrade to the Prime Package.

- Purchased licenses cannot be downgraded.

- Licenses can be deleted and re-entered as long as the MAC address tied to the license is still valid.

In case of expiration of the evaluation license, GigaVUE-FM will revert back to supporting only 1 physical and 1 virtual node.

The list below shows the node priorities in case a License is invalid and nodes are deactivated. In such a case, the nodes will be visible but deactivated. They can be re-activated if the license is reinstalled. This is especially important if the evaluation license expires and you need extra time to enter a valid license.

(1) If a cluster exists:

- Master node

  In case of multiple clusters, the cluster with the top level priorities as shown in standalone will take over. For example, a cluster with master as GigaVUE-FM and GigaVUE-OS-2404 will have preference over a cluster with master as GigaVUE-HC2.
- Standalone node *(Based on the node priority levels as shown below)*
- Standby Master, in case the master is removed
- Stack/Cluster member
- Unreachable
- Unknown

(2) If there is no cluster *(G Series nodes have top preference)*

- GigaVUE-FM and GigaVUE-OS-212
- GigaVUE-FM and GigaVUE-OS-420
- GigaVUE-FM and GigaVUE-OS-2404
- GigaVUE-FM and GigaVUE-OS-0216
- GigaVUE-FM and GigaVUE-OS-TA100-CXP
- GigaVUE-HC3
- GigaVUE-HC2
- GigaVUE-HC1
- GigaVUE-FM and GigaVUE-OS-TA10
- GigaVUE-FM and GigaVUE-OS-TA40
- GigaVUE-FM and GigaVUE-OS-TA100
- GigaVUE-FM and GigaVUE-OS-TA10A
- White box with GigaVUE-OS

In cases where nodes have connectivity issues as listed below, the next level nodes as shown in Scenarios (1) and (2) will take effect:

- Nodes should not have any connectivity issue
- Nodes can be reached but node response has parsing problem

- Nodes can be reached but authentication is invalid
- Node cannot be reached
- Nodes cannot be added

GigaSMART Licensing

There are different types of licenses available for GigaSMART applications.

Topics:

Types of Software Licenses

This table shows the different types of software licenses available as of 5.7.00.

License	Node-locked or Floating*	Time-bound or Perpetual (Term License)	Subscription
App Filtering, App Metadata	Floating	Yes	Yes
Other SMART License	Floating	Yes	N/A
Advanced Feature License (GigaVUE TA Series)	Node-Locked	Perpetual	N/A
Cloud SKUs**	Node-Locked with GigaVUE-FM	Yes	Yes
GigaVUE-FM	Yes	No	N/A
Trial License	Floating	Yes	N/A
Existing License (<5.7)	Yes	Perpetual (Other than GigaVUE Cloud Suite, Application Filtering Intelligence)	Yes (GigaVUE Cloud Suite, Application Filtering Intelligence)

1 **Floating means Floating license with GigaVUE-FM/GigaVUE-OS 5.7 that can be assigned to supported nodes as needed.*

2 ***GigaVUE-FM does not support floating licenses when running on GigaVUE Cloud Suite for Azure or GigaVUE Cloud Suite for AWS. For assistance, contact Gigamon customer support. (Ref: FM-26425)*

GigaSMART Floating Licenses

Flexible floating software licensing options are available for GigaSMART applications with GigaVUE-OS and GigaVUE-FM 5.7.00. Features include:

- A flexible licensing model to include floating licenses, subscriptions licenses, and perpetual licenses.
- New streamlined and easy to use order management system for subscription licenses.
- Floating licenses are available through the GigaVUE-FM, which now has a License Manager to manage and activate floating licenses.
- The Gigamon licensing portal requires a Gigamon Community login to access all software licenses.

> NOTE: Existing perpetual licenses that are fixed to a specific card (also referred to as "node-locked") can still be managed via the GigaVUE-OS CLI, however, the more flexible licensing options (such as trials, floating, and subscriptions) are available through GigaVUE-FM. Some GigaSMART applications, such as De-duplication, Inline SSL, and Application Intelligence, are only available through a subscription license.

> NOTE: Refer to the Release Notes v5.7.00 for additional information about floating licenses.

> NOTE: Contact your Gigamon Sales Representative to learn more about the available floating license options.

Licensing GigaSMART Applications

GigaSMART applications are enabled using license keys.

