



GigaVUE-OS Administration Guide

GigaVUE

Product Version: 6.14

Document Version: 1.0

(See Change Notes for document updates.)

Copyright © 2026 Gigamon Inc. All rights reserved.

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

Trademark Attributions

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

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

Change Notes

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

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

Contents

GigaVUE-OS AdministrationGuide	1
Change Notes	2
Contents	3
GigaVUE-OS Administration	10
Administer GigaVUE Nodes	10
GigaVUE-HC1	11
GigaVUE-HC3	11
GigaVUE-HC1-Plus	11
GigaVUE-HCT	12
GigaVUE-TA25	12
GigaVUE-TA100	12
GigaVUE-TA200	12
GigaVUE-TA400	12
Notes on GigaVUE TA Series Nodes	13
Any Packet, Any Destination	13
The Gigamon Deep Observability Pipeline	14
Features and Benefits	15
Add the Configuration Boot File Path	22
Create the Configuration Boot File	22
Upload the Configuration Boot File	23
Set Time Manually	26
Use NTP Time Server for Clock Synchronization	27
Clock Management Best Practice for devices connected to GigaVUE-FM ..	28
Perform One-Time NTP Server Synchronization	28
Role-Based Access: Rules and Notes	28
User Management	28
Role Management	29
Port Ownership	29

External Syslog Servers and Clustered Nodes	31
Delete an External Syslog Server	32
Packet Format for Syslog Output	32
Configure the Email Server Settings	33
Configure the Event Settings	33
Add Email Notification Recipients	34
Interface	35
DNS	38
Safe Mode	38
Limited Mode	39
Enable SNMP Trap for Safe Mode and Limited Mode	40
Collect Information for Technical Support	41
Generate Sysdump or Debug Dump File	41
Management Port Security	45
Configure Role-Based Access: A Summary	47
About Locks and Lock Sharing	47
Overview of the AAA Page	49
Authentication Priority	49
User Mapping	49
Password	50
Lockout	50
Non Local User Authentication	51
Maximum SSH Sessions	51
Configure Maximum Authentication Attempts	52
Change the Password on admin Account	52
Messages Associated with Changing the admin Account	
Password	52
Best Practices for Passwords	53
GigaVUE-OS Password Policies	54
FAQ for Logins and Passwords	56
Do Passwords Expire?	56
What Happens After Unsuccessful Logins?	56
Can a User be Forced to Change Their Password?	57
Are Passwords Displayed?	57
Who Creates Users and Passwords?	57

Configure AAA Authentication Options	57
Remote Authentication Only	60
Authorization of User Account	60
Next Steps	60
Grant Roles with External Authentication Servers	61
Use Local Role Assignments	61
Use AAA Server Role Assignments	61
Use Combination of Local and AAA Role Assignments	62
Assign Role in AAA Servers	62
Create Users for AAA and Remote Authentication Server	63
Configure AAA Authorization	63
Example	64
Add AAA Servers to the Node's List	65
RADIUS Server	66
Add a RADIUS Server	66
Delete a RADIUS Server	67
Add a TACACS+ Server	67
Delete a TACACS+ Server	68
Configure an IPv6 Address	68
Add an LDAP Server	69
Set the LDAP Server Default Settings	69
Delete an LDAP Server	71
Configure an IPv6 Address	71
Configure Roles in External Authentication Servers	71
Configure Cisco ACS: RADIUS Authentication	72
Enable Extra Roles for RADIUS on the GigaVUE Node	72
Example of Assigning the Class Attribute in RADIUS Authorization Profile (ACS 5.x)	72
Configure Cisco ISE: RADIUS Authentication	72
Configure Cisco ACS: TACACS+ Authentication	75
Enable Extra Roles for TACACS+ on the GigaVUE HC Series Node	75
Example of Assign local-user-name to Shell Profile (ACS 5.x)	75
Configure Cisco ISE: TACACS Authentication	76
Configure LDAP Authentication	78
Enabled TLS Cipher Suites	82
Are all versions of GigaVUE-FM validated for FIPS compliance?	82
Can you enable FIPS using the fmctl command?	82
Can you add a device that is not FIPS-compliant to a FIPS enabled GigaVUE-FM?	82
What happens to the GigaVUE-FM database after you enable FIPS?	82

How do I perform backup and restore operation on a FIPS enabled GigaVUE-FM?	83
Is the FIPS certification applicable for GigaVUE-FM instance irrespective of where it is deployed?	83
Configure UC APL	85
Accept DoD Web Server Certificates	86
Enable Login Failure Tracking	86
Display Unsuccessful Login Attempts	86
Configure Common Criteria	87
Configure Enhanced Cryptography Mode	88
Enable Enhanced Cryptography Mode	88
Ciphers to Use with Enhanced Cryptography Mode	88
Cryptographic Algorithms	89
Status of Enhanced Cryptography Mode	89
Configure Secure Password	89
Enable Secure Password Mode	89
Set up the Secure Password	90
Encrypt Syslog Audit Data	91
Encryption Procedure	91
Display Logging Information	92
Chassis View + Transceiver View	95
Chassis View + Port View	96
Line Card and Module Numbering	96
Actions Menu	98
Reload a GigaSMART Line Card or Module	99
Change VLAN Tag mode	100
Configure Change VLAN Tag	100
Rules and Notes	101

Change Port Mode	102
Enable Advanced Fabric Hashing	104
Fabric Advanced Hashing	105
Role-Based Access and Flow Mapping®	107
Set Map-Sharing Permission Levels	107
Locks and Lock Sharing	108
Create Roles	108
Add Users	110
Create Roles	110
Associate Roles with Port Permissions	112
Set Locks and Lock-Shares	113
Remove a Lock from a User's Port	113
Remove a User's Lock-Share	113
Lock a Port for a User	113
Set Map-Sharing Permission Levels	114
Save the Configuration	118
Upgrade PLD	118
Work with Configuration Files in the Configurations	
Page	119
Configuration File Options	119
Configuration Actions	120
Upload a Configuration	120
Import a Configuration	120

Enable Events for Backup	122
BackUp Nodes and Clusters	123
How to Schedule Backups	123
Download Backup Files	125
Add Comments to Backup File	125
Set Do Not Purge Flag	126
Delete Backup Files	126
Restore Nodes and Clusters	127
View Restore Logs	128
Configure the SNMP Server and Notification	
Destinations	132
Configure SNMP v3 Users	133
Enable Notifications	134
Delete a Destination for SNMP Notifications	135
Enable or Disable Events for SNMP Notifications	136
Receive Traps	136
View Associated Log Messages	136
Configure Other SNMP Server Settings	140
Recommendations for Vulnerabilities	141
Available SNMP Statistics for Data Ports	141
SNMP Statistics	142
Display the System Health Statistics	144
Enable the System Health Threshold Notification	148
Configure the System Health Threshold	148
View the System Health Events	149
Enable System Health Events for SNMP Notifications	150
View the System Health Diagnostics	150
Port Utilization Availability by Port Type	151
View Port Utilization	151
Format of show port utilization Output	151
Examples	152

Port Utilization Thresholds	152
Utilization Alarm/SNMP Notification Generation	153
Configure Port Utilization Thresholds and Notifications ..	153
Set Alarm Buffer Thresholds	155
Configuration Example	157
Buffer Usage Alarm	158
TLS 1.2 Ciphers	159
TLS 1.3 Ciphers	160
Rules and Notes - Limitations	161
System Warnings	162
Exceptions	162
How to Download Software and Release Notes from My Gigamon	167
Premium Support	169
Glossary	170

GigaVUE-OS Administration

This guide describes how to get started and administer the GigaVUE-OS.

Featured Content:

- [Administer GigaVUE Nodes](#)
- [Software Licensing Reference](#)
- [GigaVUE-FM CLI Commands](#)
- [Mapping of SNMP Traps with GigaVUE-FM Events and Alarms](#)
- [GigaVUE® Fabric Management Events](#)
- [Corrective Actions For GigaVUE-FM Alarms](#)
- [Related Commands](#)

Administer GigaVUE Nodes

Featured topics:

- [Access Nodes From GigaVUE-FM](#)
- [Get Started with GigaVUE Nodes](#)
- [Configure Security Options](#)
- [Chassis](#)
- [Manage Roles and Users—GigaVUE-OS](#)
- [Reboot and Upgrade Options](#)
- [Backup and Restore](#)
- [Use SNMP](#)
- [Monitor Utilization](#)

Introducing the GigaVUE Nodes

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

- [About the GigaVUE HC Series and GigaVUE TA Series](#)
- [GigaVUE HC Series Features and Benefits](#)

About the GigaVUE HC Series and GigaVUE TA Series

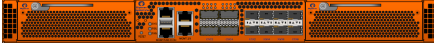
The GigaVUE HC Series delivers performance and intelligence in each of its Traffic Deep Observability Pipeline nodes, with port density and speeds that scale to your needs, from

1Gb to 100Gb. With an intuitive web-based interface (GigaVUE-FM) and a powerful GigaVUE-OS, the Gigamon Deep Observability Pipeline is able to replicate, filter, and selectively forward network traffic to monitoring, management, and security tools.

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

- GigaVUE-HC1
- GigaVUE-HC1-Plus
- GigaVUE-HCT
- GigaVUE-HC3
- GigaVUE-TA25
- GigaVUE-TA100
- GigaVUE-TA200
- GigaVUE-TA400
- Certified Traffic Aggregation White Box

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

GigaVUE-HC1	▪ 1RU Footprint ▪ Built-in GigaSMART functionality ▪ Standard GigaVUE-OS CLI and GigaVUE-FM GUI ▪ Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes	
GigaVUE-HC3	▪ 3RU Footprint ▪ Four Module Slots (Bays) ▪ Internal Control Card ▪ Extension Board ▪ Dedicated Cluster Management Port ▪ Standard GigaVUE-OS CLI and GigaVUE-FM GUI ▪ Supports all GigaVUE-HC3 Modules ▪ Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes	
GigaVUE-HC1-Plus	▪ 1RU Footprint ▪ Two Module Slots (Bays) and one Fixed Base Module ▪ 4x100G/40G, 8x25G, 10G, 1G connectivity ▪ Supports GigaSMART applications with a fixed rear GigaSMART Module.	

	- Supports Flex Inline in unprotected ports with 100G/40G/10G/25G/4x10G/4x25G speed Nodes. - Cluster with GigaVUE HC Series and GigaVUE TA Series. - All ports, excluding BPS ports, of same type and speed can be used to create GigaStream.	
GigaVUE-HCT	1RU and half rack width system - One Module Slot (Bay) and one Fixed Base Module 2x100G/40G connectivity - Supports Flex Inline in unprotected ports with 100G/40G/4x10G/4x25G speed Nodes. - Cluster with GigaVUE HC Series and GigaVUE TA Series. - All ports, excluding BPS ports, of the same type and speed can be used to create GigaStream.	
GigaVUE-TA25	1 RU Footprint 48 25Gb/10Gb/1Gb ports and 8 100Gb/40Gb ports - Standard GigaVUE-OS CLI and GigaVUE-FM GUI - Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes	
GigaVUE-TA100	1RU Footprint 32 x 100Gb/40Gb Ports - Standard GigaVUE-OS CLI and GigaVUE-FM GUI - Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes	
GigaVUE-TA200	2RU Footprint 64x 100Gb/40Gb Ports - Standard GigaVUE-OS CLI and GigaVUE-FM GUI - Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes	
GigaVUE-TA400	1RU Footprint 32 400Gb/ 100Gb/40Gb QSFP-DD/ QSFP28/QSFP+ ports - Standard GigaVUE-OS CLI and GigaVUE-FM	

GUI

- **Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes**

Notes on GigaVUE TA Series Nodes

- On the GigaVUE-TA100, only the first 16 out of 32 100Gb ports are enabled. Two port licenses are available to enable an additional 8 or 16 ports to expand from 16 ports to 24 ports or from 16 ports to 24 ports and then to 32 ports.
- On the GigaVUE-TA200, only the first 32 out of 64 100Gb ports are enabled. A port license is available to enable an additional 32 ports.
- The ports on the GigaVUE-TA100 can be used as network, tool, or hybrid ports.
- For more information about the GigaVUE TA Series nodes, refer to the *GigaVUE TA Series Hardware Installation Guide*.

GigaVUE HC Series Features and Benefits

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

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

Any Packet, Any Destination

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

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

The Gigamon Deep Observability Pipeline

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

The Gigamon Deep Observability Pipeline 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 Gigamon Deep Observability Pipeline as a data socket that provides immediate access for ad hoc tool deployment without impact to the production network. Gigamon's Deep Observability Pipeline nodes accommodate the growing number of network monitoring tools and network security tools. [Figure 1The Gigamon Deep Observability Pipeline](#) summarizes these features.

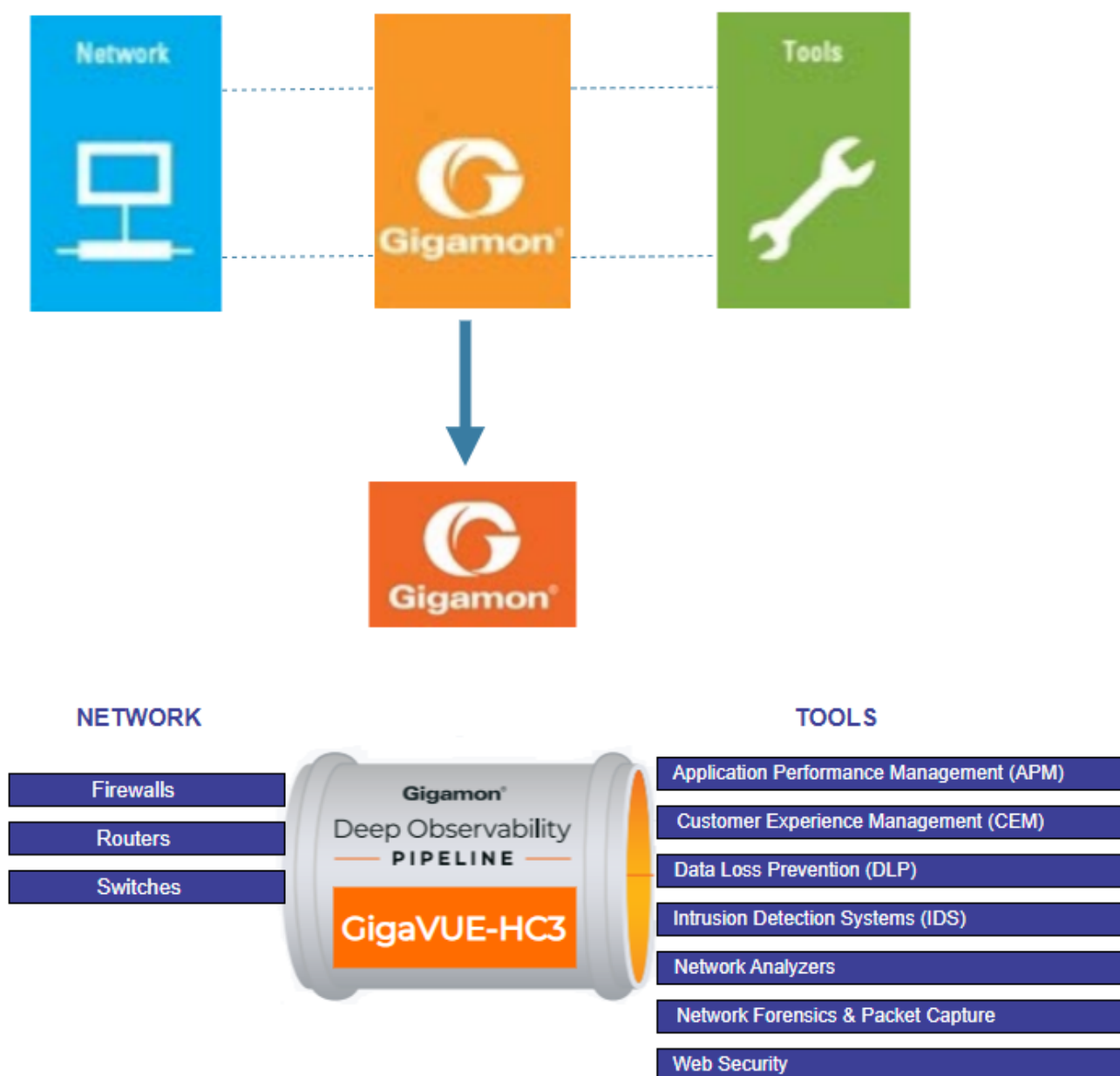


Figure 1 The Gigamon Deep Observability Pipeline

Features and Benefits

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

Benefit	Descriptions
CLI Management	Configure the operations of the GigaVUE HC Series node using a command-line interface, the GigaVUE-OS: - Local access over the serial console port on control card. - Remote network access using SSH2 over the 10/100/1000 Ethernet Mgmt port on control card. - Secure access to the CLI, either through local authentication or optional RADIUS/TACACS+/LDAP support.
Scalable Port Density	Use the line cards that best suit your port density needs. Depending on the line cards installed in the node, you can have as many as 256 10Gb ports (a node fully populated with PRT-H00-Q02X32 line cards). In addition, the GigaVUE HC Series node evolves with network speeds, including line cards with 40Gb and 100Gb support for data centers and service providers.
Cluster Support	Connect multiple GigaVUE HC Series nodes in a self-healing, intelligent cluster. When you create a cluster of GigaVUE HC Series nodes, available ports appear as a unified fabric, with ingress ports able to send packets to any egress port, regardless of its physical chassis. Nodes are connected through stack links consisting of one or more 10Gb, 40Gb, or 100Gb ports. Cluster management traffic can be carried out-of-band on its own network or inband on stack links.
Share SPAN Ports	Connect a SPAN port to a network port on the GigaVUE HC Series node and multicast that traffic to multiple different tool ports, giving multiple different tools access to the same data. Use Flow Mapping® to send specific traffic to different tool ports, ensuring that each tool sees the data that best suits its individual strengths. You can move, add, and reconfigure tools at will without affecting production networks.
Aggregate Links	Send the data from multiple different network ports to one or more tool ports, allowing you to combine traffic from multiple access points into a single stream for analysis.
Flow Mapping®	The GigaVUE HC Series Flow Mapping® feature lets you direct traffic arriving on network ports to one or more tool ports based on different packet criteria, including VLAN IDs, IP addresses, port ranges, protocols, bit patterns, and so on. You can drop some traffic intentionally using drop rules and also create a shared-collector destination for any packets not matching the maps configured on a shared set of network ports.
GigaVUE-FM Support	Deploy Gigamon's umbrella fabric management system, GigaVUE-FM to manage all of your GigaVUE HC Series, GigaVUE GigaVUE TA Series nodes. The GigaVUE HC Series is fully compatible with GigaVUE-FM, allowing you to centralize deployment of images, configuration backups, and alert management.
Role-Based Access	Role-based access makes it easy to share the Gigamon Deep Observability Pipeline between different groups of users with different needs. Administrators can assign egress ports to different groups of users. Users can then select the traffic they need to see from shared ingress ports. Administrators adjust map priority to ensure that each packet is delivered to the correct destination.
Cisco-Style CLI	The GigaVUE HC Series node's CLI offers a similar style to the familiar Cisco interface, minimizing relearning for IT professionals.
Command	Type only as many letters of a command as are needed to positively differentiate

Benefit	Descriptions
Abbreviation	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 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, and GigaVUE-HC3, the modules are interchangeable between the front bays of each chassis type, but not with each other, due to form and factor.
Flexible 10Gb/1Gb Support	All 10Gb ports in GigaVUE HC Series line cards can be used with 1Gb Ethernet media by inserting a copper or optical SX/LX SFP instead of an SFP+. Interoperability and support are ensured by purchasing SFPs from Gigamon – transceivers purchased from other vendors are not supported.

Access Nodes From GigaVUE-FM

You can access Gigamon nodes that have been added to GigaVUE-FM from the GigaVUE-FM interface. For instructions to add a node to GigaVUE-FM, refer to [Add New Physical Node or Cluster to GigaVUE-FM](#).

To access a node from the GigaVUE-FM interface:

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

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

Refer to the following topics for detailed information:

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

Web

This section provides the steps required to configure the GigaVUE HC Series node's web server used for GigaVUE-FM access to the node. GigaVUE-FM is Gigamon Web-based GUI for the GigaVUE HC Series node, providing graphical user interface configuration.

To access the Web page of the node:



1. On the left navigation pane, click  under **Physical** select **Nodes**. This displays the list of Devices/Cluster Nodes managed by this instance of GigaVUE-FM.
2. Click the Cluster ID of any node to open the node.
3. Once you are in the node, click **Settings** > **Global Settings** > **Web**.
4. Select or enter the following details:

Field	Description
Setting	
Web Server SSL Minimum Version (optional)	The SSL minimum version for the web server: • TLS v1.0: • TLS v1.1: • TLS v1.2:
HTTP Port	HTTP port.
HTTPS	Use the toggle option to enable and disable HTTPS.
HTTPS Port	HTTPS port number.
Auto Logout Timeout	The maximum duration of user inactivity before a Web session is logged out automatically.
Web Session Renewal	Specifies the length of time before a session expires that the Web server will issue a new cookie and renew the session. This should be set at least as long as the auto-logout setting so that sessions do not expire before they have a chance to be renewed.
Session Timeout	
Web Proxy Settings	
Web Proxy Address	Web proxy address. This can be either IPv4 or IPv6 address.
Web Proxy Port	Web proxy port. If you do not specify a port, the default is 1080.
Authentication Type	Can be either basic or none.
Basic Auth Username	Basic authentication username.
Basic Auth Password	Basic authentication password.

Click **Apply** to save the configuration.