Contact your Sales Representative for information on obtaining a license key to enable additional GigaSMART applications. Refer to the **license** command in the *GigaVUE-OS CLI Configuration Guide* for details.

Note: The "show license" command also displays the start time and end time to support term licenses.

For **perpetual licenses**, the Expiration Date column has the word Never to indicate that there is no expiration date.

For **evaluation licenses**, the Expiration Date column has a specific date on which the license expires. For more information on evaluation licenses, refer to GigaSMART Evaluation Licenses.

GigaSMART Evaluation Licenses

Use an evaluation license to evaluate GigaSMART applications. During the evaluation period of 45 days, you will have access to the full functionality of the GigaSMART applications under evaluation. You can obtain an evaluation license for any GigaSMART application, for either a single or for a number of GigaSMART applications combined in a bundle.

To obtain an evaluation license, contact your Sales Representative. A license key will be generated by Gigamon and sent to you. You then install the license, which enables the GigaSMART application for evaluation purposes.

Install Evaluation Licenses

You install an evaluation license the same way you install a perpetual license, using the **license** command.

The key consists of a long string beginning with LK2, which is a protocol, followed by the line card or module (SMT_HC0_R), followed by the content of the license key.

Notify Evaluation License Expiry

After installation, the evaluation license will expire after 45 days, on a specific date.

To notify you as the evaluation license approaches the expiry date, you can enable a notification. When enabled, the notification will be sent when there are 30, 15, 10, 5, 4, 3, 2, and 1 days remaining before the license expires.

Use the following CLI command to enable the evaluation license reminder:

```
(config) # snmp-server enable notify evallicensereminder
```

You can also use the **show license** command to display the expiration date of an evaluation license.

How to Combine Evaluation and Perpetual Licenses

An evaluation license can be for a number of GigaSMART applications combined in a bundle. If you have a perpetual license for one GigaSMART application, for example, de-duplication, and you want to evaluate a bundle that contains 10 GigaSMART applications, including de-duplication, the 45-day evaluation period will apply to the other 9 GigaSMART applications, while the perpetual license will apply to de-duplication.

If you obtain a perpetual license after an evaluation license, the perpetual license will overwrite the evaluation license.

GigaSMART Application after Expiry

Once an evaluation license expires, access to the GigaSMART application is disabled. If maps were configured using GigaSMART applications on the evaluation license, traffic will be dropped when the evaluation license expires.

> NOTE: Traffic will flow through maps with perpetually licensed GigaSMART applications.

In addition, the **gsop** command will not be available once the evaluation license has expired.

However, if a new evaluation license for the same GigaSMART application is installed, a new 45-day evaluation period will begin.

Move Evaluation and Perpetual Licenses

Evaluation and perpetual license keys are saved on the GigaSMART line card or module, while license information is stored in the configuration database. The license key on the line card or module has to match the license information stored in the database, otherwise a license mismatch will result.

Line cards or modules may sometimes need to be moved or swapped. For the procedure to move a license, refer to Move Licensed GigaSMART Line Card to a New Slot. This procedure will clear a license mismatch under certain circumstances. Moving a license depends on the license type, as well as the expiry date, as follows:

License Key Saved on GigaSMART Line Card/Module	License Information Stored on Configuration Database	Can be Moved?
Perpetual License	Evaluation License	Yes
Evaluation License	Perpetual License	No
Evaluation License with an earlier expiry date than the one stored on the configuration database	Evaluation License	No
Evaluation License with a later expiry date than the one stored on the configuration database	Evaluation License	Yes

Move Licensed GigaSMART Line Card to a New Slot

On the GigaVUE-FM and GigaVUE-OS HD Series, you can move a GigaSMART line card from one slot to another. On the GigaVUE-HC2 or GigaVUE-HC3, you can move a GigaSMART front module from one bay to another. However on the GigaVUE-HC2, you cannot move the GigaSMART rear module from the rear to the front.

If there are no GigaSMART operations (gsops) configured on the line card or module to be moved, you can move the line card or module to the new slot or bay.

If there are GigaSMART operations (gsop), GigaSMART groups (gsgroup), and maps configured on the line card or module to be moved, the system will report a license mismatch if you try to move it without first removing the related configuration.