Enabled TLS Cipher Suites

GigaVUE-OS supports the commonly-supported TLS 1.2 ciphers. The following ciphers are supported in TLS 1.2:

Supported TLS 1.2 Ciphers

Cipher Name	Key Exchange (Kx)	Authentication (Au)	Encryption (Enc)	MAC
ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE	RSA	AES_256_GCM_SHA384	SHA384
ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE	RSA	CHACHA20_POLY1305_SHA256	SHA256
ECDHE_RSA_WITH_ARIA_256_GCM_SHA384	ECDHE	RSA	ARIA_256_GCM_SHA384	SHA384
ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE	RSA	AES_128_GCM_SHA256	SHA256
ECDHE_RSA_WITH_ARIA_128_GCM_SHA256	ECDHE	RSA	ARIA_128_GCM_SHA256	SHA256
ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE	RSA	AES_256_CBC_SHA384	SHA384
ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	ECDHE	RSA	CAMELLIA_256_CBC_SHA384	SHA384
ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE	RSA	AES_128_CBC_SHA256	SHA256
ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	ECDHE	RSA	CAMELLIA_128_CBC_SHA256	SHA256
DHE_RSA_WITH_AES_256_GCM_SHA384	DHE	RSA	AES_256_GCM_SHA384	SHA384
DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	DHE	RSA	CHACHA20_POLY1305_SHA256	SHA256
DHE_RSA_WITH_AES_256_CCM	DHE	RSA	AES_256_CCM	256
DHE_RSA_WITH_ARIA_256_GCM_SHA384	DHE	RSA	ARIA_256_GCM_SHA384	SHA384
DHE_RSA_WITH_AES_128_GCM_SHA256	DHE	RSA	AES_128_GCM_SHA256	SHA256
DHE_RSA_WITH_AES_128_CCM	DHE	RSA	AES_128_CCM	128
DHE_RSA_WITH_ARIA_128_GCM_SHA256	DHE	RSA	ARIA_128_GCM_SHA256	SHA256
DHE_RSA_WITH_AES_256_CBC_SHA256	DHE	RSA	AES_256_CBC_SHA256	SHA256
DHE_RSA_WITH_CAMELLIA_256_	DHE	RSA	CAMELLIA_256_	SHA256

Cipher Name	Key Exchange (Kx)	Authentication (Au)	Encryption (Enc)	MAC
CAMELLIA_256_CBC_SHA256			CBC_SHA256	
DHE_RSA_WITH_AES_128_CBC_SHA256	DHE	RSA	AES_128_CBC_SHA256	SHA256
DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	DHE	RSA	CAMELLIA_128_CBC_SHA256	SHA256

Secure (Crypto/FIPS) mode

The following Secure (Crypto/FIPS) mode ciphers are supported in TLS 1.2:

Supported Secure (Crypto/FIPS) mode TLS 1.2 Ciphers

Cipher Name	Key Exchange (Kx)	Authentication (Au)	Encryption (Enc)	MAC
ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE	ECDSA	AES_256_GCM_SHA384	SHA384
ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE	ECDSA	AES_128_GCM_SHA256	SHA256
ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE	ECDSA	AES_256_CBC_SHA384	SHA384
ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE	ECDSA	AES_128_CBC_SHA256	SHA256

About

To view the About page (refer to the following figure):

1. On the left navigation pane, go to **Inventory**  and select **Physical > Nodes**.
2. Click on a node listed in the page.
3. In the Node Overview page, select **About** (under support).

The **About** provides the following information:

- Product Name—The name of the product, GigaVUE-OS.
- Version—The current version running. For example, 4.8.00.
- Build ID and Build Date—Information about when the current build was created.
- Version Summary—A detailed description of the currently installed version.
- Git Hash—Additional build information.
- U-Boot Version—The currently installed u-boot version.
- CPLD Version—System information.

- TS Version—System information. This field displays information only when a timestamp card is inserted in the chassis.
- Model—The node model. For example, GigaVUE-HC1-Plus.
- Serial Number—Serial number of the node.
- Host Name—The host name assigned to the node. For information about setting the host name, refer to [Configure the Host Name](#)
- Host ID—Host id of the node.
- Start-up time—The date that the current version was installed and the number of hours, minutes, and seconds that the node has been running.

GigaVUE-OS Information

Name	Information
Product Name	GigaVUE-OS
Version	6.4.00.02
Build ID	413960
Build Date	Debug 2023-10-12
Version Summary	GigaVUE-OS 6.4.00.02 Build 413960 Debug 2023-10-12 21:36:51 x86_64 gihc3 root@jenkins-slave601:git:9bc89e4b4ede
Git Hash	9bc89e4b4ede9556cab35b3bfcd22f811ba95366
U-Boot Version	N/A
Ts Version	—
Model	HC3
Serial Number	JD39A
Host Name	gigamon-a0d39a
Host ID	eaf72ba0d39a

© 2023 Gigamon Inc. All Rights Reserved.

Figure 2 About Page

Zero Touch Provisioning (ZTP)

Zero-Touch Provisioning (ZTP) automates the deployment of devices with minimal user intervention, particularly after a factory reset or fresh installation. With ZTP enabled by default, the device automatically connects to the network, fetches its configuration from a pre-configured source, and provisions itself based on custom configuration files defined by the user. These files must be error-free, valid, and meet the supported configuration criteria.

Prerequisites

Before configuring ZTP, ensure the following:

- A valid DHCP server is available in the network.
- The DHCP server is configured with the appropriate URL path for the device to download the configuration file.

Configuration Boot File Setup for Zero Touch Provisioning (ZTP)

The following sections describe how to set up the configuration boot file for ZTP:

- [Add the Configuration Boot File Path](#)
- [Create the Configuration Boot File](#)
- [Upload the Configuration Boot File](#)

Add the Configuration Boot File Path

1. Add the configuration boot file path to the DHCP server.
 - a. **For unique configurations per device:** Use ***.conf** in the path. The device will then request a configuration file named with its specific serial number (e.g., device_serial_number.conf). Ensure each device has its serial-number-specific configuration file present in the path.
 - b. **For identical configurations across all devices:** Use a single configuration file named **boot.conf** in the path.

Sample configuration for Linux based DHCP server

```
DHCPv4 server config(/etc/dhcp/dhcpd.conf)
subnet 3.3.33.0 netmask 255.255.255.0 {
range 3.3.33.5 3.3.33.10;
default-lease-time 600;
max-lease-time 7200;
if (substring(option vendor-class-identifier, 0, 7) = "gigamon") {
option ztp-url "http://3.3.33.6/bootfile.conf";
}
}
```

Create the Configuration Boot File

1. Define the configuration in the boot file that the device will use:
 - a. **Hostname:** Specifies the device hostname.
 - b. **Local User Configuration:** Defines user credentials. For security reasons, password must be provided in encrypted format. you can use a Gigamon device for password encryption.
 - c. **Log Server Configuration:** Specifies log server details for device log storage.
 - d. **SNMP Server Configuration:** Provides SNMP server details for monitoring.
2. Save the configuration file with an appropriate name (e.g., Serialnumber.conf or boot.conf).

Sample configuration via ZTP bootfile:

```
hostname HC1
username admin password 9
VB8LxzVH1iNEs7BfNgTqOleOTsU86OXnNTnK1izrVPC63IwuNP1IV+D+ATVrHRUy
ip domain-list
logging 10.114.10.57
logging 10.114.10.57 trap info
logging fcab:1:1:2160:34f8:8bb1:d2d:20b8
logging fcab:1:1:2160:34f8:8bb1:d2d:20b8 trap warning
logging local info
snmp-server community public
snmp-server enable communities
no snmp-server host 20.114.210.62 disable
snmp-server host 20.114.210.62 traps port 7744 version 2c
no snmp-server host fcab:1:1:2160:34f8:8bb1:d2d:20b8 disable
snmp-server throttle event bcmsoctemp interval 120
snmp-server throttle event bottomswitchtemp interval 120
snmp-server throttle event cpusoctemp interval 120
snmp-server traps event userauthfail
snmp-server traps event vportstatechange
snmp-server traps event watchdogreset
no snmp-server user fm-snmp-user v3 enable
snmp-server user fm-snmp-user v3 encrypted auth sha "" priv aes-128 ""
snmp-server user user1 v3 enable
```

Upload the Configuration Boot File

1. Upload the configuration boot file to the server location specified in the DHCP server.
2. Ensure the file is in the correct path as mentioned in the DHCP server and accessible by devices.

Verify the Zero Touch Provisioning (ZTP) Process

1. Perform a factory reset or fresh installation to initiate the ZTP process.
2. The device automatically requests an IP address from the DHCP server, retrieves the configuration boot file specified by the URL, and applies the configurations from the boot file.
3. Use the **show system ztp** command to check the ZTP status.

NOTE: In all the failure scenarios, the system will prompt the user with the jump-start.

Security Considerations

The security of the Zero Touch Provisioning process is entirely dependent on DHCP, and any customer choosing to deploy it should ensure the security of the DHCP infrastructure. A compromised DHCP server, or an environment where a rogue DHCP server could be enabled, potentially compromise the security of the Gigamon ZTP process and therefore the end-device.

Gigamon further strongly recommends that passwords should be encrypted if they are present in the configuration. The configuration file is passed in clear text, and this fact should be acknowledged and risk-managed for any deployment.

NOTE: ZTP will be enabled in the case of a fresh installation or following a factory reset (command: 'reset factory all'). In normal operation, including a normal reload of a configured box or following a software upgrade, ZTP will be disabled.

Limitations

1. ZTP functionality is limited to the DHCP client on the management interface only.
2. When both DHCPv4 and DHCPv6 are enabled on the management interface, the same boot file URL must be configured on both DHCP servers.
3. ZTP is not supported on the DELL S4112F-ON and G-TAP A Series 2 devices.
4. The ZTP configuration boot file can be downloaded only through HTTP.
5. In the event of a configuration failure during ZTP, successfully applied configurations will not be reverted.
6. ZTP does not support cluster configurations through the boot file.
7. It is not recommended to include AAA configurations in the ZTP boot file, as GigaVUE-OS currently does not support password encryption for AAA configurations.
8. Configurations that require user input (e.g., yes/no) are not supported through the ZTP boot file.

Get Started with GigaVUE Nodes

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

- [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](#)

Configure the Host Name

It is generally a good idea to configure the GigaVUE-OS node’s name, date, and time as part of your initial configuration. For information on setting options related to time and date, refer to [Configure Time Options](#). The Hostname is shown on the Hostname page, which is shown in [Figure 3Hostname Page](#).

To set the host name, do the following:

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

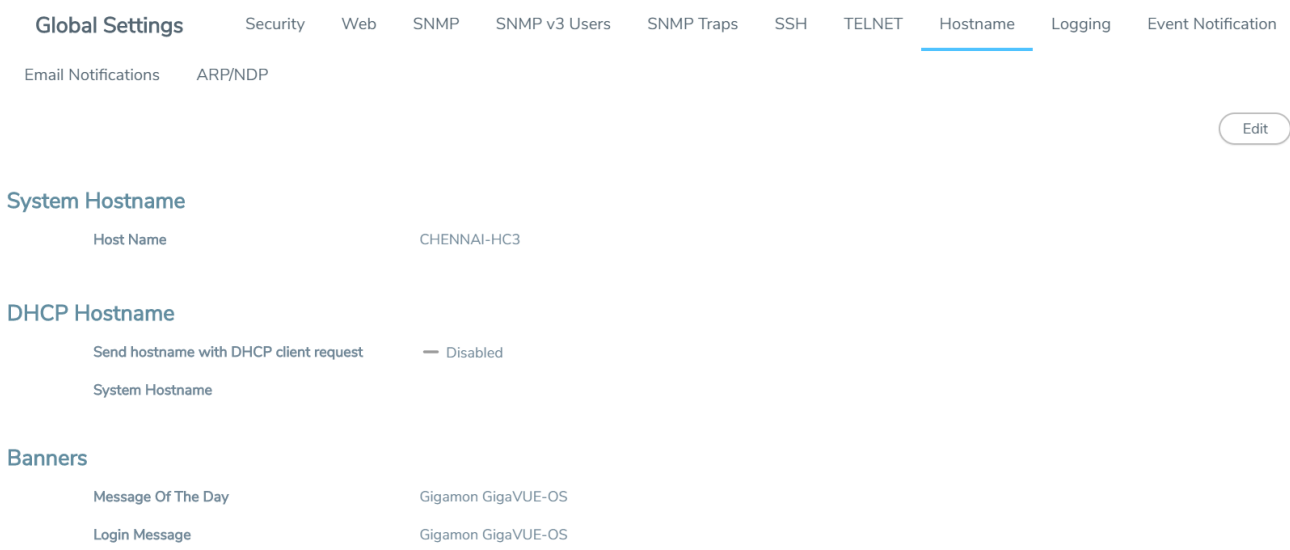


Figure 3 Hostname Page

Configure Time Options

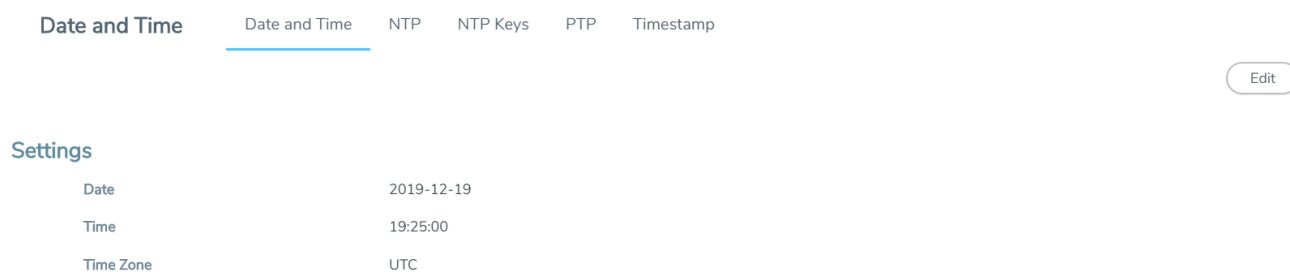
The GigaVUE-OS nodes include a variety of features for setting the time. By default, the GigaVUE HC Series node is configured to use its local clock, as configured with the Date and Time page by selecting **Settings > Date and Time**. The following table provides references to information about the various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

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

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

Set Time Manually

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



To set the time manually, do the following:

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

1. Select **Settings > Date and Time > Date And Time**.
2. Click **Edit**.

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

Use NTP Time Server for Clock Synchronization

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

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

Server IP/ Host Name	IP Address/ Host Name
Version	3 or 4
Server	☐ Enabled
NTP Key	1
Key	☒ Enabled

3. Specify the address of the time server in the Server IP/Host Name field. Provide the service details for which the device should be synced with the server for updating the clock time and date.

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. NTPv4 is an extension of NTPv3 that supports IPv4 and IPv6.
5. Select **Enable** to enable the server. If enabled the respective device will be synced with the NTP server to sync up the clock details.
6. Enter the NTP Key. The key is used to secure the exchange with an NTP time server.
7. Select **Enable** in the Key field to enable the Key.
8. Click **Save**.

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

Clock Management Best Practice for devices connected to GigaVUE-FM

Before adding a device to GigaVUE-FM, you must set up the clock using NTP. Additionally, ensure that both GigaVUE-FM and the connected devices are synchronized to the same clock to prevent the following issues:

- GigaVUE-FM and connected devices falling out of sync.
- License deletion due to clock fluctuations.

Perform One-Time NTP Server Synchronization

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

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

Role-Based Access: Rules and Notes

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

- [User Management](#)
- [Role Management](#)
- [Port Ownership](#)

User Management

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

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

Role Management

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

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

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

Port Ownership

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

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

Configure Logging

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

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

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

1. Using administrator user credentials, log in to GigaVUE-FM.



2. On the left navigation pane, click , and then select **Physical>Nodes**. Select the required node or cluster.
3. Select **Settings > Global Settings > Logging**.
4. Click **New Server**. The Add Log Server page appears.
5. Select the required hosts.
6. Select the logging protocol: **UDP** or **TCP**

For UDP, do the following:

- a. Enter the external server's IP address in the **Server Address** field.
- b. Port Number for UDP is 514, which is selected by default.
- c. 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 **Server 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 Port Number field.

For SSH, do the following:

- a. Use the Toggle option to enable SSH.
- b. 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.

Use the following buttons in this page to manage Logging.

Button	Description
Actions	Use the Actions drop-down button to perform the following tasks. • Sync Device: Syslog servers configured through device CLI do not get reflected in the GigaVUE-FM GUI. Click the Actions > Sync Device button for GigaVUE-FM to sync with the device and retrieve the syslog servers. GigaVUE-FM prompts a message after the syslog server retrieval is completed and the syslog servers added through the CLI get reflected in the GUI. • Edit: Use to edit the existing servers. Select the node that you want to edit and click the edit option to modify the details of the node. Note: You cannot select multiple nodes and do a bulk edit.
New Server	Use to add a new log server.

External Syslog Servers and Clustered Nodes

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

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

Delete an External Syslog Server

Remove a logging server by doing the following:

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

Packet Format for Syslog Output

Syslog packets sent by the GigaVUE HC 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 HC Series node.
- Timestamps are provided in **Mmm dd hh:mm:ss** format, where Mmm is the standard English language abbreviation of the month (for example, Jan, Feb, Mar).
- Syslog packets include the IP address of the Mgmt port.

Configure Automatic Email Notifications

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

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

Configure the Email Server Settings

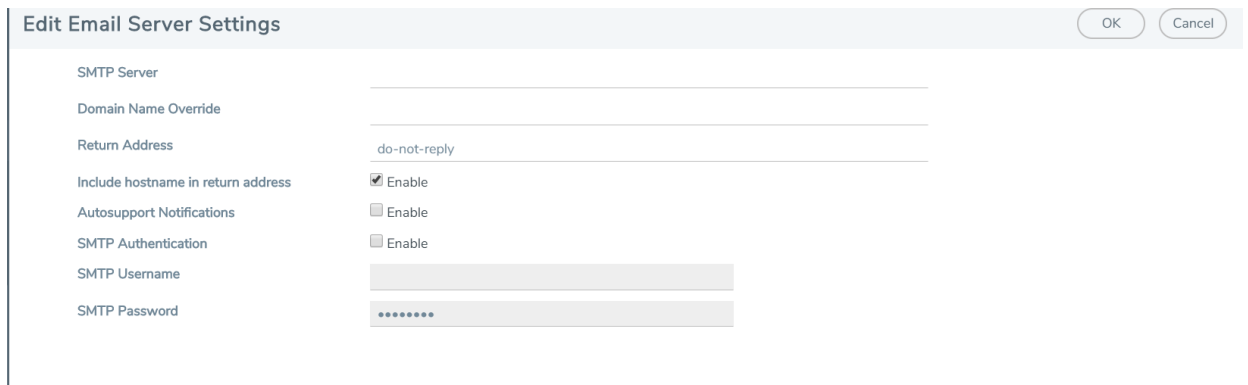
To configure the server settings for automatic email notifications for the GigaVUE node, do the following:



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

The Email Notifications page shows the current server settings, the events enabled for notification, and the recipients for the notifications.

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



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

Configure the Event Settings

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



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

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

- Select the event or events about which the email recipient should be notified.
- Click **OK**.
- Add a recipient for the notifications. For the steps to add a recipient, refer to the next section [Add Email Notification Recipients](#).

Add Email Notification Recipients

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



- On the left navigation pane, click , and then select **Physical>Nodes**. Select the required node or cluster.
- Select **Settings > Global Settings > Email Notifications**, and then click **Add**.
- 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.
- 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 or detailed output should be included in the email. Not that not all events have both summary and detail formats
 - Send info Notification** — send information about the event, but without detail.
 - Send Failure Notification** — send only notification about failure events. No email is sent when failure notification is enabled and an information event is generated.

5. Click **OK**.

Use a Custom Banner

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

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

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

Interface

The Interface page shows status information about the various interfaces.