To clear the settings related to the GigaSMART line card or module from its previous slot, allowing you to create new GigaSMART operations, GigaSMART groups, and maps using the GigaSMART line card or module in its new slot, use the following procedure:

1. Issue the following CLI command:

   `(config) # show running-config`

2. Copy and paste the output to a file such as Notepad, for reference.
3. Remove the map that uses the gsop defined on the gsgroup of the GigaSMART line card or module to be moved, using the following CLI command:

`(config) # no map alias <alias>`

4. Remove the gsop that was defined on the gsgroup of the GigaSMART line card or module to be moved, using the following CLI command:

`(config) # no gsop alias <alias>`

5. Remove the gsgroup that was defined on GigaSMART line card or module to be moved, using the following CLI command:

`(config) # no gsgroup alias <alias>`

6. Issue the following CLI command on GigaSMART line card or module to be moved:

`(config) # no card slot <slot ID>`

7. Assuming that the new slot does not have a GigaSMART line card or module inserted, issue the following CLI command on the new slot:

`(config) # no card slot <slot ID>`

8. Issue the following CLI command on the new slot:

`(config) # card slot <slot ID>`

On the new slot, configure gsgroup, gsop, and reapply the map that uses the gsop on the GigaSMART line card or module.

GigaSMART Application Licenses

GigaSMART applications are enabled using license keys. This section provides summaries of the applications associated with each GigaSMART License:

Base GigaSMART Applications

- **GigaVUE-FM and GigaVUE-OS-HC0 Module** – The base applications include Packet Slicing, Masking, Trailer, and IP and L2GRE Tunnel Decap.
- **GigaVUE-HC3 SMT-HC3-C05 Module** – The base applications include Packet Slicing, Masking, Trailer, and IP and L2GRE Tunnel Decap.
- **GigaVUE-HC1 Node** – The base applications include Packet Slicing, Masking, and Trailer.

GigaSMART applications with the Base license available on GigaVUE-FM and GigaVUE-OS H Series nodes:

- GigaSMART Packet Slicing
- GigaSMART Masking

- Using GigaSMART Trailers
- GigaSMART IP Encapsulation/Decapsulation (GigaSMART Tunnel)
- GigaSMART Layer 2 GRE Tunnel Encapsulation/Decapsulation
- GigaSMART VXLAN Tunnel Decapsulation
- GigaSMART Custom Tunnel Decapsulation

Advanced Tunneling License/Tunneling License

> **NOTE:** Advanced Tunneling license on GigaVUE-HC2, and GigaVUE-HC3. Referred to as "Tunneling license" on GigaVUE-HC1,

The **Advanced Tunneling License/Tunneling License** enables the following GigaSMART applications:

- GigaSMART IP Encapsulation/Decapsulation (GigaSMART Tunnel)
- GigaSMART Layer 2 GRE Tunnel Encapsulation/Decapsulation
- GigaSMART VXLAN Tunnel Decapsulation
- GigaSMART Custom Tunnel Decapsulation
- GigaSMART ERSPAN Tunnel Decapsulation

De-Duplication License

The **De-Duplication License** enables the following GigaSMART applications:

- GigaSMART De-Duplication

Header Stripping License

The **Header Stripping License** enables the following applications:

- GigaSMART Header Addition
- GigaSMART Header Stripping

Adaptive Packet Filtering (APF) License

The **Adaptive Packet Filtering License** enables the following GigaSMART applications:

- GigaSMART Adaptive Packet Filtering (APF)

Application Session Filtering (ASF) License

The **Application Session Filtering License** enables the following GigaSMART applications:

- GigaSMART Application Session Filtering (ASF) and Buffer ASF

GTP Filtering & Correlation License

The **GTP Filtering & Correlation License** enables the following GigaSMART applications:

- GigaSMART GTP Correlation
- GigaSMART GTP Whitelisting and GTP Flow Sampling

- GTP Scaling
- GTP Stateful Session Recovery

SIP/RTP Correlation License

The **SIP/RTP Correlation License** enables the following GigaSMART application:

- GigaSMART SIP/RTP Correlation

FlowVUE License

The **FlowVUE License** enables the following GigaSMART applications:

- GigaSMART FlowVUE

NetFlow Generation License

The **NetFlow Generation License** enables the following GigaSMART applications:

- GigaSMART NetFlow Generation

SSL Decryption Licenses

The **SSL Decryption Licenses** enable the following GigaSMART applications:

- GigaSMART Out-of-Band SSL Decryption
- GigaSMART SSL Decryption for Inline and Out-of-Band Tools

NOTES:

- GigaSMART load balancing does not require a separate license. Stateless load balancing is included with base licenses. Stateful load balancing for GTP and ASF are included with the GTP Filtering & Correlation and Application Session Filtering (ASF) licenses. Stateful load balancing for tunnel is included with the tunneling licenses. Refer to GigaSMART Load Balancing in GigaVUE-FM User's Guide.
- GigaSMART MPLS traffic performance enhancement does not require a separate license. Refer to GigaSMART MPLS Traffic Performance Enhancement in GigaVUE-FM User's Guide.