To access the interface page:

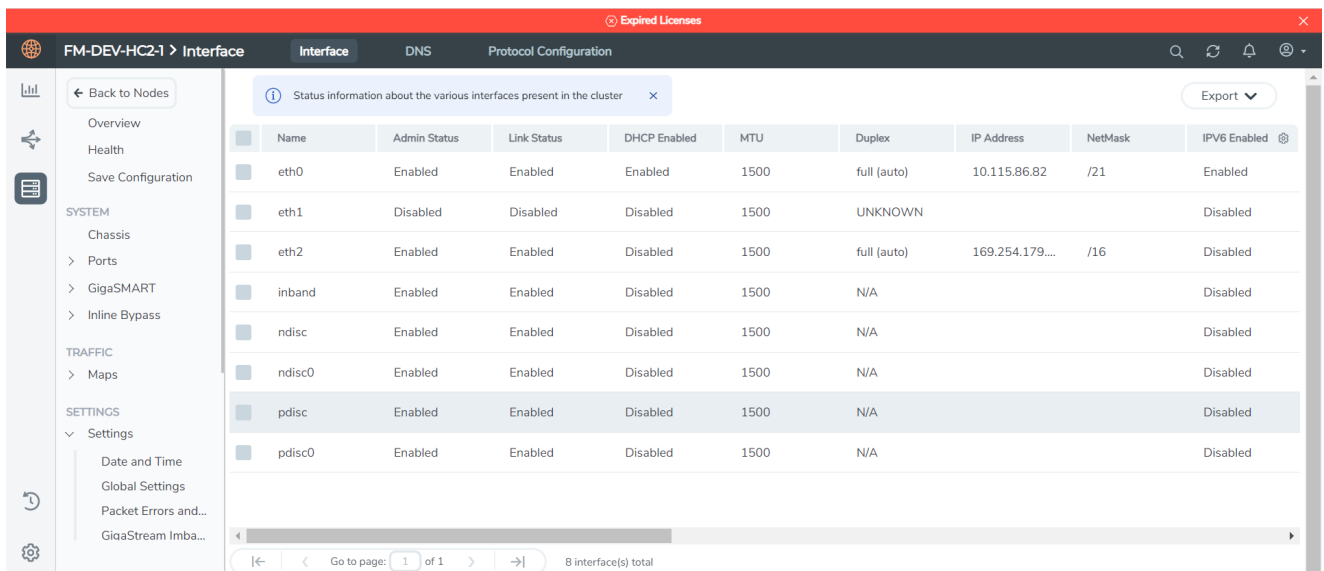
1. On the left navigation pane, go to **Inventory**  and select **Nodes**.
2. Click on a node for which you want to set the interface settings.
3. Select **Settings > Interface > Interface**. The page provides the following information:

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

- **Ethernet status information** (eth0, eth1, eth2). The number of interfaces depends on the model of the node. The following information is provided about the interface:
 - Name
 - Admin Status
 - Link Status
 - DHCP enabled

- MTU
- Duplex
- IP address
- Netmask
- IPv6 Enabled
- Autoconf enabled
- Autoconf route
- Autoconf privacy
- DHCPv6 running
- Speed
- Type
- ifindex
- ifsource
- HW addr
- Cluster Name
- Description
- IPv6 addresses
- IPv6 address
- **Interface inband status** provides information when the node is configured for inband clustering: The following information is provided about the inband interface:
 - Admin Status
 - Link Status
 - Duplex
 - MTU
 - HW addr
 - ifSource
 - Autoconf enabled
 - Autoconf privacy
 - IPv6 addresses
 - Dhcp enabled
 - Speed
 - IP address
 - Netmask
 - Type
 - ifindex
 - IPv6 enabled
 - Autoconf route
 - DHCPv6 running
 - IPv6 address

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



FM-DEV-HC2-1 > Interface

Interface DNS Protocol Configuration

Status information about the various interfaces present in the cluster

Export

Name	Admin Status	Link Status	DHCP Enabled	MTU	Duplex	IP Address	NetMask	IPv6 Enabled
eth0	Enabled	Enabled	Enabled	1500	full (auto)	10.115.86.82	/21	Enabled
eth1	Disabled	Disabled	Disabled	1500	UNKNOWN			Disabled
eth2	Enabled	Enabled	Disabled	1500	full (auto)	169.254.179...	/16	Disabled
inband	Enabled	Enabled	Disabled	1500	N/A			Disabled
ndisc	Enabled	Enabled	Disabled	1500	N/A			Disabled
ndisc0	Enabled	Enabled	Disabled	1500	N/A			Disabled
pdisc	Enabled	Enabled	Disabled	1500	N/A			Disabled
pdisc0	Enabled	Enabled	Disabled	1500	N/A			Disabled

Go to page: 1 of 1 8 interface(s) total

Figure 4 Interface Page

DNS

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

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

Cluster Safe and Limited Modes

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

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

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

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

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

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

Safe Mode

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

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

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

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

A node will automatically enter safe mode.

When a node is in safe mode:

- The node displays a banner indicating it is in safe mode. (Refer to [Cluster Safe and Limited Modes](#).)
- An SNMP trap is sent to notify the user when the mode changes.
- Configured traffic continues to be forwarded.
- Traffic provisioning is not allowed on the affected node. Any other configuration remains as is.
- If the standby node in the cluster is in safe mode, it can still become the leader if the current leader fails or switches over, but the database on the standby node may not be in sync, so it is not recommended to continue in that state. Instead, take immediate action to recover the node.
- In safe mode, the member nodes in the cluster do not process any incoming traffic configuration from the cluster leader.
- SSH is not supported in safe mode if Enhanced Cryptography is enabled. This is a requirement of FIPS. If you are working in an Enhanced Cryptography environment and the node enters in to SAFE mode, you will get a 'connection refused' error. Restart the device to recover the node from SAFE mode. SSH will work again.

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

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

Limited Mode

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

When a node is in limited mode:

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

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

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

Enable SNMP Trap for Safe Mode and Limited Mode

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

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

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

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

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

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

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

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

Collect Information for Technical Support

Collecting the following information can help Technical Support:

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

To generate a system dump file, refer to [Generate Sysdump or Debug Dump File](#).

To contact technical support, refer to [Contact Technical Support](#).

Generate Sysdump or Debug Dump File

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

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

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

Name drop-down list to generate the debug file for the respective node.

5. Click **Generate**.

To generate the system dump file for a standalone node:

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

Configure Port Packet Drop/Error in Devices

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

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

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

Packet Errors and Drop

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

Save and Apply

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

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

To configure threshold values for a specific port:

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

Alarms

Buffer Threshold (%) Rx 0 Tx 0

Utilization Threshold (%) High 0 Low 0

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

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

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

The configuration is applied to that specific port.

NOTE: To configure the threshold values globally for all the devices managed by GigaVUE-FM refer to [Configure Port Packet Drop/Error in GigaVUE-FM](#)

Related topics

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

Configure Security Options

This chapter describes how to set options relating to security – who can log into the node, how they are authenticated, and what rights they have once logged in.

The chapter includes the following sections:

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

About Security and Access

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

Security Tools	Description
Roles/Groups	Roles specify which users have access to a given port. The following built-in roles are provided: • Admin – This role provides access to all command modes, including Standard, Enable, and Configure. Admin users also have access to all commands and all ports. They are also members of all groups. • Default – This role also provides access to all command modes. Users with the Default Role has no access to unassigned ports. New users are created with the Default role automatically. However, you can remove it if you do not want to allow a user access to unassigned ports • Monitor – This built-in role provides view-only access to ports and configurations Administrators create additional custom roles and assign them to users together with the Default role. For example, if you create a role named Security_Team and assign it to tool port 5/1/x2, users assigned the Security_Team role will be able to access tool port 5/1/x2. Conversely, users without a role that gives them some access to tool port 5/1/x2 will not even be able to see it in the CLI. Users can have multiple assigned roles, allowing administrators to fine-tune access to the

Security Tools	Description
	Gigamon Deep Observability Pipeline.
Permissions	Administrators assign Permissions to specify what users can do with a port to which they have access. You can assign the following permission levels: • Level 1: Can view the port but cannot make any changes to port settings or maps. When applied to a network port, can view maps attached to the network port. This level is used for users who only need to monitor the activities of the port. • Level 2: Can use the port for maps, create tool-mirror to/from port, and change egress port filters. Can configure port-lock, lock-share, and all traffic objects except port-pair. Also includes all Level 1 permissions. • Level 3: Can configure port parameters (such as administrative status of the port, speed, duplex, and autonegotiation), as well as create port pairs. Also includes all Level 2 and Level 1 permissions. • Level 4: Can change the port type. Also includes all Level 3, 2, and 1 permissions. Permissions are hierarchical so that higher levels include all lower-level permissions (for example, a Level 3 user also has Level 2 permissions and can configure all traffic distribution, set locks, and share locks). Administrators can configure permissions differently on a port-by-port basis for a given role. This can be useful in situations where you want to give a group full authority to reconfigure maps and port parameters for a set of tool ports but only map creation permissions for a network port shared with other groups.
Port Locking/Sharing	Port locking lets a user with Level 2+ access to a port prevent other users from changing any settings for a locked port. This is useful in situations where a user needs undisturbed access to a port for short-term troubleshooting. When a port is locked, all users with Level 2+ access to the port will temporarily only have Level 1 access (read-only). Normal configured permissions are restored when the lock is released. Users can also share a locked port with any other specified user. Sharing a locked port provides the account with whom the port is shared the same port permissions as the account sharing the port. So, for example, if UserX has Level 2 permissions on port 12/5/x3, he can share a lock on 12/5/x3 with any other user account, providing them with Level 2 permissions regardless of their normal privileges on the port.
Authentication	The GigaVUE HC Series node can authenticate users against a local user database or against the database stored on an external authentication server (LDAP, RADIUS, or TACACS+). Admin users can specify the authentication methods used for logging in using AAA Authentication. Note: The serial console port always retains local authentication as a fallback option to prevent unintended lockouts.

Management Port Security

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

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

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

About Role-Based Access

GigaVUE nodes use role-based access control to manage access to the Gigamon Deep Observability Pipeline, providing different groups of users with different analysis needs full access to the packets they need for their tools. [Figure 5Role-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 5Role-Based Access in Action](#) shows 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.

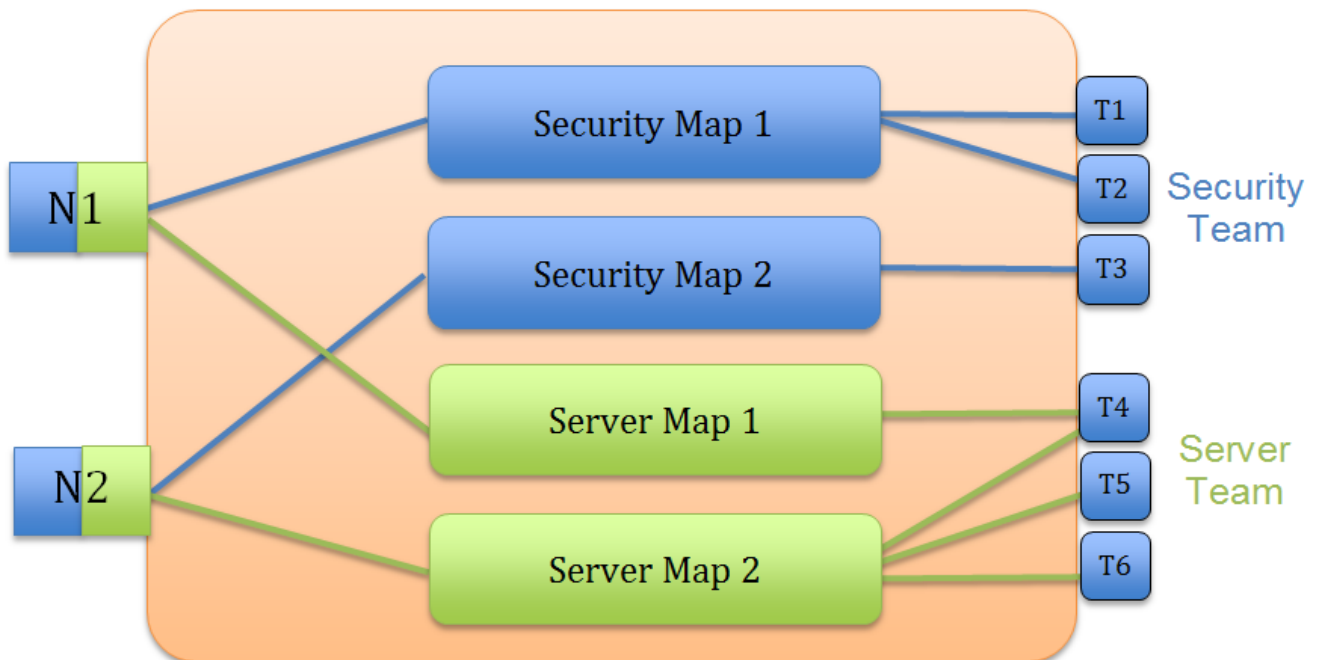


Figure 5 Role-Based Access in Action

Configure Role-Based Access: A Summary

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

Step	Description
Configure Roles	Administrators use the Roles page in the UI to create roles. At first, roles are empty containers. You can create as many as you need to share the Gigamon Deep Observability Pipeline effectively. For example, if you have an IT organization with six different groups (Security, Desktop, Application Performance Management, Server, Archive, and so on), each with different packet needs, you may want to create separate roles for each of them and assign them to different sets of tool ports. Note: The built-in “Default” role has no access to unassigned ports.
Create Users with Roles Assigned	Once you have roles created, you can assign them to users. You can assign roles to existing users or as you create new users. Users can have multiple roles assigned, giving them access to different sets of ports. Use the User page to assign roles. Keep in mind that admin-level users automatically have access to all roles. Administrators assign roles to default-level users.
Associate Roles with Ports and Permissions	The final step is to associate roles with ports and permissions. A user with a particular role will have access to all ports assigned that role at the designated permission level. Use Assigned to Roles fields on the Ports page to associate roles with ports and permissions.
Restriction for Removing a Role	An error message is displayed if you try to remove a role when it is used in a port tool-share. Remove the port tool-share first and then the role.
Fine Tune and Evolve	The Gigamon Deep Observability Pipeline 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 6Sharing Locks](#)

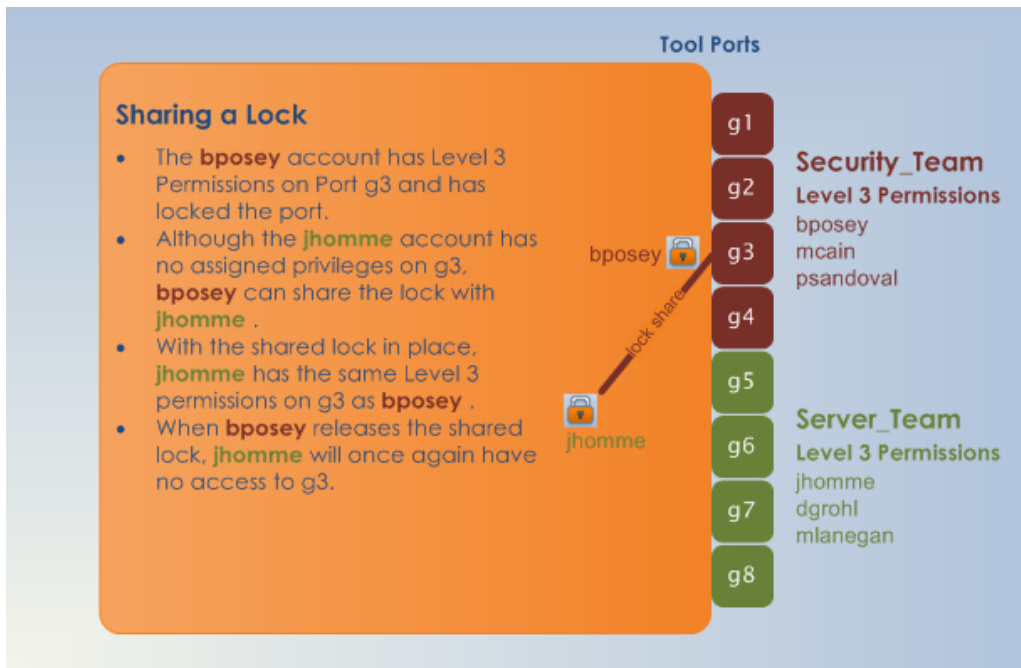


Figure 6 Sharing Locks

Notes:

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

Configure Authentication and Authorization (AAA)

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

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

Refer to the following sections for details:

- [Configure AAA Authentication Options](#)
- [Grant Roles with External Authentication Servers](#)

- [Add AAA Servers to the Node's List](#)

Overview of the AAA Page

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

Authentication Priority

The **Authentication Priority** section of the AAA page specifies which authentication methods should be used for logging in to the GigaVUE HC 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.

Maximum SSH Sessions

In the maximum number of SSH sessions section, users with administrative privileges can configure the number of concurrent SSH sessions that can be opened on a device. The range of SSH configurations supported globally is 1-10. SSH connection limit corresponds to the total active sessions across all users (not per individual user). Once the configured maximum limit is reached, the device will prevent from the opening of any new SSH sessions. The administrator can configure the maximum session limit from GigaVUE-FM or CLI.

Configure Maximum Authentication Attempts

You can set a limit of up to three authentication attempts per SSH connection by using the SSH server configuration command. Refer to the [ssh](#) section.

Change the Password on admin Account

The default password on the admin account is admin123A!. After the first login, you must change the password to a non-default value.

If you have not changed the default password before the upgrade, you will be prompted to enter a non-default password. When upgrading through the CLI, **configuration jump-start** will automatically launch and prompt the system administrator to change the password on the **admin** account. For details, refer to the [Password Policies](#) section in the *GigaVUE-OS CLI Reference Guide*.

Messages Associated with Changing the admin Account Password

There are messages associated with changing the default password on the **admin** account since this password must be changed.

If the following message is displayed, the system administrator must change the default password on the admin account:

```
ATTENTION: Admin account password must be changed to a non-default value for security purposes.
```

If the system administrator tries to change the password back to the default through the CLI, it will not be allowed and the following message will be displayed:

```
(config) # username admin password admin123A!% Default password is not allowed.
```

NOTE: Using the **reset factory** CLI command deletes passwords on user accounts. When you login with the **admin** account, you will be prompted for a new password through the **jump-start** script.

If the node was upgraded from GigaVUE-FM and the default password is in use, the first time you log in to GigaVUE-FM after the upgrade, you are required to change the default admin password through the CLI. GigaVUE-FM will display the following message:

This password is not allowed. If this is your password, you must change it through the CLI.

For changing passwords and password policies, refer to [Setup Some Basic Accounts](#) and [GigaVUE-OS Password Policies](#).

For best practices for other passwords, other than for the admin account, refer to [Best Practices for Passwords](#).

Best Practices for Passwords

To maintain the highest level of security on GigaVUE HC Series and GigaVUE TA Series nodes, customers are strongly recommended to configure passwords for all user accounts and to change default passwords. Specifically, any user accounts that have no passwords, and the default password for the admin account.

Starting in software version 5.9.00, you must configure password for the monitor account, without which you cannot login to the device.

NOTE: The monitor account is designed to give a read-only access to the GigaVUE-OS. The monitor account is disabled by default. To enable it, assign a password to the account. GigaVUE-FM users can use the monitor account as long as it is enabled (has a password).

To change the password on the default **monitor** account, do the following:

1. Log in to GigaVUE-FM as the **monitor** user.
2. Click on the **monitor** menu in the UI header and select **Change Password**.
3. On the Change Password for “monitor” page, enter a new password in the **New Password field** and confirm the password in the **Confirm New Password** field.

When entering the new password, the system displays “Invalid Password” underneath the New Password field until the password meets the password criteria described in [GigaVUE-OS Password Policies](#).

4. Click **Save**.

The system logs you out of the system to reset the password. To log in again as the monitor user, use the password created in [Step 3](#).

User accounts with no password configured should be updated to include a password. Alternatively, a user account without a password configured can be disabled by doing the following:

1. Log in as the **admin** user.
2. Select **Roles and Users > Users**.
3. On the User Setup page, select the user whose account you want to disable and then click **Edit**.
4. On the Edit User page, make sure the **Enable** checkbox is not selected.
5. Click **Save**.

The system displays a message if the account was updated successfully and the Enabled field shows false, indicating the user account is no longer enabled.

User accounts that do not have passwords set can also be disabled. Refer to [Configure Secure 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.

GigaVUE-OS Password Policies

GigaVUE-OS Nodes observes several policies designed to ensure strong password protection for user accounts.

Policy	Description
Password Standards	Passwords must meet the following standards: • include 8-30 character • include at least one numeral • include at least one lower case letter • include at least one upper case letter • include at least one special character (for example, !, #, \$, %, ^, &, or * –ASCII 0x21, 0x2F, 0x3A, 0x40, 0x5B, 0x5F, 0x7B, 0x7E) Note: .The following special characters are not supported: • " • / • ? However, you can use these characters in the password as described in GigaVUE-OS Password Policies section. • must not include user-name or parts of full-name
Password Recommendations	The following are password recommendations: • passwords should be configured on all user accounts • passwords should be changed on default accounts such as the monitor account • passwords should be unique, meaning never used elsewhere or at another time • passwords should not be shared, meaning each user account should have their own password • passwords should be long, meaning at least 15 to 20 characters • passwords should be complex, meaning a mix of numerals, upper case letters, lower case letters, and special characters Note: It is recommended that you do not include the at sign, @, in passwords. Under some circumstances, this can lead to the failure of some CLI commands, such as image fetch or configuration upload. Note: The monitor account is designed to give a read-only access to the GigaVUE-OS. The monitor account is disabled by default. To enable it, assign a password to the account. GigaVUE-FM users can use the monitor account as long as it is enabled (has a password).

Policy	Description
Password Change Rights	Only admin users can change the passwords of other users.
Password on Default admin Use	The password on the default admin account must be changed during initial configuration using configuration jump-start. If the following message is displayed, the system administrator must change the default password on the admin account: ATTENTION: Admin account default password must be changed for security. If the system administrator tries to change the password to the default, it will not be allowed and the following message will be displayed: Default password is not allowed. If the node was upgraded through GigaVUE-FM and the default password for the admin account has not been changed, the following message is displayed: Admin account password must be changed via the CLI to a non-default value for security purposes.

FAQ for Logins and Passwords

This section answers frequently asked questions for logins and passwords.

Do Passwords Expire?

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

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

What Happens After Unsuccessful Logins?

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

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

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

Can a User be Forced to Change Their Password?

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

Are Passwords Displayed?

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

Who Creates Users and Passwords?

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

Configure AAA Authentication Options

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

The valid authentication the authentication methods are:

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

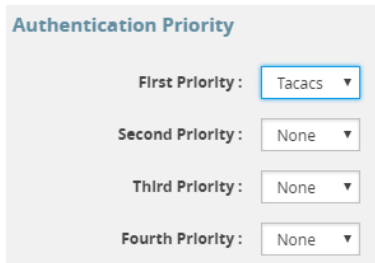
You can enable any of or all of the authentication methods ((TACACS+, RADIUS, LDAP, and local) at the same time. If you enable more than one method, the GigaVUE HC Series node uses the methods in the same order in which they are specified, falling back as necessary:

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

Refer to the following examples.

Example 1

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

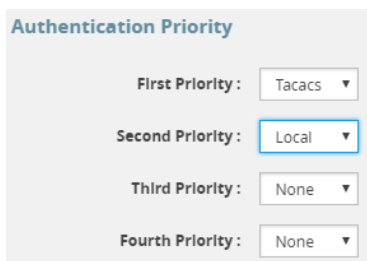


The image shows a configuration window titled "Authentication Priority". It contains four rows, each with a label and a dropdown menu. The first row is "First Priority" with "Tacacs" selected. The second row is "Second Priority" with "None" selected. The third row is "Third Priority" with "None" selected. The fourth row is "Fourth Priority" with "None" selected.

Priority	Method
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:

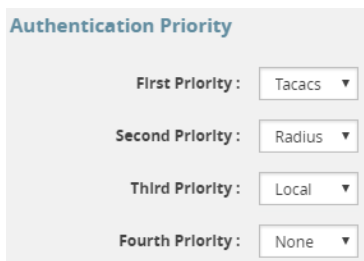


The image shows a configuration window titled "Authentication Priority". It contains four rows, each with a label and a dropdown menu. The first row is "First Priority" with "Tacacs" selected. The second row is "Second Priority" with "Local" selected. The third row is "Third Priority" with "None" selected. The fourth row is "Fourth Priority" with "None" selected.

Priority	Method
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:



The image shows a configuration window titled "Authentication Priority". It contains four rows, each with a label and a dropdown menu. The first row is "First Priority" with "Tacacs" selected. The second row is "Second Priority" with "Radius" selected. The third row is "Third Priority" with "Local" selected. The fourth row is "Fourth Priority" with "None" selected.

Priority	Method
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 7 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.

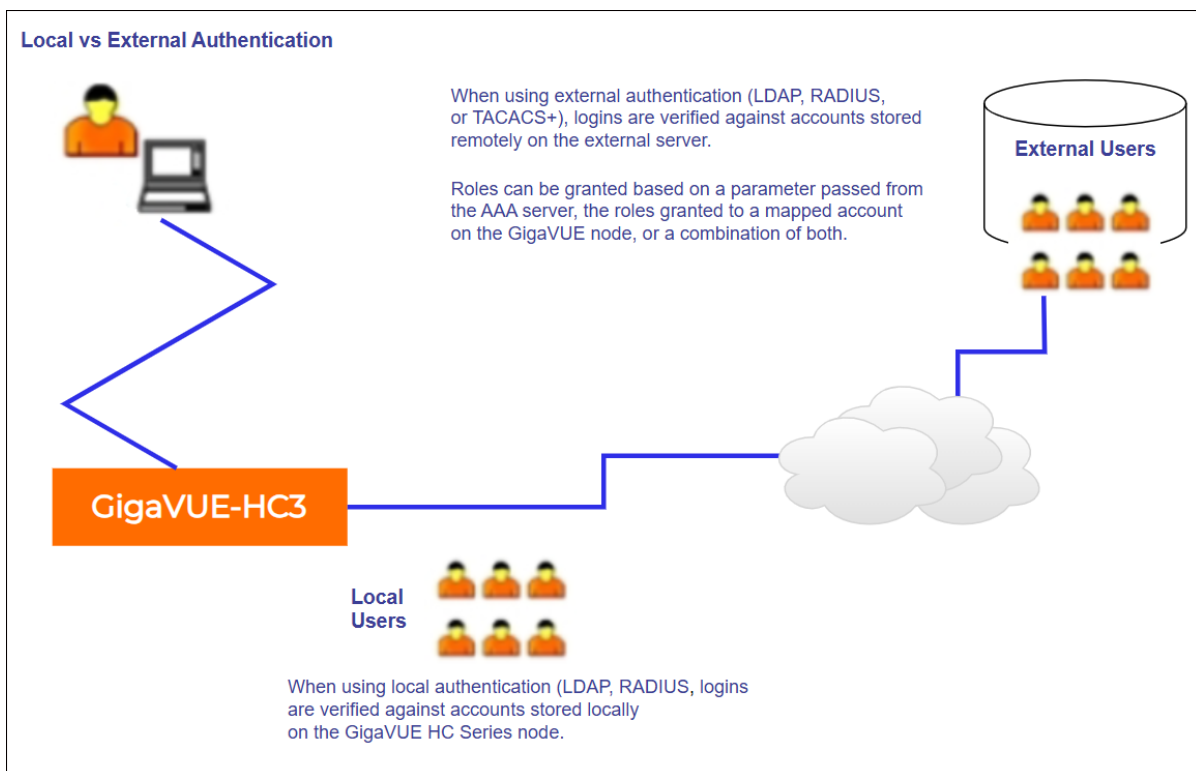
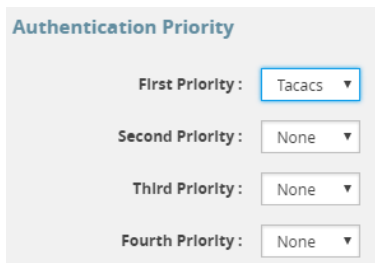


Figure 7 Local vs. External Authentication

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

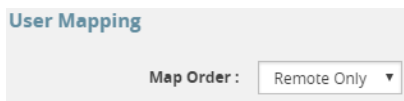
First Priority: Tacacs ▼

Second Priority: None ▼

Thlrd 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](#).

Authorization of User Account

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

Next Steps

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

- Add the RADIUS, TACACS+, or LDAP server to the GigaVUE HC Series node's list using the corresponding **RADIUS**, **TACACS+**, or **LDAP** pages. Refer to [Add AAA Servers to the Node's List](#).

- Set up GigaVUE HC Series nodes and users within the external authentication server itself. Depending on your authorization model, you can grant privileges to externally authenticated users based on the roles assigned to a corresponding account on the local node, the roles passed from the AAA server, or a combination of both. Refer to [Grant Roles with External Authentication Servers](#) for details.

Grant Roles with External Authentication Servers

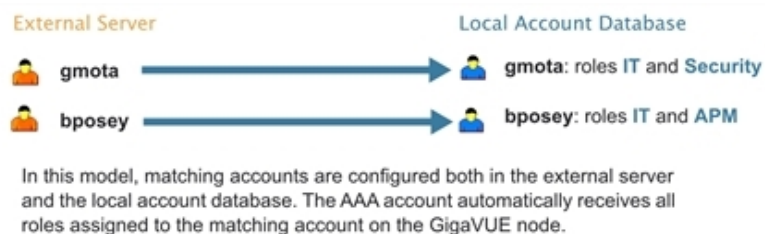
Roles are configured on the GigaVUE HC Series node itself. Roles consist of a set of ports and permission levels specifying what a user with the role assigned can do on the port.

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

- [Use Local Role Assignments](#)
- [Use AAA Server Role Assignments](#)
- [Use Combination of Local and AAA Role Assignments](#)

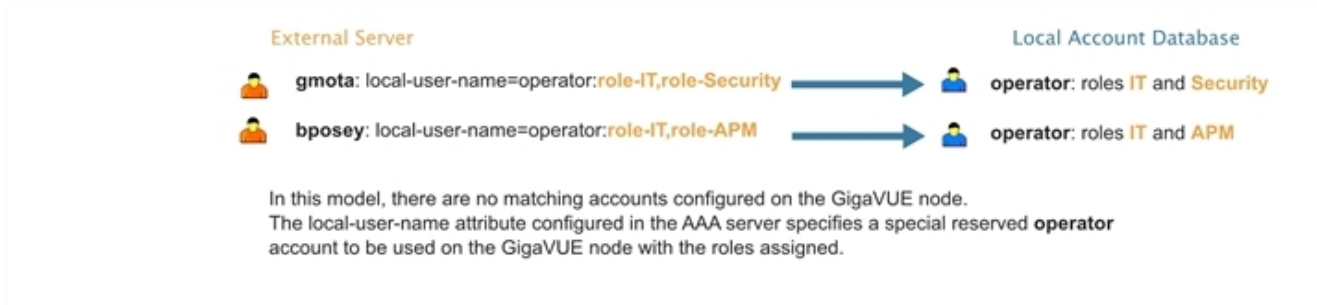
Use Local Role Assignments

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



Use AAA Server Role Assignments

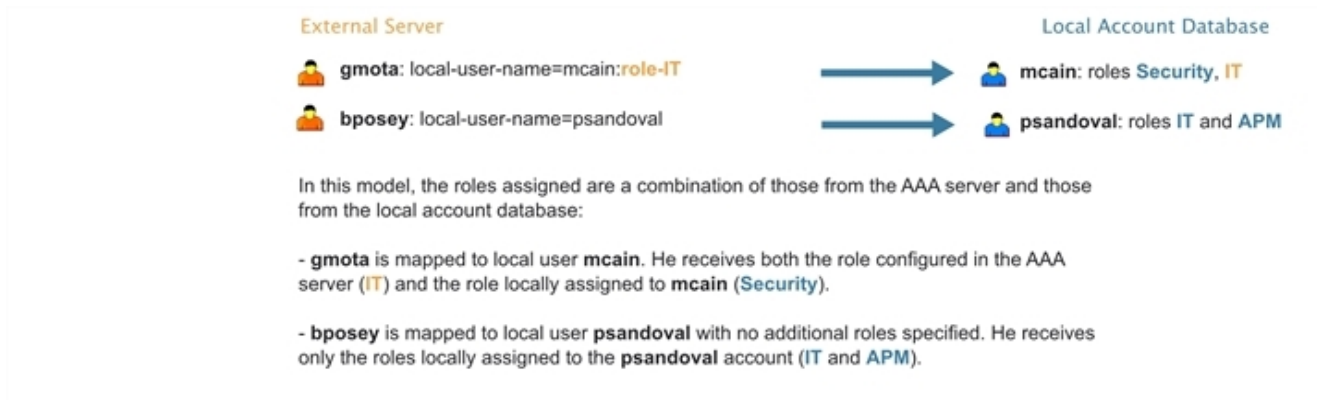
In this model, you configure the GigaVUE node to accept roles passed from the AAA server. Then, you set up a **local-user-name** attribute for the account in the AAA server to pass a reserved account name (**operator**) and one or more roles to the GigaVUE node. In this case, the roles are fully assigned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



Use Combination of Local and AAA Role Assignments

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

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



Assign Role in AAA Servers

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

Create Users for AAA and Remote Authentication Server

To create users for AAA and the remote authentication server:

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

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

The screenshot shows the AAA configuration interface. At the top, there are tabs for 'Authentication', 'Authentication Type', 'RADIUS', 'TACACS+', and 'LDAP'. The 'Authentication' tab is active. Below it, the 'Authentication Priority' section has four dropdown menus: 'First Priority' (Tacacs), 'Second Priority' (None), 'Third Priority' (None), and 'Fourth Priority' (None). A message below states: '* You are currently unauthorized to authenticate against: Local'. The 'User Mapping' section has two dropdowns: 'Map Order' (Remote Only) and 'Map Default User' (operator). The 'Password' section has a checkbox for 'Enabled' (checked) and a 'Duration' field set to 90 Days.

The settings in the example configuration are as follows:

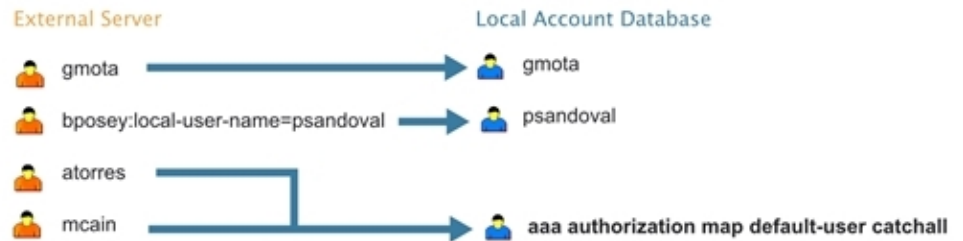
- AAA authorization:
 - Map Order: Remote Only means the user has a local account matching the external username account.
 - Map Default User: networker is a common user member of internal netops role and TACACS+ netops group.
- Authentication method(s):
 - Tacacs means that TACACS+ is the only authentication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

Configure AAA Authorization

For details on the AAA authorization command, refer to [Overview of the AAA Page](#).

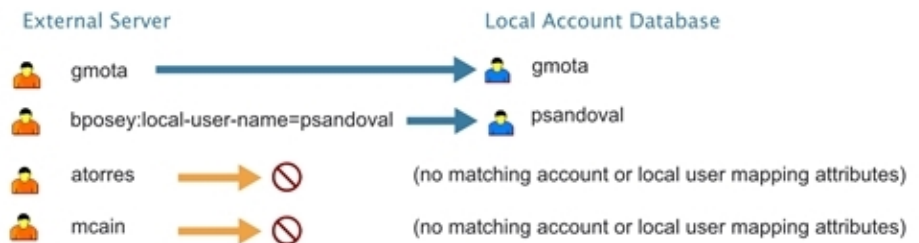
map order = remote-first

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



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)



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).

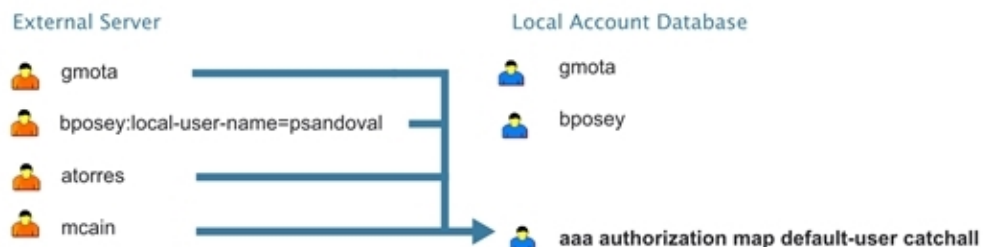


Figure 8 How the **map order** Argument Works

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 RADIUS server at IPv4 address 192.168.0.62 to the GigaVUE HC Series node's list.

- Select **Settings > Authentication > Radius**.
- Click **Add**. The Add Radius Server page displays.
- For **Enabled** select **Yes**.
- In the **Server IP** field, enter 192.168.0.62
- In the **Key** field, enter gigamon.
- Click **Save**.

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

Add AAA Servers to the Node's List

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

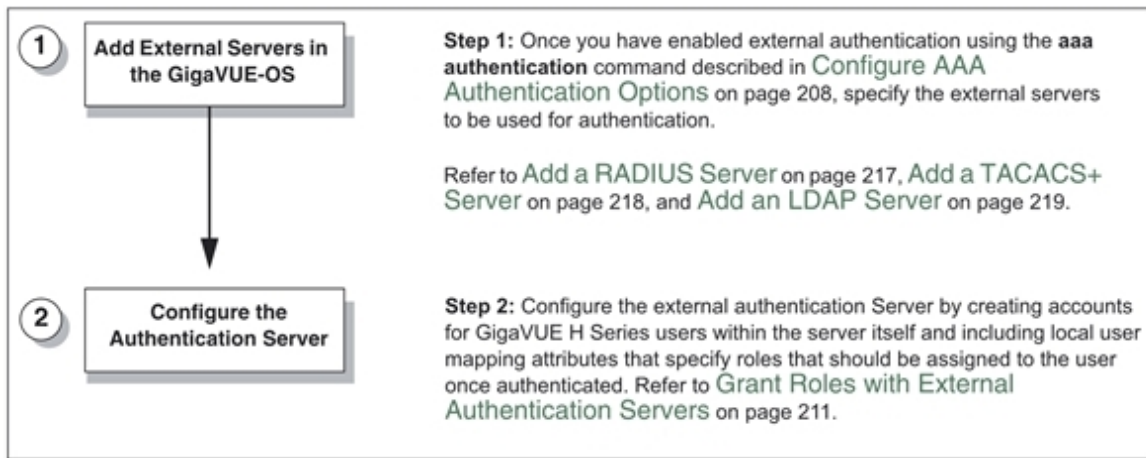


Figure 9 Steps to Use the Node with an External Authentication Server

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.

Use the following buttons to manage the RADIUS server.

Add	Use to add a RADIUS server. Refer to Add a RADIUS Server section for details.
Actions	Use to perform the following tasks: Edit: Use to edit the RADIUS server configuration. Delete: Use to delete the selected RADIUS server. Refer to Delete a RADIUS Server for details.
Default Settings	Use to apply the default settings for RADIUS
Export	Use to export the selected RADIUS servers or all RADIUS servers in CSV or XLSX format.

Add a RADIUS Server

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 Server page. For an example, refer to [Figure 10 Adding a Radius Server](#).

- a. You can enter either an IPv4 or IPv6 address for the **Server IP/DNS Name**. The same IP address can be used for more than one RADIUS server if the **Auth Port** values are different.
 - b. Specify the shared secret key to be used for encryption of authentication packets sent between the GigaVUE HC Series node and this specific RADIUS server.
4. Click **Apply** to save the configuration.

The screenshot shows the 'Authentication' configuration page for RADIUS. The 'Authentication Type' is set to RADIUS. The 'Add RADIUS Server' section contains the following fields:

- Enabled:** A dropdown menu set to 'Yes'.
- Server IP/DNS Name:** A text input field with the placeholder 'Enter Server IP/DNS Name'.
- Auth Port:** A text input field containing '1812'.
- Shared Secret:** A text input field containing '114135'.
- Use defaults for following:** A checkbox that is checked.
- Timeout:** A text input field containing '3'.
- Retransmit:** A text input field containing '1'.

At the bottom of the page, there are two status bars: 'Attempted Sync Time: Aug 29, 2023 14:07:02' and 'Successful Sync Time: Aug 29, 2023 14:07:02'.

Figure 10 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 **Actions** button and select **Delete**.

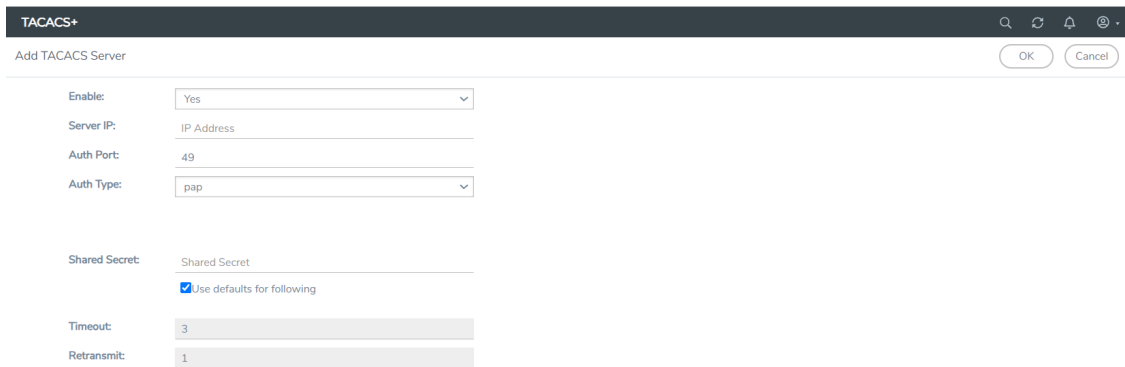
Add a TACACS+ Server

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 TACACS server, do the following:

1. Select **Settings > Authentication > TACACS+**.

2. Click **Add**.
3. Enter the TACACS information on the ADD TACACS Server page. For an example, refer to [Figure 11 Adding a TACACS Server](#)
4. Click **Save**.



The screenshot shows the 'Add TACACS Server' configuration page. The form includes the following fields and values:

Field	Value
Enable	Yes
Server IP	IP Address
Auth Port	49
Auth Type	pap
Shared Secret	Shared Secret
Use defaults for following	☒
Timeout	3
Retransmit	1

Figure 11 Adding a TACACS Server

Delete a TACACS+ Server

To delete a TACACS+ 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 field on the Add TACACS Server page (select **Settings > Authentication > TACACS > Add**.)

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

Add an LDAP Server

Admin users use the **LDAP** page to specify the LDAP servers to be used for authentication. You can specify multiple LDAP servers. Servers are used as fallbacks in the same order they are specified—if the first server is unreachable, the second is tried, and so on, until all named servers have been used. If a server is reachable and authentication fails, the authentication process terminates.

To add an LDAP Server, do the following:

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

For Common Criteria, specify SHA password hashing when configuring the remote LDAP server. For details on Common Criteria, refer to [Common Criteria](#).

Set the LDAP Server Default Settings

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

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

Table 2: LDAP Default Settings

Default Setting	Description
User Base DN	Identifies the base distinguished name (location) of the user information in the schema of LDAP server. 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

Default Setting	Description
	• 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 HC 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 can select one 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. This is a global setting. It cannot be configured on a per-host basis.
Timeout	Specifies how long the GigaVUE HC 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 HC 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

Default Setting	Description
	the default ports.
SSL Port	Configures LDAP SSL port number.
SSL Cert Check	Enables LDAP SSL/TLS certificate verification. Use Off to disable.
SSL ca-list	Configures LDAP to use a supplemental CA list. Set to default Ca list to use the CA list configured with the Enhanced Cryptography (refer to Configure Enhanced Cryptography Mode). Set to None if you do not want to use a supplemental list.

Delete an LDAP Server

To delete an LDP Server, do the following:

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

Configure an IPv6 Address

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

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

Configure Roles in External Authentication Servers

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

- [Grant Roles with External Authentication Servers](#)
- [Configure Cisco ACS: RADIUS Authentication](#)
- [Configure Cisco ISE: RADIUS Authentication](#)
- [Configure Cisco ACS: TACACS+ Authentication](#)
- [Configure Cisco ISE: TACACS Authentication](#)
- [Configure LDAP Authentication](#)

Configure Cisco ACS: RADIUS Authentication

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

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

Enable Extra Roles for RADIUS on the GigaVUE Node

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

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

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

In the Cisco Secure ACS screen:

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

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

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

Configure Cisco ISE: RADIUS Authentication

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

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

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

CISCO ISE RADIUS Configuration	
Local user account configuration	
User 1 with admin auth profile	<pre>username adminauthprofile password 7 \$1\$Nc/LLAFM\$EwiU.qjNQHoqnWSaqQiNG0</pre>
User 2 with read only auth profile	<pre>no username nonadminauthprofile disable username nonadminauthprofile full-name "" username nonadminauthprofile roles replace monitor</pre>
AAA remote server configuration	Assume the radius server host as 1.1.1.1. Add this radius-server to the GigaVUE-OS HC Series nodes list using the following commands: <pre># radius-server host 1.1.1.1 # radius-server host 1.1.1.1 key ***** # radius-server extra-user-params roles enable</pre>

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

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

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

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

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

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

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

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

Configure Cisco ACS: TACACS+ Authentication

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

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

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

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

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

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

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

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

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

Configure Cisco ISE: TACACS Authentication

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

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

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

CISCO ISE RADIUS Configuration	
Local user account configuration	
User 1 with admin auth profile	<pre>username adminauthprofile password 7 \$1\$Nc/LLAFM\$EwiU.qjNQHoqnWSaqQING0</pre>
User 2 with non admin auth profile (that replaces the monitor role)	<pre>no username nonadminauthprofile disable username nonadminauthprofile full-name "" username nonadminauthprofile roles replace monitor</pre>
AAA remote server configuration	<pre>Assume tacacs server host as 1.1.1.1 and shared key as *****. tacacs-server host 1.1.1.1 timeout 5 retransmit 3 # tacacs-server host 1.1.1.1 key ***** #tacacs-server extra-user-params roles enable # tacacs-server key ***** tacacs-server retransmit 3 tacacs-server service Gigamon tacacs-server timeout 5</pre>
AAA Configuration	<pre>aaa authentication login default tacacs+ local aaa authorization map default-user monitor aaa authorization map order remote-first</pre>

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

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

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

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

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

Configure LDAP Authentication

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

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

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

- a. Select **Settings > Authentication > LDAP**.
- b. Click **Default Settings**.
- c. Set the **Extra Roles** field to **Yes**.