Related Commands

This section describes the related commands for GigaVUE-FM.

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]

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>]

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 a saved configuration file from a remote host. Use HTTP(S), FTP, TFTP, 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 configuration file named myconfig 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/myconfig** You can also use the **<filename>** argument to give the retrieved file a new name on the GigaVUE-FM and GigaVUE-OS H Series node. For example, the following command retrieves **myconfig** and names it **newconfig** on the node: **fmctl image fetch scp://bbochy:catch1@192.168.1.75/myconfig newconfig** NOTE: You cannot retrieve a file with the same name as the currently active 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]	Configures the logging server. For example: **fmctl logging 1.2.3.4:9514 facility * priority debug tcp**
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

Argument	Description
	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 instance. The admin password must be a minimum of 11 characters and a maximum of 30 characters. The characters 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. For example: `fmctl set UI admin password <new 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:

Argument	Description
	`fmctl --interface eth1 set mapping fm`

[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>

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 Gigamon Community

Documentation

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

Table 1: Documentation Set for Gigamon Products

GigaVUE-FM and GigaVUE-OS 5.10 Hardware and Software Guides
Hardware
how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE-FM and GigaVUE-OS devices; reference information and specifications for the respective GigaVUE-FM and GigaVUE-OS devices
*G-TAP A Series 2 Installation Guide
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE TA Series Hardware Installation Guide *(now including TA25)*
*GigaVUE-OS Installation Guide for DELL S4112F-ON
how to install GigaVUE-OS and configure ports on COTS DELL S4112F-ON
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
how to install GigaVUE-FM on VMware ESXi, MS Hyper-V, and KVM
how to migrate GigaVUE-FM on VMware ESXi, Hardware Appliance, and AWS
GigaVUE-OS Upgrade Guide
how to upgrade the embedded GigaVUE-OS on GigaVUE H Series and GigaVUE TA Series nodes
Administration

GigaVUE-FM and GigaVUE-OS 5.10 Hardware and Software Guides

GigaVUE-OS and GigaVUE-FM Administration Guide

how to administer the GigaVUE-OS and GigaVUE-FM software (note, new file name for PDF)

Fabric Management

GigaVUE-FM User's Guide

how to install, deploy, and operate GigaVUE-FM

how to configure GigaSMART operations

includes instructions for GigaVUE-FM and GigaVUE-OS features

Cloud Configuration and Monitoring

how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the respective cloud platform

GigaVUE Cloud Suite for AnyCloud Configuration Guide

how to deploy the GigaVUE Cloud Suite solution in any cloud platform

GigaVUE Cloud Suite for AWS Configuration Guide

GigaVUE Cloud Suite for AWS Quick Start Guide

quick view of AWS deployment used in conjunction with the GigaVUE Cloud Suite for AWS Configuration Guide

GigaVUE Cloud Suite for AWS SecretRegions Configuration Guide

GigaVUE Cloud Suite for Azure Configuration Guide

GigaVUE Cloud Suite for Kubernetes Configuration Guide

GigaVUE Cloud Suite for Nutanix Configuration Guide

GigaVUE Cloud Suite for OpenStack Configuration Guide

GigaVUE Cloud Suite for VMware Configuration Guide

Gigamon Containerized Broker

Reference

GigaVUE-OS-CLI Reference Guide

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

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)

GigaVUE-FM/Venafi TPP Integration Guide

GigaVUE-FM and GigaVUE-OS 5.10 Hardware and Software Guides
instructions to configure Bulk Certificate Provisioning from Venafi Trust Protection Platform (TPP) to GigaVUE-FM (FM).
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 .
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM. **GigaVUE-OS H-VUE Online Help** provides links the online documentation.

How to Download from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Docs** 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 & Documentation** 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

To send feedback and report issues in our documentation, complete the short survey at the following link:

https://www.surveymonkey.com/r/gigamondocumentationfeedback

Contact Technical Support

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

The Gigamon 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 Gigamon Community site to:

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

The Gigamon 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.