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

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

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

The attribute format is as follows:

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

Supported Clients

The following versions of serial, SSH clients are supported:

Table 3: Tested SSH Clients

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

Default Ports

The following default ports are normally open on GigaVUE nodes:

Table 4: Open Default Ports

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

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

Table 5: Default Ports, Normally Closed

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

Port Number	Description
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 Compliance in GigaVUE-FM

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

Refer to the following sections for details:

Rules, Notes and Limitations

Refer to the following rules and notes for FIPS:

- After upgrading GigaVUE-FM instance from pre 5.16.00 to 5.16.00 or above, GigaVUE-FM boots in non-FIPS mode.
- FIPS is disabled by default in GigaVUE-FM. You can enable FIPS whenever needed. However, once enabled you cannot disable it.
- Only users with super admin privileges can enable FIPS.

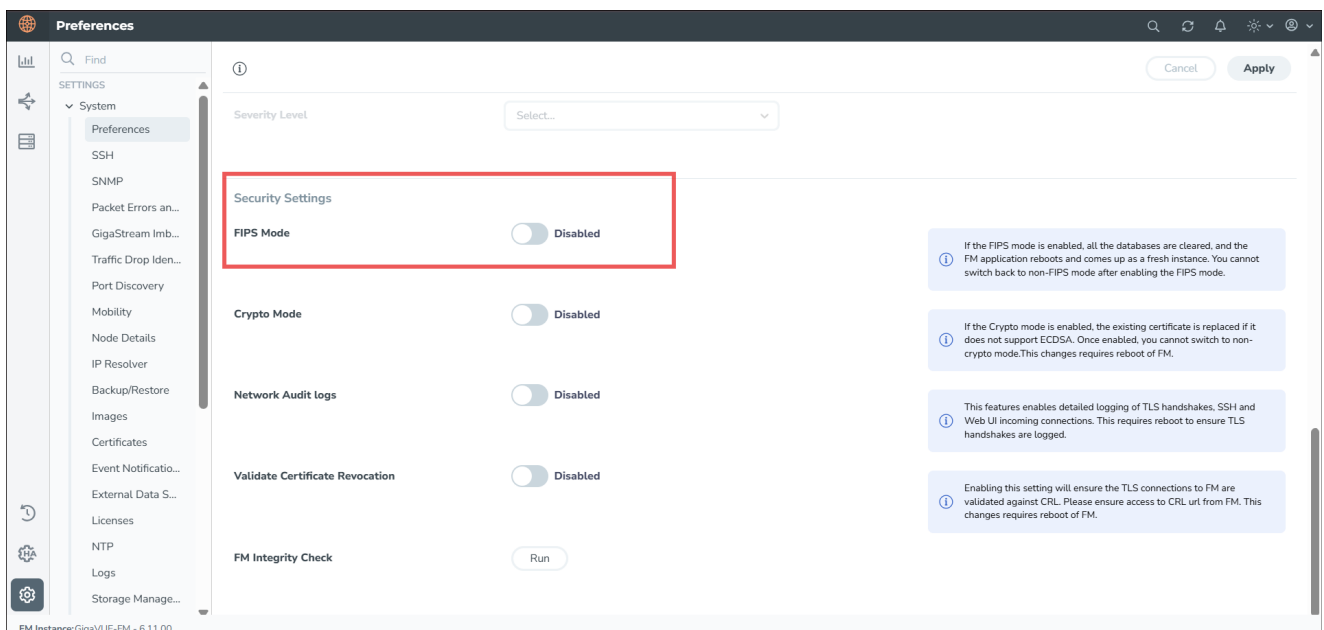
Refer to the Frequently Asked Questions section for further details.

Configure FIPS in GigaVUE-FM

To configure FIPS in GigaVUE-FM:

1. Go to **Settings** and go to **System > Preferences**.
2. Under **Security Settings**, enable the **FIPS Mode**.
3. Click **Apply** to save the changes.
4. GigaVUE-FM will restart automatically after switching to FIPS Mode. Once the reboot completes, clear your browser cache and cookies to ensure the GigaVUE-FM IDP URL loads correctly.

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



Configure FIPS in GigaVUE-FM High Availability Group

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

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

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

Enabled TLS Cipher Suites

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

Supported TLS 1.2 Ciphers

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

Frequently Asked Questions

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

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

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

Can you enable FIPS using the `fmctl` command?

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

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

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

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

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

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

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

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

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

Legacy Mode in GigaVUE-OS

Legacy cryptography mode allows older SSH and TLS clients to connect to the device by enabling weaker, outdated encryption algorithms. Use this mode only when you must support legacy systems, because it reduces the overall security of the device.

In Classic mode, the device uses strong, modern encryption algorithms by default. When you switch to Legacy mode, the device adds older algorithms such as SHA-1-based key exchanges and message authentication codes, so older clients can still connect.

Legacy mode affects the following services:

- SSH, SCP, and SFTP
- HTTPS
- LDAPS
- SMTP

To turn Legacy mode on, use:

system security legacy

To turn it off, use:

no system security legacy

When you enable Legacy mode, the device displays a warning because the weaker algorithms may expose your environment to security risks. When you disable Legacy mode, the device reminds you to test SSH access to ensure that current clients still work.

To check whether Legacy mode is enabled, run:

show system security

The output includes a **Legacy mode** field. If Legacy mode is active, the login banner also shows **Classic mode (legacy)**.

Legacy mode cannot run at the same time as Secure Cryptography mode or FIPS mode. If either of those modes is enabled, you must disable it before you can enable Legacy mode.

Argument	Description
security legacy	In legacy mode, the following algorithms are enabled: Key Exchange Algorithms ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha256 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha1 MACs hmac-sha2-512 hmac-sha2-256 hmac-sha1
TLS Cipher	The following TLS ciphers are supported when legacy mode is enabled: TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256 ECDHE-PSK-AES256-CBC-SHA384 RSA-PSK-AES256-CBC-SHA384 DHE-PSK-AES256-CBC-SHA384 ECDHE-PSK-CAMELLIA256-SHA384 RSA-PSK-CAMELLIA256-SHA384 DHE-PSK-CAMELLIA256-SHA384 PSK-AES256-CBC-SHA384 PSK-CAMELLIA256-SHA384 ECDHE-PSK-AES128-CBC-SHA256 RSA-PSK-AES128-CBC-SHA256 DHE-PSK-AES128-CBC-SHA256 ECDHE-PSK-CAMELLIA128-SHA256 RSA-PSK-CAMELLIA128-SHA256 DHE-PSK-CAMELLIA128-SHA256 PSK-AES128-CBC-SHA256 PSK-CAMELLIA128-SHA256 ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384

Argument	Description
	ECDHE-ECDSA-AES128-GCM-SHA256
	ECDHE-RSA-AES128-GCM-SHA256
	ECDHE-ECDSA-AES256-SHA384
	ECDHE-RSA-AES256-SHA384
	ECDHE-ECDSA-AES128-SHA256
	ECDHE-RSA-AES128-SHA256

Refer to [Web](#), for the supported TLS Cipher Suites.

UC APL Compliance

GigaVUE HC Series products are compliant with Unified Capabilities Approved Products List (UC APL).

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

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

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

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

Configure UC APL

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

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

Accept DoD Web Server Certificates

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

(config) # web https require-dod-cert

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

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

Enable Login Failure Tracking

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

(config) # aaa authentication attempts track enable

Disable login failure tracking with the following CLI command:

(config) # no aaa authentication attempts track enable

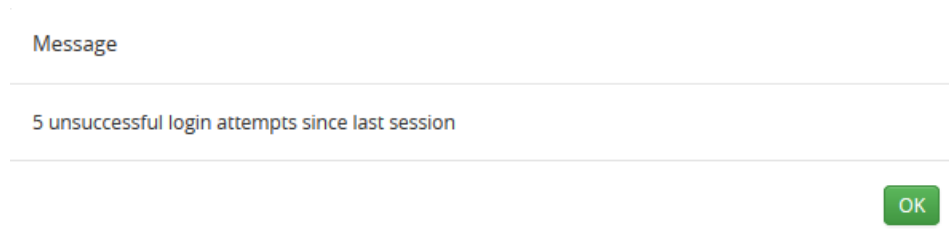
Unsuccessful login attempts are displayed on the CLI. Refer to [Display Unsuccessful Login Attempts](#).

Display Unsuccessful Login Attempts

UC APL requires the system display the number of unsuccessful login attempts since the last successful login for a particular user when they log in. An unsuccessful login attempt includes an incorrect username or incorrect password.

After an unsuccessful login attempt, there is a delay of a few seconds before you can attempt to log in again.

If there has been an unsuccessful login attempt, a message is displayed in the UI when you successfully log in.



If there have not been any unsuccessful login attempts, no message is displayed.

Common Criteria

The Common Criteria for Information Technology Security Evaluation, or Common Criteria, is an international standard (ISO/IEC 15408) for computer security certification.

Common Criteria is a framework in which computer system users can specify their security functional requirements and security assurance requirements (SFRs and SARs, respectively) through the use of Protection Profiles (PPs), vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if those claims are met.

Common Criteria provides assurance that the process of specification, implementation, and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner, at a level that is commensurate with the target environment for use.

Common Criteria is used as the basis for a Government driven certification scheme. Typically, evaluations are conducted for the use of Federal Government agencies and critical infrastructure.

Gigamon is actively keeping our products certified. Visit the NIAP CCEVS website to see the current GigaVUE-OS and models that are currently certified or check which version of the GigaVUE-OS is currently in-evaluation.

Configure Common Criteria

To make a GigaVUE node certified with Common Criteria, the following configuration steps are required:

- enable enhanced cryptography mode. Refer to [Configure Enhanced Cryptography Mode](#).
- enable secure passwords mode and configure a password length of 15. Refer to [Configure Secure Password](#).
- configure syslog to send audit data securely. Refer to [Encrypt Syslog Audit Data](#).

Implementing the following security configuration changes will not be immediately reflected in the GigaVUE-FM GUI:

- Enabling or disabling Secure Cryptography Enhanced mode
- Enabling or disabling Secure Password mode
- Switching from Secure Cryptography Enhanced to FIPS 140-3 mode

The lapse is due to the time taken for the device to reboot and implement the security configuration changes. The changes will be reflected in the GigaVUE-FM GUI after the next config sync cycle.

Configure Enhanced Cryptography Mode

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

The enhanced cryptography mode is disabled. There are two steps to enable it:

- Configure the mode.
- Reload either the node, if it is a standalone, or cluster, if the node is in a clustered environment.

NOTE: Refer to the GigaVUE Release Notes for the latest browser support information for Secure Cryptography Mode.

Enable Enhanced Cryptography Mode

To enable enhanced cryptography mode do the following:

1. Select **Settings > Global Settings > Security Settings**.
2. Use the toggle option to enable **Secure Cryptography Enhanced** option.
3. Click **Apply** to save the configuration.

If you enable enhanced cryptography, the FIPS mode will be disabled.

Ciphers to Use with Enhanced Cryptography Mode

Use the following ciphers with enhanced cryptography mode:

Secure Cryptography Mode

All Platforms

AES128-CBC

AES256-CBC

NOTE: Refer to the GigaVUE Release Notes for the latest cipher support information in Secure Cryptography Mode.

Use the following ciphers with normal (non-secure) cryptography mode:

Normal Cryptography Mode		
GVCCV2	Other PowerPC Platforms	Intel Platforms
AES128-CTR AES192-CTR AES256-CTR	AES128-CTR AES192-CTR AES256-CTR	AES128-CTR AES192-CTR AES256-CTR AES128-CBC AES256-CBC

Cryptographic Algorithms

When enhanced cryptography mode is enabled, the cryptographic algorithms are limited as follows:

SSH Host Key Algorithm	SSH Key Exchange	Encryption Algorithms	Hash-based Message Authentication Code
ECDSA	Diffie-Hellman-group14-sha1	AES128-CBC, AES256-CBC	HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-512

Status of Enhanced Cryptography Mode

If enhanced cryptography mode is configured on a GigaVUE node, once the node or cluster has been reloaded, a status is displayed when you log in.

Configure Secure Password

A secure password is a unique combination of letters, numbers, and symbols that is difficult for others to guess. Using strong passwords helps protect your accounts and sensitive information from unauthorized access.

Enable Secure Password Mode

To enable secure password mode:



1. From the left pane, click **(Inventory)**.
2. Select **Nodes**.
3. Click **Cluster ID**.
4. Go to **Settings > Global Settings > Security**.
5. Use the toggle button to enable the **Secure Passwords** option. The Secure Passwords are disabled by default.
6. Click **Apply**.

The system displays a notification that the security settings have been updated.

Set up the Secure Password

When you create a password from the User Setup page, the password must contain at least one character of each of the following:

- at least 8 characters and up to a maximum of 64 characters in length
- uppercase letters
- lowercase letters
- numbers
- special characters, for example, !, @, #, \$, %, ^, &, or *
- at least eight characters must differ from the old password and the new password

In all cases, each character at every position is unique. Since the new password exceeds eight characters in length and satisfies all other criteria, it will be accepted.

For example, the following table provides guidance on setting up a secure password.

Old Password	New Password
gigamon123A!!	!!gigamon123A
gigamon123A!!	GIGAMON123a!!

To create a user and set the password:



1. From the left pane, click **(Inventory)**.
2. Select **Nodes**.
3. Click **Cluster ID**.
4. Go to **Settings > Global Settings**.
5. Select **Roles and Users > Users**.
6. On the User Setup page, click **Add**. The Add New User page appears.

7. Enter the account details for the user, including Name, Password, Current admin Password, New Password, and Confirm Password.
8. Click **Save**.

Refer to [System](#) for details.

Encrypt Syslog Audit Data

Syslog audit data, such as messages and traps, are usually sent unencrypted between a GigaVUE node and the syslog server using UDP over port 514. The messages are sent in plain text. To allow secure transmission, starting in software version 4.4, you can send encrypted syslog audit data by using TCP and SSH options.

Sending syslogs over TCP provides a more reliable transport than UDP, with no dropped data. Tunneling using SSH provides encryption of syslog data.

On the GigaVUE node, the procedure for sending encrypted syslog audit data is as follows:

- identify the TCP port on which the syslog server is listening. (Refer to your syslog server administrator for the port number.)
- configure the TCP port of the syslog server on the GigaVUE node
- generate a public key to allow authentication between the GigaVUE node and the syslog server
- configure a secured connection

On the syslog server, integrate the key into the authorized keys.

NOTE: There can be multiple logging servers. SSH is optional for each logging server.

Encryption Procedure

Use the following sample procedure to encrypt syslog audit data:

1. Generate the public key (for example, using the admin user) with the following steps.

NOTE: The SSH Server needs to be enabled before completing these steps.

- a. Select **Settings > Global Settings > SSH**.
- b. Click **Add**. The SSH Client Key page appears.
- c. In the **Username** field, enter admin and select **rsa2** for **Type**.

- d. Click Generate **Client Keys** and copy the key contents.
2. Log in to the syslog server to paste the key, and then do the following:
 - a. Change the directory to `.ssh`.
 - b. Edit the `authorized_keys` file, located in the `.ssh` directory, using any editor (such as `vi`), then paste the key contents.

If the `authorized_keys` file does not exist, create it

If the `authorized_keys` file exists but does not have write access, change the access; for example, `chmod 644 authorized_keys`
 - c. Change the access on the `authorized_keys` file back to secure. For example, `chmod 600 authorized_keys`
3. Configure the secured TCP connection.
 - a. Select **Settings > Global Settings > Logging**.
 - b. Click **Add**.
 - c. On the Add Loggings Settings page, select **SSH**.
 - d. Enter an IP address, Log Level, TCP port, and user name.

Note: You can specify an IPv4, IPv6, or hostname.
 - e. Click **Save**.

NOTES:

- To ensure the TCP connection is established, check the syslog server logs.
- If the TCP connection goes down, an attempt to re-establish the connection occurs every minute.
- If the database on the GigaVUE node is reset, a new public key will have to be generated and set up.
- In a cluster environment, the public key will be synchronized over the cluster so that all the nodes in the cluster can establish TCP/SSH connections.

Display Logging Information

To display logging information, select **Settings > Global Settings Logging**. This displays the Logging page. [Figure 12Logging Page](#) shows an example.

Global Settings Security Web SNMP SNMP v3 Users SNMP Traps SSH Hostname **Logging** Event Notification Email Notifications

ARP/NDP

Log Setting Total Nodes: 2 Add Server OK Cancel

Host Name	Logging	Server	Server Log Level	Protocol	Port	Ssh Enabled	Username Ssh keypair name
gigamon-4038c0	☒ Enabled ☐ Disabled ☐ Delete	10.115.54.91	Warning ▼	UDF ▼	514	☐ Ssh enabled	Enter Username
gigamon-4038c0	☒ Enabled ☐ Disabled ☐ Delete	10.115.38.83	Warning ▼	UDF ▼	514	☐ Ssh enabled	Enter Username

Figure 12 Logging Page

NOTE: The SSH Enable column will display **Invalid** if SSH is enabled, but missing Username or TCP Port information.

Chassis

The Chassis page provides a detailed snapshot of a selected GigaVUE HC 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 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 13Chassis View](#). Chassis View includes two types of views. Port View and Transceiver View. Transceiver View is the default view.

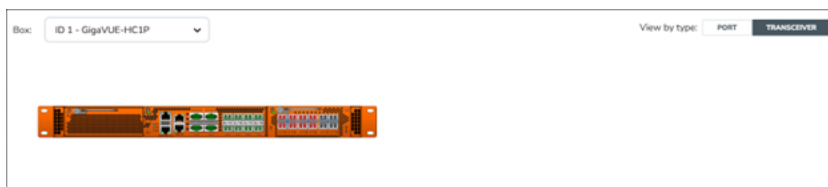


Figure 13 Chassis View

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 14 Chassis View of Node in a Cluster](#) shows an example.

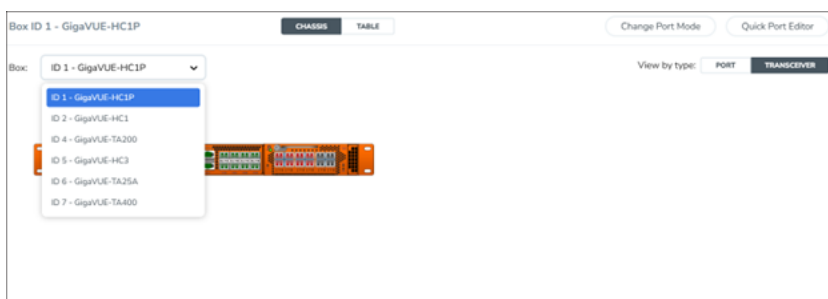


Figure 14 Chassis View of Node in a Cluster

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](#).

[Figure 15 Chassis View—HC3](#) and [Chassis View](#) show some examples of chassis displayed on the Chassis page.

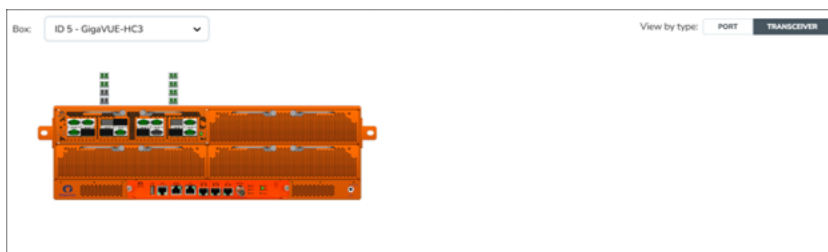


Figure 15 Chassis View—HC3

Hovering over a port in either Port View or Transceiver view displays information about the port: type, port ID, and alias. Hovering over a slot displays information about the slot. For details about port IDs, refer to [Line Card and Module Numbering](#).

Chassis View + Transceiver View

The Chassis + Transceiver view selection is made by clicking the Transceiver View button on the Chassis View page. This view shows you the GigaVUE HC Series node with all the line cards/modules displayed. All the line cards/modules have the transceivers and LEDs displayed.

When the Chassis and Transceiver views are selected, the image of the chassis indicates which transceivers are physically available on the node and whether the ports are up or down. The colors indicate the following:

- Green—the port is up
- Red—the port is down
- Black—the transceiver is missing

Figure 16 Chassis + Transceiver View shows an example of a Chassis + Transceiver View.

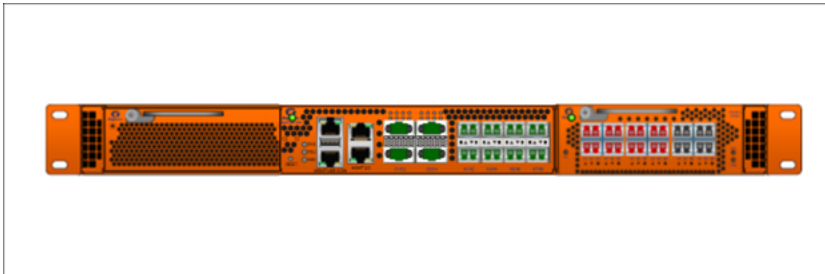


Figure 16 Chassis + Transceiver View

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-TA200. When fanout is used, the fanout is displayed on the Chassis page as shown in **Figure 17** Chassis + Transceiver View with Fanout Ports.

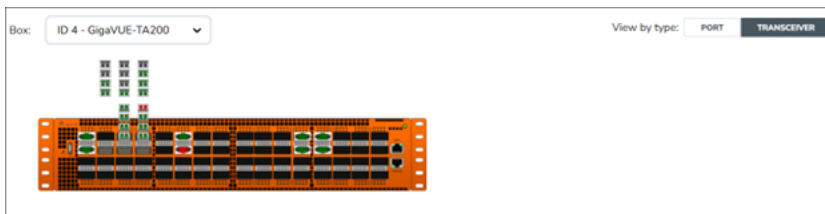


Figure 17 Chassis + Transceiver View with Fanout Ports

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 as shown in [Figure 16 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.

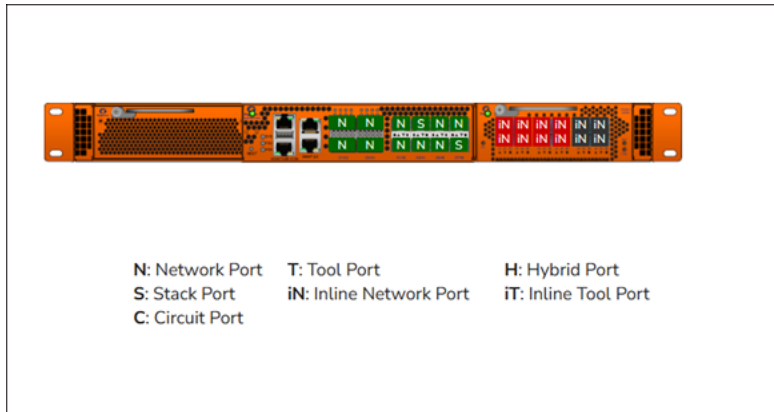


Figure 18 Chassis View + Type View

Line Card and Module Numbering

Line cards and modules use standard conventions for numbering network and tool ports, both on the faceplates of the line cards or modules, and in the information displayed in Chassis view when hovering over a port. On faceplates, the numbers are as follows:

100Gb Ports	Numbered with a leading C . For example, the PRT-HD0-C01 includes 100Gb port C1 ; PRT-HD0-C02X08 includes ports C1 and C2 .
40Gb Ports	Numbered with a leading Q . For example, the PRT-H00-Q02X32 includes 40Gb ports Q1 and Q2 .
10Gb/1Gb Ports	Numbered with a leading X . For example, the PRT-HC0-X24 includes 10Gb/1Gb ports X1 to X24; the bypass combo modules include 10Gb ports X1 to X16.
10/100/1000 Ports	Numbered with a leading G . For example, the PRT-T H00-X12G04 includes 10/100/1000 ports G1 to G4 .

The port labels on the line card or module faceplates use upper-case C, Q, X, and G characters to identify ports. However, Chassis View uses lowercase notation to refer to ports (for example, c1, q1, x4, and g1).

When displaying ports in Chassis View, the format is box ID/slot ID/port ID. For example, 1/1/x6 refers to box 1, slot 1, port X6.

On chassis with multiple slots/bays, the slots or bays are numbered as follows:

- **GigaVUE-HC1:** Bays are numbered as follows:
 - the base chassis in the center, is numbered 1
 - the left module is numbered 2
 - the right module is numbered 3
- **GigaVUE-HC3:** Bays are numbered 1-4 from left upper, left lower, right upper to right lower.

Table View

The Table View selection shows the GigaVUE HC Series or GigaVUE 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 19 Chassis Table View for a Gigamon HC3 CCv2](#) shows an example of the Table View. For GigaVUE-HC3s, 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 (HC3 CCv2) AND 100G modules, PRT-HC0-C02. For GigaVUE-HC1, the Environment section includes a column that shows the GigaSMART CPU Temperature. To select Table View, click the Table View button.

Box ID	Chassis Id/Serial Number	Hardware Ty...	Mode	Gigamon Discovery	Hardware Revision	Product Code	Node UUID
5	J38C0	HC3-Chassis	default	Disabled	1.0	132-00DK	564d455a-b277-13b3-0...

Go to page: 1 of 1 Total Records: 1

Slot Id	Hardware ...	Configured	Heal...	Operation S...	Fabric Hash	Filter Templ...	Power Req. ...	Power Prior...	Hardware R...	Product Code	Serial Num...	Alar...
1	PRT-HC3-...	✓	✓	Up	N/A	None	60	1	1.0-0	132-00DY	1DY0-1000	0
2	PRT-HC3-...	✓	✓	Up	N/A	None	160	2	1.0-0	132-00DW	1DW0-2001	0
3	SMT-HC3-...	✓	✓	Up	N/A	None	200	3	1.0-0	132-00DX	1DX0-1005	0
4	PRT-HC3-...	✓	✓	Up	N/A	None	160	4	1.0-0	132-00DW	1DW0-2002	0

Go to page: 1 of 2 Total Records: 5

Slot Id	Har...	CPU(°C)	e1CPU(°C)	e2CPU(°C)	Exhaust(°C)	Intake(°C)	Switch(°C)	12v
1	PR...	-	-	-	0	0	-	0
2	PR...	-	-	-	0	0	-	0
3	SM...	-	0	0	0	0	-	0
4	PR...	-	-	-	0	0	-	0

Go to page: 1 of 2 Total Records: 5

Figure 19 Chassis Table View for a Gigamon HC3 CCv2

The Table View provides the following information about the chassis and its components:

Chassis Information	Description
Properties	Provides information about the chassis: Chassis ID/Serial Number, VLAN Tag Mode, Hardware Type, Mode, Gigamon Discovery, Operation Status, Hardware Revision, Product Code, and Node UUID . NOTE: Click on the Box ID to view the Fabric Hash setting for the chassis.
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.
Power Supplies	Describes the power supply modules installed in the chassis. This section also includes the current health status of each module. For a GigaVUE-HC3 node, the Power Supplies section includes Power Management. Refer to <i>GigaVUE-HC3 Hardware Installation Guide</i> for details. NOTE: Click on the Power Module ID to view the PSU diagnostic attributes in a Quick View.
Fan Trays	Describes the fan trays installed in the chassis. This section also including the current health status of each tray.
Fan RPM	Provides the current RPM of each fan.

Actions Menu

The Actions menu allows you to perform actions on cards installed in the chassis slots when in Chassis + Table View. The Actions menu is only active when a card is selected. The actions that you can perform are as follows:

Action	Description
Configure	Selecting this action sets the port and traffic settings for the system.
Unconfigure	Selecting this action for a card removes all port and traffic settings for the system.
Enable/Disable Gigamon Discovery	Used to enable/disable Gigamon Discovery protocol
Fabric Advance Hash	Used to configure fabric advanced hashing parameters for stack GigaStreams and GigaSMART groups. For details, refer to Fabric Advanced Hashing
Start Up	Selecting this action reboots the card.

Action	Description
Shut Down	Selecting this action shuts down the card.
Change VLAN Tag Mode	Used for configuring the VLAN tag mode for GigaVUE-TA25 node. For more details refer to Change VLAN Tag mode .
Enable Fabric Hash	Used for improving packet distribution on PRT-H00-Q02X32 and PRT-HD0-Q08 line cards. For details, refer to Enable Advanced Fabric Hashing

Reload a GigaSMART Line Card or Module

Occasionally, the GigaSMART line card or module will need to be reloaded for changes to take effect and to allocate resources accordingly. Reloading also provides applications with contiguous memory.

The following message displays when the GigaSMART line card or module needs to be reloaded:

Resource allocation changes have been made that require GigaSMART card 2/1/1 to be reloaded in order for them to take effect.

When this message is displayed, you cannot change the configuration relating to that application until after the reload. For example, you cannot use the GigaSMART Operation, associated with the GigaSMART Group in a map.

Use the following steps to reload a GigaSMART line card or module:

1. Switch to Table View.
2. Under **Cards**, select the GigaSMART line card or module.
3. Select **Actions > Shut Down**.

Use the following steps to bring the GigaSMART line card or module backup:

1. Switch to Table View.
2. Under **Cards**, select the GigaSMART line card or module.
3. Select **Actions > Start Up**.

Change VLAN Tag mode

Change VLAN Tag mode allows you to configure, single tagged or double tagged VLAN traffic at the chassis level for GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus and GigaVUE-HCT. This mode can be configured based on your incoming traffic and network requirements. This configuration has two modes which are as follows:

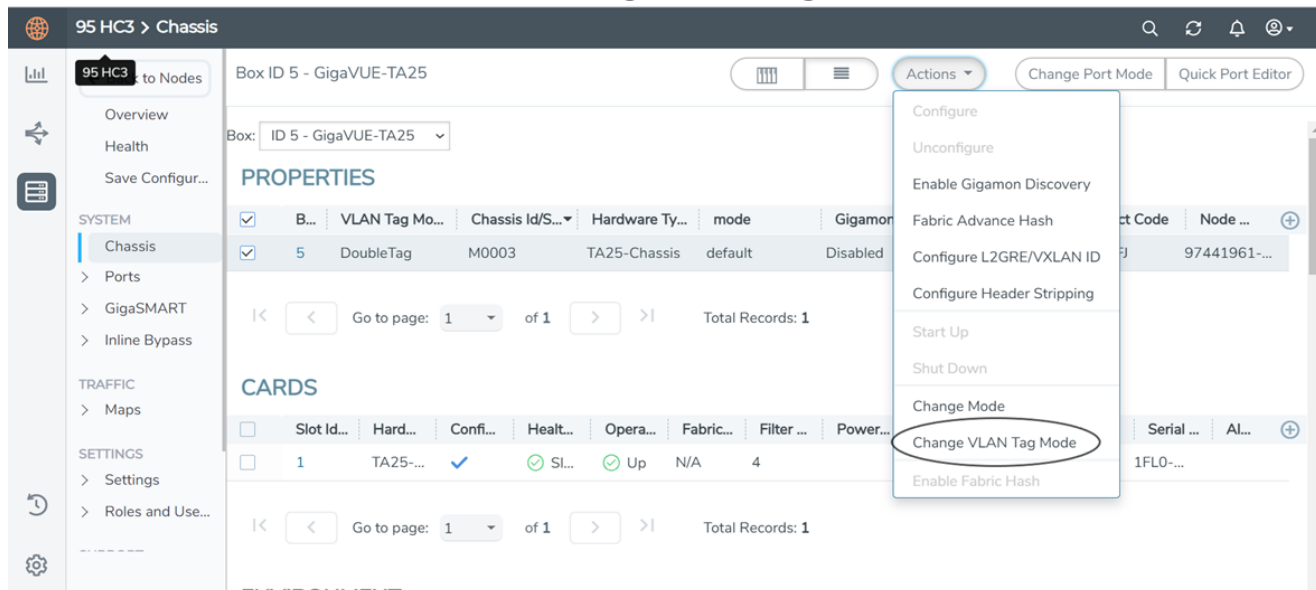
1. **Single Tag Mode**- This provides visibility of untagged and single-tagged VLAN packets. Single tagged traffic allows GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus and GigaVUE-HCT to enable the following features:
 - VLAN rules are supported in port filters.
 - Egress VLAN stripping is supported as in legacy devices, even when the source and destination belongs to the same or different set of devices.
 - MAC rewrite functionality is supported in cluster mode.
 - When L2 circuit encapsulation tunnels or GSOP maps are in use, then the port filters will support both IPv4 and IPv6 rules.
 - This functionality is enabled even when a GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus and GigaVUE-HCT are in a cluster. In the same cluster, there can be two GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus and GigaVUE-HCT devices functioning with two different tag modes.
2. **Double Tag Mode**-This is the default mode, which supports both single and double tagged VLAN packets. When the deployment environment needs visibility to all types of packets i.e untagged or single-tagged/double tagged or priority VLAN tagged (VLAN Tag 0) packets, then this is the recommended operating mode. In this mode the above features enabled in single-tagged mode will exist as a limitation for GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus and GigaVUE-HCT. For GigaVUE-TA25E the limitation; when L2 circuit encapsulation tunnels or GSOP maps are in use, then the port filters will support both IPv4 and IPv6 rules is not applicable in E-tag mode.

Configure Change VLAN Tag

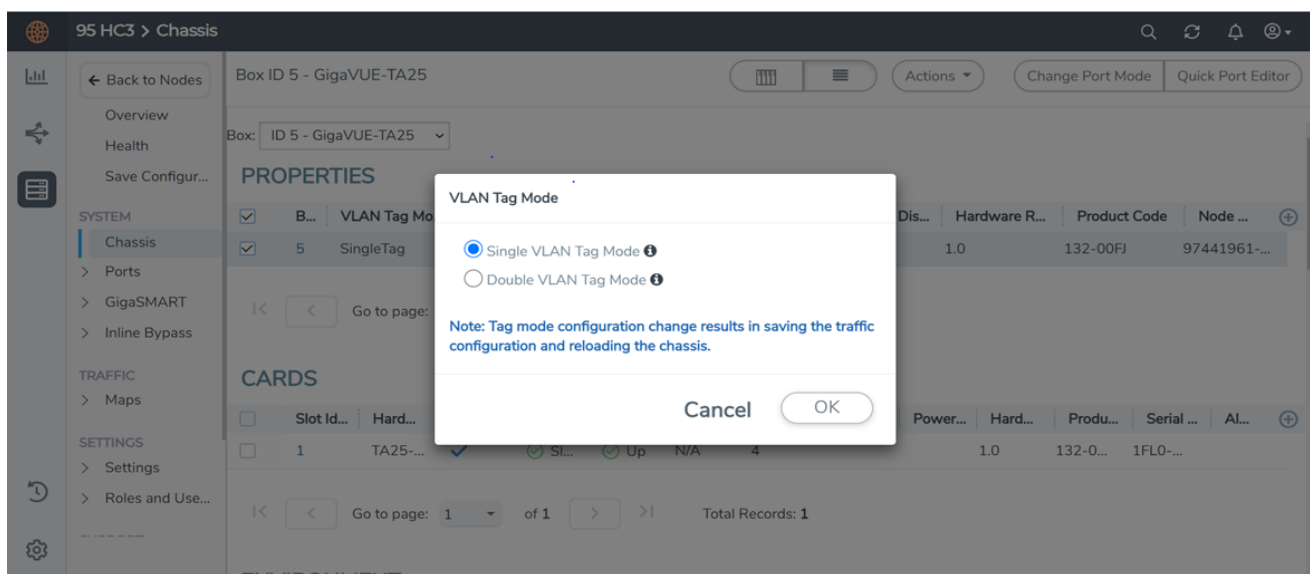
The chassis page has a **Actions** button. To configure either single or double tagged VLAN do the following:

1. Select your GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus and GigaVUE-HCT node.

- Click on **Actions** buttons and select **Change VLAN Tag Mode**.



- Select the VLAN Tag mode as required.
- Confirm the selection and click on **OK**.
- Once the VLAN tag is configured the device will save the traffic and initiate reloading the device.



Rules and Notes

- While configuring the VLAN tag mode the chassis will be reloaded only if it is in UP state. Otherwise it will apply the configuration without reloading the chassis. The user will be notified about the reload. After confirmation, the active configuration will be applied and the chassis will be reloaded after saving the active configuration.

2. If double tagged packets enter a single tag mode in GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus and GigaVUE-HCT chassis then the inner VLAN would be dropped during egress.
3. Modifying tag-mode via *config switch-to* operation is supported whereas it is not supported via *config text-apply* operation.
4. In a Single tag-mode, adding vlan port-filter-rule along with VLANs matching the ingress-vlan-tag(on network-port)/add-vlan-header gsop in the transit/second map is not supported due to platform limitation.
5. In single-tag mode, priority tagged VLAN (VLAN TAG 0) packets are stripped off the VLAN tag at egress. It is recommended to use double tag mode in this case.

Change Port Mode

Change port mode can be configured only on selected platforms. The port breakout modes are as follows:

- **none**—Specifies no port breakout mode. This is the default mode for all GigaVUE nodes.
- **4x10G**—Specifies the **4x10G** port breakout mode. This mode provides a 4 x 10Gb breakout option for 100Gb/40Gb ports. The **4x10G** mode only applies to GigaVUE-TA40, GigaVUE-TA100, GigaVUE-TA200, GigaVUE-TA100-CXP, the PRT-HD0-C06X24 line card on GigaVUE HD Series, and the PRT-HC3-C08Q08, PRT-HC3-C16, SMT-HC3-C05, and BPS-HC3-C25F2G modules on GigaVUE-HC3.

NOTE: Starting in software version 5.5, GigaVUE-TA40 supports 4x10G breakout at port level. Port breakout mode in GigaVUE-TA40 is configured as follows:

 - 24 out of the 32 ports provide 4x10Gb breakout support. The first 12 ports and the last 12 ports provide support for breakout functionality with 96 sub-ports operating as 10Gb ports
 - Ports q1 to q12 and q21 to q32 support breakout functionality
 - Ports q13 to q20 do not support breakout functionality
 - Port are named as q1x1....q1x4, q2x1...q2x4 (similar to other hardware devices) to support the breakout functionality
- **4x25G**—Specifies the **4x25G** port breakout mode. This mode provides a 4 x 25Gb breakout option for 100Gb QSFP28 SR ports. The **4x25G** mode only applies to GigaVUE-TA200 and the PRT-HC3-C08Q08, PRT-HC3-C16, and SMT-HC3-C05 modules on GigaVUE-HC3.
- **2x40G**—Specifies the **2x40G** port breakout mode. This mode provides a 2 x 40Gb breakout option for 100Gb/40Gb ports. The **2x40G** mode only applies to the PRT-HC3-C08Q08 module on GigaVUE-HC3.

For the BPS-HC3-C25F2G module on GigaVUE-HC3, refer to the *GigaVUE-HC3 Hardware Installation Guide*.

The 100Gb ports that support **4x10G** mode can operate at 40Gb speed with QSFP+ SR or PLR4 transceivers. When a parent port is configured in **4x10G** mode, it can be broken out into four 10Gb ports, called subports. The subports will all have the same speed (10Gb). Subports will have x1 to x4 appended to their port ID, for example, 1/1/c2x1.

The 100Gb ports that support **4x25G** mode can be broken out into four times 25Gb ports, called subports. The subports will all have the same speed (25Gb). Subports will have x1 to x4 appended to their port ID, for example, 1/1/c2x1.

The 100Gb ports that support **2x40G** mode can operate at 40Gb speed with QSFP+ SR and LR transceivers. When a parent port is configured in **2x40G** mode, it can be broken out into two 40Gb ports, called subports. The subports will all have the same speed (40Gb). Subports will have q1 to q2 appended to their port ID, for example, 1/1/c1q1 and 1/1/c1q2.

In general, subports created from port breakout modes can function as network, tool, or hybrid ports, as well as GigaStream port members, but they cannot function as stack ports. However, starting in software version 5.3, 10Gb stacking is supported only on GigaVUE-TA100 and PRT-HC3-C08Q08 on GigaVUE-HC3 when ports are broken out into **4x10G** mode.

NOTE: On the PRT-HD0-C06X24 line card on GigaVUE HD Series, when 40Gb ports are broken out into 4 X 10Gb subports, no ports on that line card can be used as stack-links, not any other C port or any X port.

Each port can only have one mode.

The Chassis page has a Port Mode Editor available. The Port Mode Editor is used to set ports to breakout mode. To configure a port breakout mode, do the following:

1. Click **Change Port Mode**.

NOTE: The **Change Port Mode** button is only active on nodes that support it.

The Port Mode Editor page shown in [Figure 20Port Mode Editor](#) displays.

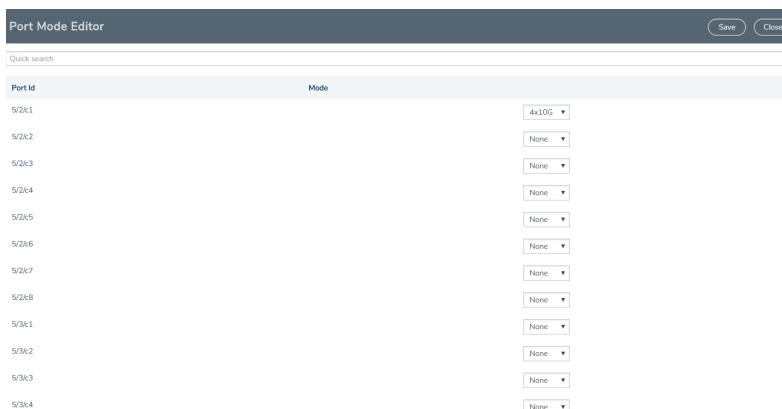


Figure 20 Port Mode Editor

2. Select the **Port Mode** for the ports that you want configure: **none**, **4x10G**, **4x25G**, or **2x40G**. For example, set port 36/1/c3 to **4x10G**.

Use the Quick search field to find a specific port. For example, entering 36/1/c3 in the Quick search field displays the ports with the IDs 36/1/c3, 36/1/c30, 36/1/c31, 36/1/c32.

3. Click **Save**.

The system returns you to the Chassis View page. For example on GigaVUE-TA100, the fanout ports are displayed in the chassis view as shown in [Figure 21 Breakouts Displayed on a GigaVUE-TA100 Chassis](#). In [Figure 21 Breakouts Displayed on a GigaVUE-TA100 Chassis](#), the ports that are set to **4x10G** show four additional ports.

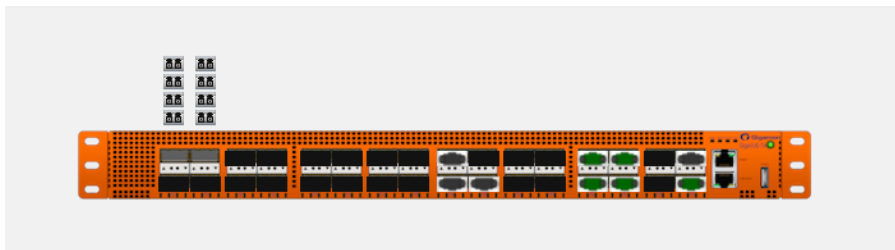


Figure 21 Breakouts Displayed on a GigaVUE-TA100 Chassis

After setting the port breakout mode, the ports will need break-out cables or breakout panel (PNL-M341 or PNL-M343). For breakout panel information, refer to the respective *Hardware Installation Guide*.

Enable Advanced Fabric Hashing

The Enable Fabric Hash option is used to enable advanced fabric hashing on a specified card and slot. Advanced fabric hashing is supported on all GigaVUE HC Series devices and GigaVUE TA Series devices.

Advanced Fabric Hash can only be enabled or disabled while in Chassis Table View. To enable or disable Advanced Fabric Hashing, do the following:

1. Select **Chassis** in the main navigation pane.
2. Switch the Chassis page to Table View.
3. Under **Cards**, find the line card on which you want to enable fabric hash and select the card. The **Fabric Hash** field for the card indicates the current state of fabric hash. In [Enable Advanced Fabric Hashing](#), fabric hash is disabled on the selected line card.
4. Select **Actions**
 - If the fabric hash is currently disabled, the **Actions** menu shows **Enable Fabric Hash**. Click on the menu selection to enable.
 - If the fabric hash is currently enabled, the **Actions** menu shows **Disable Fabric Hash**. Click on the menu selection to disable.

Fabric Advanced Hashing

Fabric Advanced Hashing is used to enable advanced fabric hashing on a chassis in GigaStream stack links and GigaSMART groups. The Fabric Advanced Hash option lets you select the criteria for sending matching flows to the same destination port within stack links.

The existing gigastream hashing can be applied only to tool/hybrid/circuit ports. Fabric advanced hashing hashes traffic based on the ipsrc, ipdst, protocol, ip6src, ip6dst. You can also select the various fields to configure hashing on stack links.

Fabric advanced hashing applies to the following modules:

- GigaVUE-HC1
- GigaVUE-HCT
- GigaVUE-HC1-Plus
- GigaVUE-HC3-v2
- GigaVUE-TA25
- GigaVUE-TA25E
- GigaVUE-TA200
- GigaVUE-TA200E
- GigaVUE-TA400
- GigaVUE-TA400E

Fabric Advanced Hash can only be enabled or disabled while in Chassis Table View. To enable or disable Fabric Advanced Hashing, do the following:

1. Select **Chassis** in the main navigation pane.
2. Switch the Chassis page to Table View.
3. Select the **Box ID** under Properties and select **Actions**.
4. Select the required **Fabric Advanced Hash** type from the drop-down.
5. The following options are available:
 - **All:** Selects all criteria
 - **Default:** Sets the fabric advanced hash algorithm to its default settings
 - **None:** Clears all fields from advanced hash
 - **Fields:** Allows you to select the required fields for advanced hash.

NOTE: If **Fabric Advanced Hash** is already configured, click the **Box-ID** field to view the Fabric Advanced Hash configuration in a Quick View.

Manage Roles and Users—GigaVUE-OS

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

- [About Role-Based Access](#)
- [Configure Role-Based Access and Setting Permissions in GigaVUE Nodes](#)

About Role-Based Access

GigaVUE HC Series nodes use role-based access to manage access to the Gigamon Deep Observability Pipeline. Through GigaVUE-FM, you can create roles and assign users to those roles, allowing you to partition separate sets of tool ports for different groups of users while different sets of network ports are shared. This makes it possible to provides different groups of users with different analysis needs to have full access to the packets they need for their tools.

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 exercise 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 <i>subscribing</i> 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.

NOTE: Map-Sharing Permissions are only available to node level users. GigaVUE-FM users cannot be added for this level of permissions.

To set permissions for a map, do the following:

1. Select **Maps** in the Navigation pane, then go to the **Maps** page.

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

2. Select the map, and then click **Edit**.
3. Go to the **Map Permissions** section of the **Edit Map** page.
4. Click in the **Owner**, **Edit**, **Listen**, or **View** field and select roles from the drop-down list.

Locks and Lock Sharing

Short-term analysis needs are always changing, occasionally creating situations where one user may temporarily need exclusive access to a port. Rather than create new roles and associations in situations like this, a user can lock a port to which they have Level 2+ access, preventing other users from changing settings. Locks can also be shared with other users, allowing users to collaborate. Sharing a locked port provides the account with whom the port is shared the same port permissions as the account sharing the port. For example, if User X has Level 2 permissions on port 12/5/x3, User X can share a lock on 12/5/x3 with any other user account, providing them with Level 2 permissions regardless of their normal privileges on the port, if any.

For information about permission levels and how to set locks and lock-sharing, refer to [Set Locks and Lock-Shares](#).

Create Roles

This section describes the steps for creating roles and assigning user to those roles. Before creating roles, refer to [About Role-Based Access](#). However, GigaVUE nodes have three built-in roles for specifying which users have access to a given port. These roles are:

- **Admin**

This role provides access to all command modes, including Standard, Enable, and Configure. Admin users also have access to all commands and all ports. They are also members of all groups.

- **Default**

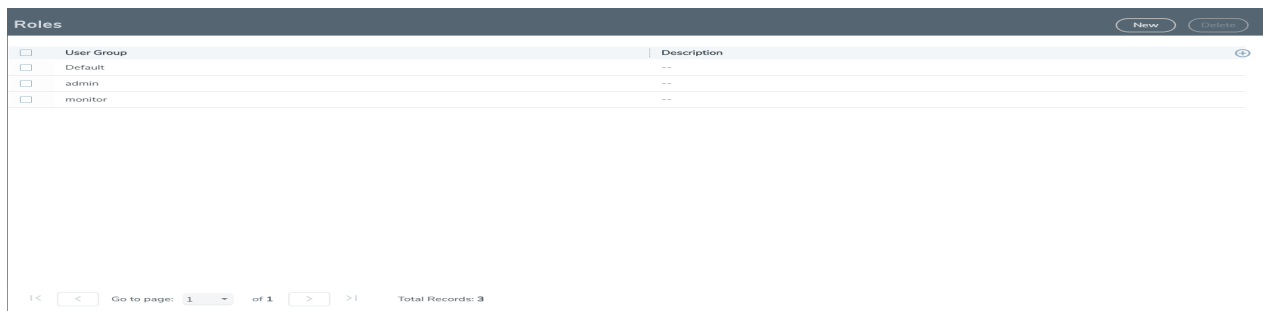
This role also provides access to all command modes. Users with the Default role has no access to unassigned ports. New users are created with the Default role automatically. However, you can remove it if you do not want to allow a user access to unassigned ports

- **Monitor**

This role provides view-only access to ports and configurations. Administrators create additional custom *roles* and assign them to users together with the Default role. For example, if you create a role named `Security_Team` and assign it to tool port 5/1/x2, users assigned the `Security_Team` role are able to access tool port 5/1/x2. Conversely, users without a role that gives them some access to tool port 5/1/x2 will not even be able to see it in GigaVUE-FM. Users can have multiple assigned roles, allowing administrators to fine-tune access to the Gigamon Deep Observability Pipeline.

To create roles and assign users to those roles, do the following:

1. Select **Roles and Users** in the Navigation pane, then select the **Roles** page.



User Group	Description
Default	--
admin	--
monitor	--

2. Click **New**.
3. On the **New Role** page, do the following:
 - o Enter a role in the **Role Name** field. For example, `Security_Team`.
 - o (Optional) Enter a description of the role in the **Descriptions** field.
4. Click **Save**.
5. Add users to the role. Refer to [Add Users](#).

Configure Role-Based Access and Setting Permissions in GigaVUE Nodes

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

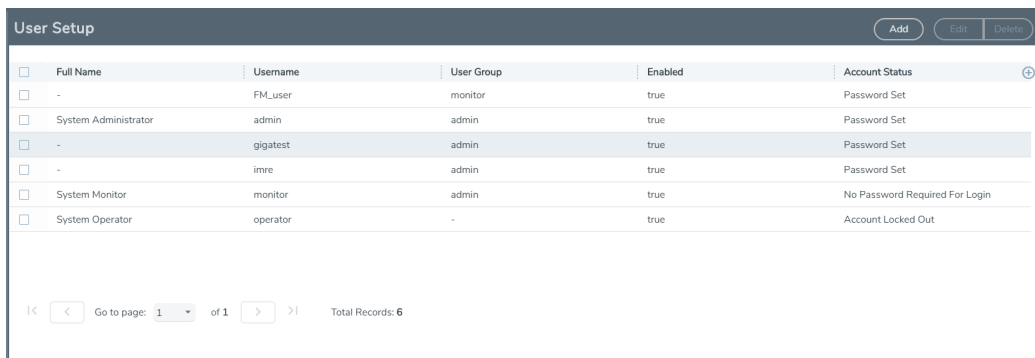
- [Add Users](#)
- [Create Roles](#)
- [Associate Roles with Port Permissions](#)
- [Set Locks and Lock-Shares](#)
- [Set Map-Sharing Permission Levels](#)

Add Users

This section provides the steps for adding users to the GigaVUE-OS nodes. Users are also assigned to roles that set their access permissions. Refer to the [Create Roles](#) section for more details.

To add users, do the following:

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



The screenshot shows the 'User Setup' page with a table of users. The table has columns: Full Name, Username, User Group, Enabled, and Account Status. There are 6 records in total. The third record, 'gigatest', is highlighted. At the bottom, there is a pagination control showing 'Go to page: 1 of 1' and 'Total Records: 6'.

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

2. Click **Add**. The **Add New User** page displays.
 3. On the Add New User page:
 - o Enter a user name for this account in **User Name** field.
 - o Enter the user's actual name in the **Name** field.
 - o Enter a password for the user in the **Password** field and in the **Confirm Password** field. Refer to the [Password Policies](#) section in the GigaVUE-OS CLI Reference Guide.
- NOTE:** GigaVUE-FM prompts you to enter your password. Enter your password and click **Submit**.
- o Assign a role to the user by clicking in **Capability** field and selecting a role from the drop-down list. For the steps to create a role, refer to [Create Roles](#).
 4. Select **Enable** to enable the user's account, and then click **Save**.
 5. The added users will then be listed in the **User Setup** page. In GigaVUE-OS, this list will also display the **Last Login** and **Number of Login Attempts** of a user.

Create Roles

This section describes the steps for creating roles and assigning user to those roles. Before creating roles, refer to [About Role-Based Access](#). However, GigaVUE nodes have three built-in roles for specifying which users have access to a given port. These roles are:

- **Admin**

This role provides access to all command modes, including Standard, Enable, and Configure. Admin users also have access to all commands and all ports. They are also members of all groups.

- **Default**

This role also provides access to all command modes. Users with the Default role has no access to unassigned ports. New users are created with the Default role automatically. However, you can remove it if you do not want to allow a user access to unassigned ports

- **Monitor**

This role provides view-only access to ports and configurations. Administrators create additional custom *roles* and assign them to users together with the Default role. For example, if you create a role named `Security_Team` and assign it to tool port `5/1/x2`, users assigned the `Security_Team` role are able to access tool port `5/1/x2`. Conversely, users without a role that gives them some access to tool port `5/1/x2` will not even be able to see it in GigaVUE-FM. Users can have multiple assigned roles, allowing administrators to fine-tune access to the Gigamon Deep Observability Pipeline.

To create roles and assign users to those roles, do the following:

1. Select **Roles and Users** in the Navigation pane, then select the **Roles** page.

User Group	Description
☐ Default	--
☐ admin	--
☐ monitor	--

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](#).

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, and change egress port filters. The user can configure port-lock, lock-share, and all traffic objects except port-pair. Also includes all Level 1 permissions.
Level 3	The user can configure port parameters (such as administrative status of the port, speed, duplex, and autonegotiation), as well as create port pairs. Also includes all Level 2 and Level 1 permissions.
Level 4	The user can change the port type. Also includes all Level 3, 2, and 1 permissions.

To associate roles with port permission, do the following:

1. Select **Ports** in the Navigation pane, then go to **Ports > All Ports**.
2. Select the port or ports on which you want to set permissions.

Ports All Ports Ports Discovery Fabric Statistics

Total Ports: 52 | Filtered By: none Dec 20, 2019 15:10:44

Port Id	Alias	Status	Type	Speed	Admin	Link Status	Transceive...	SFP Power	Avg Util T...	Port Filter	Discovery ...	Box...
15/1a1(FM-T...		Port is healt...	N		Disabled	--			0 / 0	--	none	FM-TA10...
15/1a2(FM-T...		Port is healt...	N		Disabled	--			0 / 0	--	none	FM-TA10...
15/1a3(FM-T...		Port is healt...	N		Disabled	--			0 / 0	--	none	FM-TA10...
15/1a4(FM-T...		Port is healt...	N		Disabled	--			0 / 0	--	none	FM-TA10...
15/1a1(FM-T...		Port is healt...	N		Disabled	--			0 / 0	--	none	FM-TA10...
15/1a2(FM-T...	hb1_16_1...	Observed 1...	T	10G	Enabled	up	sfp+ sr	-2.98	100 / 100	--	none	FM-TA10...
15/1a3(FM-T...	hc2_12_1...	Observed 1...	T	10G	Enabled	up	sfp+ sr	-2.31	100 / 100	--	none	FM-TA10...
15/1a4(FM-T...		Observed 1...	T	10G	Enabled	up	sfp+ sr	-1.92	100 / 100	--	none	FM-TA10...
15/1a5(FM-T...		Observed 1...	T	10G	Enabled	up	sfp+ sr	-2.37	100 / 100	--	none	FM-TA10...
15/1a6(FM-T...		Observed 1...	T	10G	Enabled	up	sfp+ sr	-33.98	100 / 100	--	none	FM-TA10...
15/1a7(FM-T...		Observed 1...	T	10G	Enabled	up	sfp+ sr	-3.00	100 / 100	--	none	FM-TA10...
15/1a8(FM-T...		Observed 1...	T	10G	Enabled	up	sfp+ sr	-1.75	100 / 100	--	none	FM-TA10...

1 < < Go to page: 1 of 5 > > Total Records: 52

3. Click **Edit**.
4. In the Permissions section of the **Ports** page, assign roles to the permissions levels.
5. Click **Save**.

Set Locks and Lock-Shares

This section provides the procedures for setting port locks and lock-sharing. Before doing these procedures, refer to [Locks and Lock Sharing](#). The procedures for setting lock and lock-sharing are as follows:

- [Remove a Lock from a User's Port](#)
- [Remove a User's Lock-Share](#)
- [Lock a Port for a User](#)

Remove a Lock from a User's Port

To remove a user's lock from a port, administrators do the following:

1. On the left navigation pane, go to **Inventory**  go to **Physical > Nodes**.
2. Select the required node.
3. Select **Ports** in the Navigation pane, then go to **Ports > All Ports**.
4. Select the port on which you want to remove a lock.
5. Click **Edit**.
6. Clear the **Lock Port** check box.

Remove a User's Lock-Share

To remove a user's lock-share, administrators do the following:

1. On the left navigation pane, go to **Inventory**  go to **Physical > Nodes**.
2. Select the required node.
3. Select **Ports** in the Navigation pane, then go to **Ports > All Ports**.
4. Select the port or ports on which you want to remove a lock-share.
5. Click **Edit**.
6. Click on the **Lock shared with Users** field and remove the user.
7. Click **Save**.

Lock a Port for a User

To lock a port for a user, administrators can do the following:

1. On the left navigation pane, go to **Inventory**  go to **Physical > Nodes**.
2. Select the required node.

3. Select **Ports > Ports > All Ports**.
4. Select the port or ports on which you want to remove a lock.
5. Click **Edit**.
6. Select **Lock Port** if it is not already selected.
7. Click on the **Lock shared with Users** field and add the user.

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 <i>subscribing</i> 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.

NOTE: Map-Sharing Permissions are only available to node level users. GigaVUE-FM users cannot be added for this level of permissions.

To set permissions for a map, do the following:

1. Select **Maps** in the Navigation pane, then go to the **Maps** page.
2. Select the map, and then click **Edit**.
3. Go to the **Map Permissions** section of the **Edit Map** page.
4. Click in the **Owner**, **Edit**, **Listen**, or **View** field and select roles from the drop-down list.

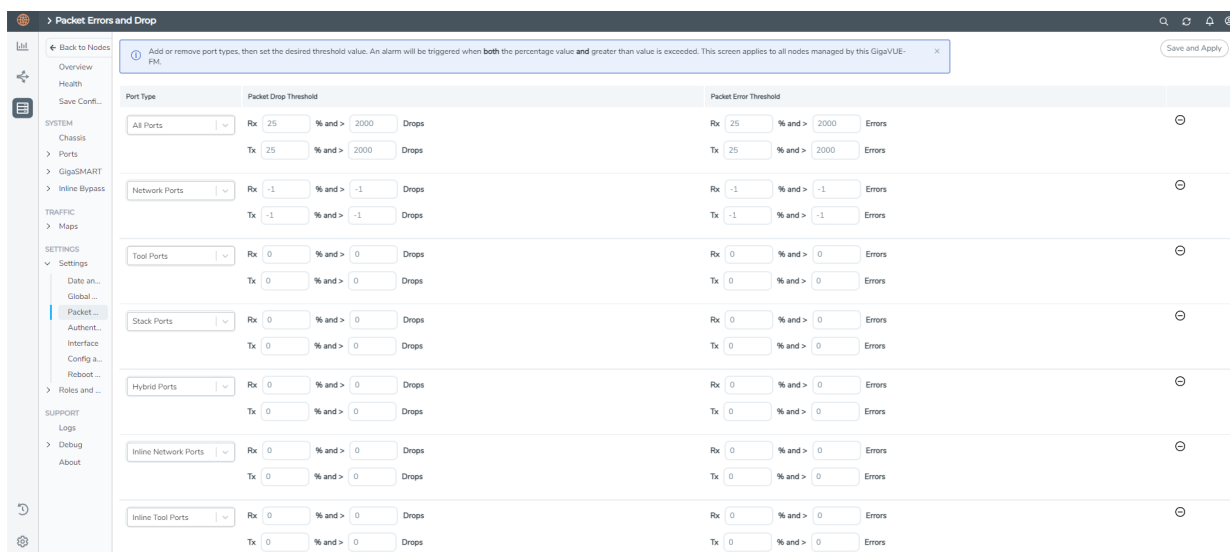
¹Requires Level 2 or Level 3 access, based on the user's role membership.

Configure Port Packet Drop/Error in Devices

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

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

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



Packet Errors and Drops

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

Save and Apply

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

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

To configure threshold values for a specific port:

1. Select **Ports > Ports > All Ports**. Select the Port ID of the port on which you want to configure the packet drop/error threshold.
2. Click **Edit** to open the port editor.

- Under **Alarms**, configure the **Packet Drop Threshold** and **Packet Error Threshold** values in % and number for both Rx and Tx traffic.

▼ Alarms

Buffer Threshold (%) Rx 0 Tx 0

Utilization Threshold (%) High 0 Low 0

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

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

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

The configuration is applied to that specific port.

NOTE: To configure the threshold values globally for all the devices managed by GigaVUE-FM refer to [Configure Port Packet Drop/Error in GigaVUE-FM](#)

Related topics

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

Reboot and Upgrade Options

This section describes how to upload and upgrade images on GigaVUE nodes. For more detailed instructions on the upgrade paths available, refer to the GigaVUE-OGigaVUE-OS 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:

- Using administrator user credentials, log in to GigaVUE-FM.



- On the left navigation pane, click , and then select **Physical>Nodes**. Select the required node or cluster.
- Select **Settings > Reboot and Upgrade**. The Reboot and PLD upgrade page displays as shown in [Figure 22Reboot Page](#).

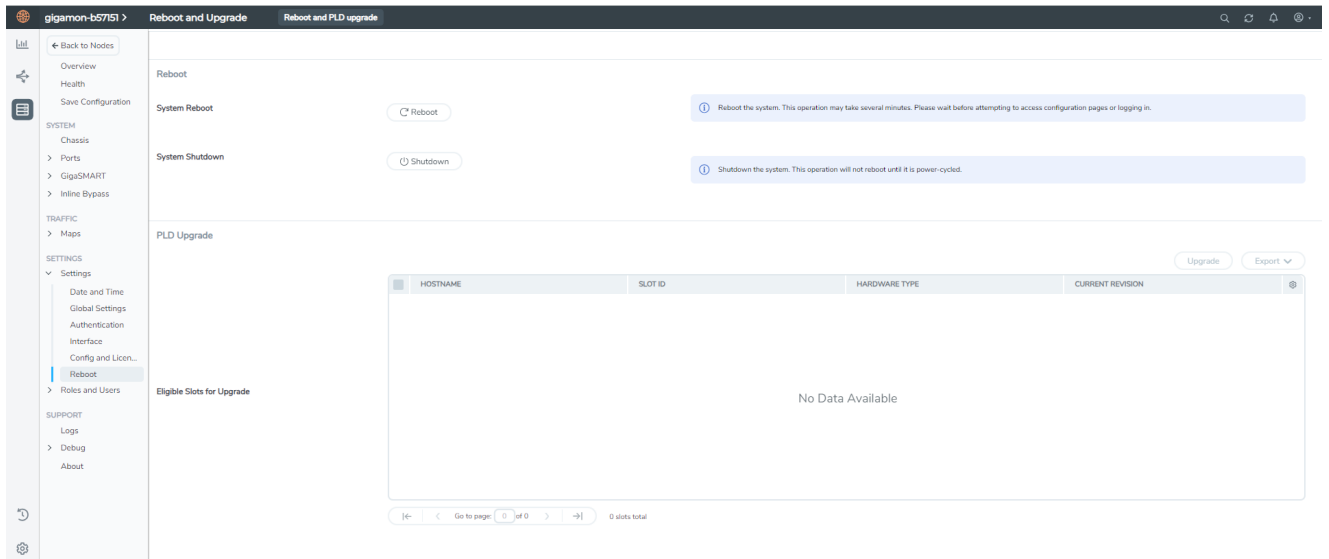


Figure 22 Reboot Page

- Click **Reboot**. Depending on the configuration changes, a dialog appears.

If no changes have been made to the current configuration, the dialog shown in the following figure appears. Click **OK** to reboot the node.

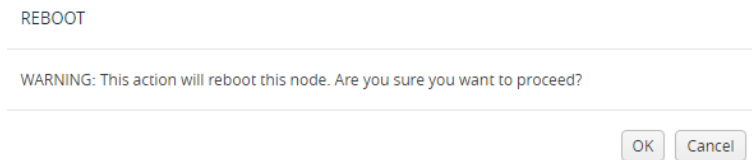


Figure 23 Reboot Dialog

If there are any changes to the current configuration, the reboot dialog displays a warning that current configuration has been modified as shown in the following figure. Click **OK** to save the configuration and reboot.

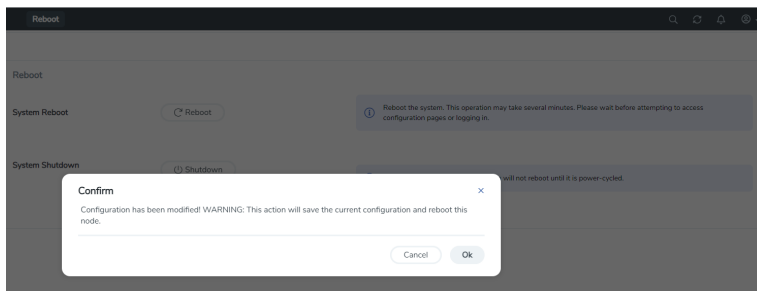


Figure 24 Save and Reboot

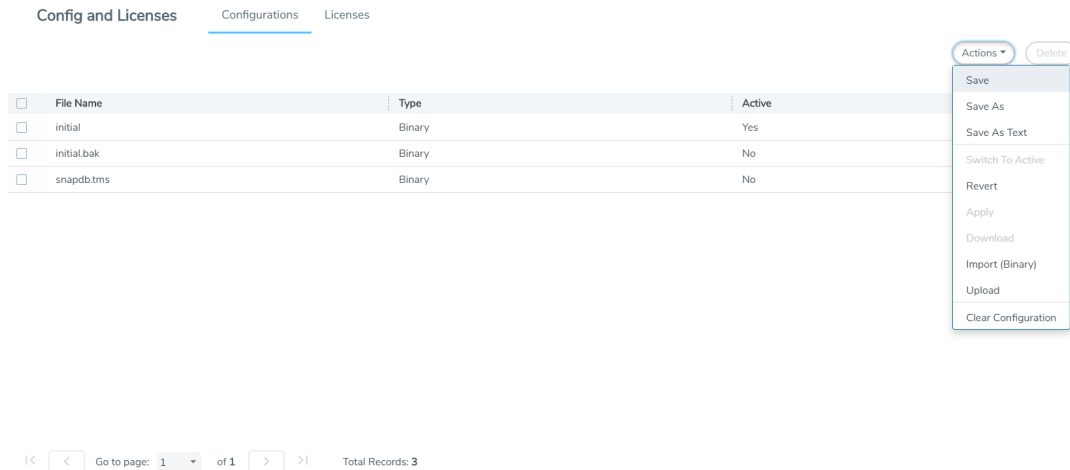
Upgrade the Software

Refer to the GigaVUE-OS Upgrade Guide for details on upgrading the software.

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** as 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 PLD

Use the following steps to upgrade Programmable Logic Device (PLD):

1. Using administrator user credentials, log in to GigaVUE-FM.



2. On the left navigation pane, click , and then select **Physical>Nodes**. Select the required node or cluster.
3. Select **Settings > Reboot and Upgrade**. The Reboot and PLD upgrade page displays.

PLD upgrade is used to upgrade Programmable Logic Devices (PLDs) such as Field Programmable Gate Arrays (FPGAs) on GigaVUE-HC3 nodes.

4. Select the required slot, 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 25 Configuration Files Page](#).

File Name	Type	Active
initial	Binary	Yes
initial.bak	Binary	No
snapdb.tms	Binary	No

Go to page: 1 of 1 Total Records: 3

Figure 25 Configuration Files Page

The following sections describe how to set the options:

- [Configuration File Options](#)
- [Configuration Actions](#)
- [Upload a Configuration](#)
- [Import a Configuration](#)

Configuration File Options

The Configuration Files page lists the configuration files currently saved on the node. The last booted configuration file is listed with Yes in the Active column. From here, you can perform the following tasks when you select a configuration file:

- Click **Switch To Active** to load the selected configuration file, applying its settings.
- Click **Delete** to remove the selected file from the system.
- Click **Download** to download the file to your local environment.

- Click **Action** to select various operations to perform on the files. For details, refer to [Configuration Actions](#).

Configuration Actions

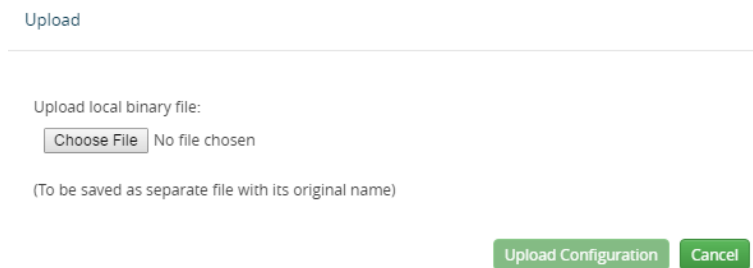
The active configuration is the combination of the last booted configuration file and all unsaved commands that led to the current running configuration. On the Configuration page, you can perform the following tasks with the **Actions** menu:

- Click **Action > Save** to save the running configuration to the active configuration file (the one listed in bold in the Configuration Files table, above).
- Click **Action > Revert** to discard the running configuration and apply the contents of the active configuration file.
- Click **Action > Save As** to save the running configuration to a new file and make it active. Use the adjacent field to provide a name for the new configuration file.
- Click **Action > Upload** to upload a binary configuration file. For details, refer to [Upload a Configuration](#).
- Click **Action > Import** to import a configuration file. For details, refer [Import a Configuration](#).

Upload a Configuration

Use the Upload Configuration options to send configuration files from the local system to the GigaVUE node. To upload a configuration file, do the following:

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



Upload

Upload local binary file:

No file chosen

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

- On the Upload Dialog, click **Choose File** to upload the binary file.
- After the file is uploaded, click Upload Configuration.

The file is saved on the GigaVUE node with its original name. This is handy when you've saved some standard configuration files to your system using the Save command in the Configuration Files section above.

Import a Configuration

To retrieve a saved configuration file from a remote host, using HTTP, HTTPS, SCP, SFTP or FTP, 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, or FTP.
3. Supply the IP address or hostname of the remote host in the **Hostname or IP Address** field.
4. Provide the credentials used to log in to the system by entering the user name in the **Remote Username** field and the user's password in the **Remote Password** field.
5. In the File Path field, provide the filename and filename path on the remote system.
6. Click **Import**.

Backup and Restore

Backing up and restoring nodes is a time consuming process. GigaVUE-FM lets you back up and restore the configuration of all of the managed GigaVUE nodes, including GigaVUE HC Series and GigaVUE TA Series. At the end of the backup or restoring process an event is posted that indicates a success or failure of the backup.

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 HC Series Nodes](#)

Nodes and Cluster Backup

This section describes how to backup GigaVUE HC Series and GigaVUE TA Series nodes. When a node is backed up, the backup file is saved in local storage on the machine where GigaVUE-FM is installed. The filename is the timestamp of the backup. Starting from 5.5, backups are in text based and binary formats. For security reasons, text configuration files do not include plain text passwords, such as SMTP passwords, AAA keys (RADIUS or TACACS+), or private keys in RSA/DSA identities. When a cluster is backed up, a backup file is created for the leader only.

You can schedule node or nodes and node clusters for immediate backup or scheduled backups to occur at a specified time. For example, you can schedule a backup for a particular day, week, month, or date.

Notes:

- Clusters can be backed up only if the Leader in the cluster is licensed.

- 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. On the left navigation pane, click , and then select **Physical>Nodes**. Select the required node or cluster.
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 26 SNMP Trap Configuration Save Enabled](#).

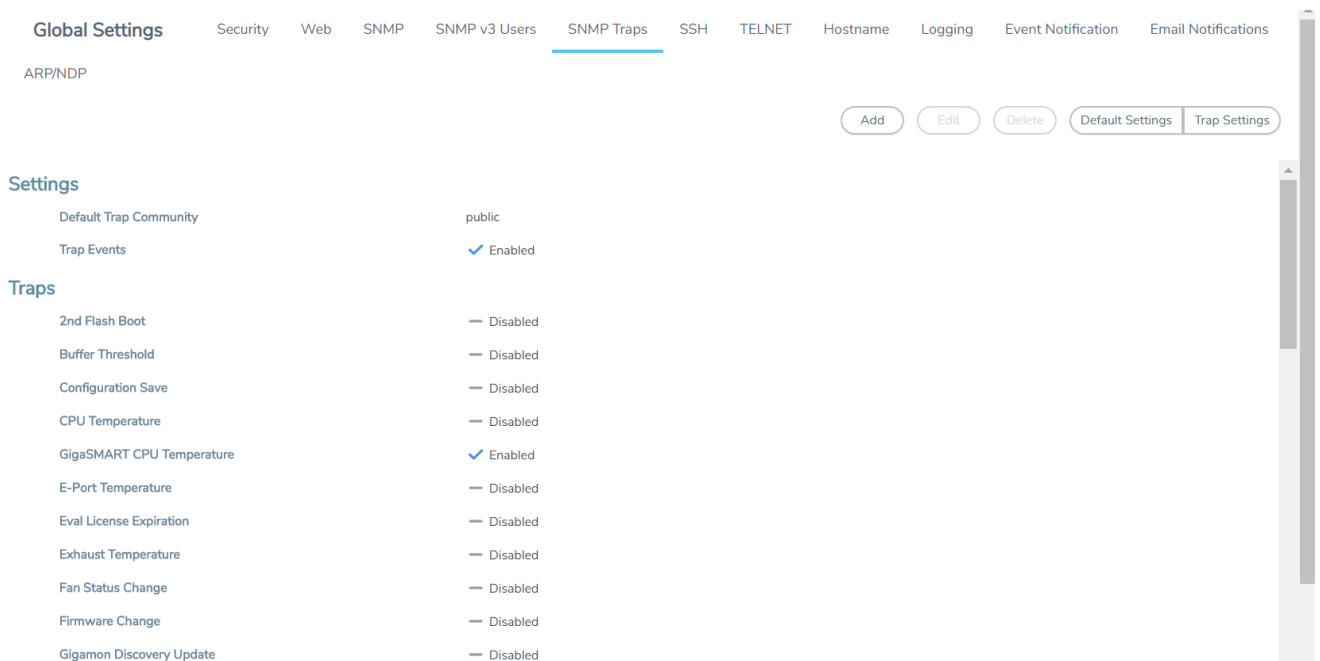


Figure 26 *SNMP Trap Configuration Save Enabled*

BackUp Nodes and Clusters

To backup a node, nodes, or clusters, do the following:

1. On the left navigation pane, click , and then select **Physical>Nodes**. Select the required node or cluster.
2. Select **Actions > Backup**. The Backup page displays, showing the nodes selected for backup.
3. Select one of the following:
 - o **Immediate**— Allows the back up to occur immediately.
 - o **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.
4. Click **OK**.

If you selected **Immediate** in [Step 3](#), 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. On the left navigation pane, click , and then select **Physical>Nodes**.
2. 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 27 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 27 Nodes Selected for Scheduled Backups

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

Table 7: 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.
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.

- 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 download 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 .
2. On the left navigation pane, select **System > Backup/Restore > Physical Nodes**.
3. Select one or more filenames on the Backup Files page.
4. Click **Delete**.

The system displays a dialogue to confirm that you want to delete the file.

5. 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

Backup files are text based and binary format. GigaVUE-FM restores the device configurations in binary format and allows you to view the configurations in text format. During the restore process, the commands listed in the configuration file are executed. If any error occur during the restore process, the text-based file makes it possible to edit the file and attempt to restore the configuration again by uploading and applying the modified file.

When restoring clusters, you can modify the file before uploading and applying it to the cluster. However, the modified file must have the same name as the backup file that was downloaded. If you change the file name, GigaVUE-FM will reject the file during the upload operation. The configuration file is applied to the current leader in a cluster and this node could be a different node than the one when the backup was done.

Notes:

- GigaVUE-FM does not support the restore operation if the cluster name changes. The cluster name should have the same name at the time of the restore operation as it did at the time of the backup operation.
- Text-based and Binary format backed up configurations created directly on the node, using the CLI, are also available for restoring from the GigaVUE-FM.
- In the Device Restore process, leader preferences for the cluster are only updated to the leader after restoring; they are not propagated to any of the standby nodes.

Restore Nodes and Clusters

To restore nodes or clusters, do the following:



1. On the left navigation pane, click , and then select **Physical>Nodes**. Select the required node or cluster.
2. Select the IP address for each node or cluster that you want to restore.
3. Select **Actions > Restore**.

The Restore From File page displays, showing the file names from which to restore.

4. 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.
5. 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/Restore > 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 occurred, 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 HC 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. On the left navigation pane, click , and then select **Physical>Nodes**. Select the required node or cluster.
2. Select **Settings > Config and Licenses > Configurations**.
The Configuration files page displays.
3. 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.

4. When confirmation dialog displays, click **Save** to save the GigaVUE HC Series node's current systems to the active configuration file.

You can also save the GigaVUE HC 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 or SCP. You can upload from a URL or IP address.

Share Configuration Files with Other GigaVUE HC 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 HC Series and GigaVUE 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](#)

Supported MIBs

Gigamon supports SNMP polling on GigaVUE HC Series and GigaVUE TA Series nodes using standard public MIBs. These MIBs enable polling of node and port statistics for integration with SNMP-based monitoring tools.

For Gigamon-specific information, you can load the private GIGAMON-SNMP-MIB. This MIB provides access to Gigamon's private MIB values and ensures that SNMP management software can correctly interpret Gigamon notification OIDs.

GIGAMON ENTERPRISE MIBs:

```
miboid['SNMP-COMMON-SMI-MIB'] = '.1.3.6.1.4.1.26866'
miboid['GIGASmart-MIB'] = '.1.3.6.1.4.1.26866.5'
miboid['GIGAMON-SNMP-MIB'] = '.1.3.6.1.4.1.26866.2.19.3'
```

STANDARD MIBs:

```
miboid['IFENTRY-MIB'] = '.1.3.6.1.2.1.2.2.1'
miboid['AT-MIB'] = '.1.3.6.1.2.1.3.1'
miboid['IP-MIB'] = '.1.3.6.1.2.1.4'
miboid['ICMP-MIB'] = '.1.3.6.1.2.1.5'
miboid['TCP-MIB'] = '.1.3.6.1.2.1.6'
miboid['UDP-MIB'] = '.1.3.6.1.2.1.7'
miboid['SNMP-MIB'] = '.1.3.6.1.2.1.11'
```

```
miboid['SNMP-HOST-MIB'] = '.1.3.6.1.2.1.25'  
miboid['IF-INTERFACE-MIB'] = '.1.3.6.1.2.1.2'  
miboid['INTERFACEX-MIB'] = '.1.3.6.1.2.1.31.1.1.1'  
miboid['CDP-MIB'] = '1.3.6.1.4.1.9.9.23'  
miboid['LLDP-MIB'] = '1.0.8802.1.1.2'  
miboid['SYSTEM-MIB'] = '.1.3.6.1.2.1.1'  
miboid['SNMPV3-MIB'] = '.1.3.6.1.6.3.18'  
miboid['IP-FORWARD-MIB'] = '1.3.6.1.2.1.4.24'
```

SNMP and Clusters

When working with a cluster of GigaVUE HC Series nodes, you configure SNMP hosts and notification events from the leader/VIP address. The settings are then pushed to each node. However, when a clustered node sends an SNMP notification, it is sent from its own Mgmt port, not from the leader/VIP address.

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

SNMP is supported on both Legacy (HiGig) and E-TAG clusters comprising of GigaVUE HC Series and GigaVUE TA Series devices. SNMP Get/Walk is supported on leader, standby, and member devices. SNMP Get/Walk can be performed using management and IP interfaces. Each device in a cluster must be polled separately for getting the port details.

NOTE: A GigaVUE TA Series node can never assume the role of a leader in a clustered environment.

Configure SNMP Notifications

GigaVUE HC Series nodes can send SNMP v2c/v3 traps to specified destinations based on a variety of events on the node. Configuring SNMP traps consists of the following major steps:

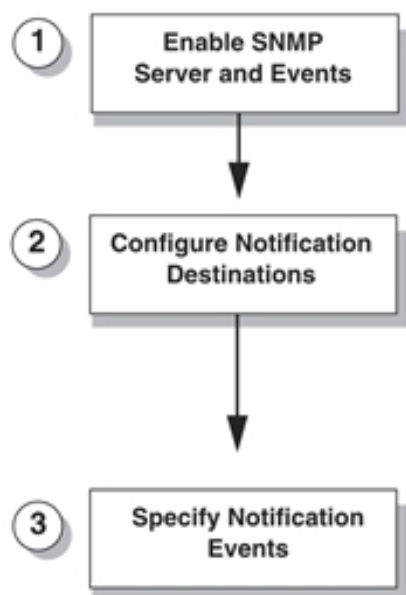


Figure 28 *Configuring SNMP Notifications*

Configure the SNMP Server and Notification Destinations

The SNMP server on the GigaVUE HC Series or GigaVUE TA Series must be enabled in order to send traps. This is done on the ADD SNMP Trap page, where you also specify the destinations for SNMP notifications sent from the GigaVUE HC Series or GigaVUE TA Series node.

NOTE: The recommended maximum number of SNMP trap destinations is five (5).

To specify a notification destination and enable the SNMP sever, do the following:

1. Select **Settings > Global Settings > SNMP Traps**.
2. Select **Remote Log Sinks** from the drop-down list.
3. Click **New**. The Add SNMP Traps page shown in [Figure 33 SNMP Settings Page](#) displays.

New SNMP Traps ⓘ

IP Address / Host Name *	Enter IP Address / Host Name
Community	Enter Community
Port *	162
Trap Type	v2c ▼
Notify Type	Select a Notify Type ▼
Trap Host	☐ Enable

Figure 29 Add SNMP Traps Page

4. Configure the notification destination by doing the following:
 - a. Enter the IP address for the trap destination in the **IP Address / Host Name** field. Both IPv4 and IPv6 addresses are supported for SNMP.
 - 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** 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.
5. Click **Apply**.

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**.

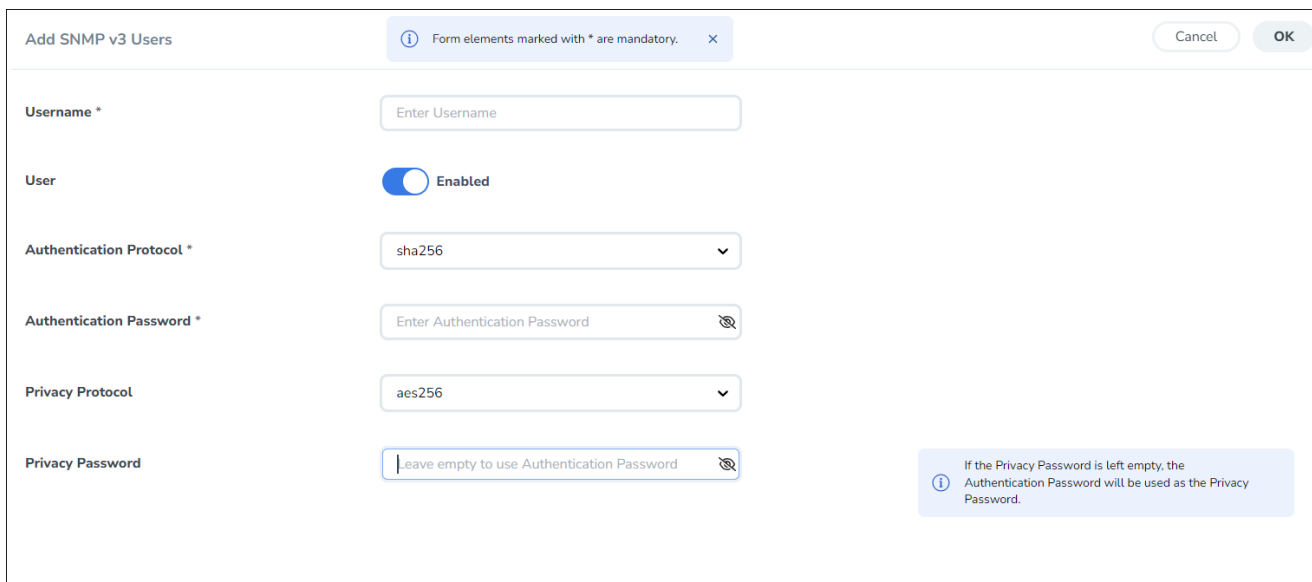


Figure 30 Add SNMP v3 Users

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** or **sha256** or **sha384** or **sha512**, which specified the mechanism to use for password hashing.

NOTE: MD5 authentication protocol is not supported in FIPS mode. When FIPS mode is enabled, SNMPv3 users must use FIPS-compliant algorithms such as SHA or SHA-2 for authentication.

- **Authentication Password**—the password used to authenticate the user specified by **Username**.
 - **Privacy Type**—the privacy type specifies the level of encryption for the password, which is either **des** or **aes-128** or **aes-256**.
 - **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 **OK**.

Enable Notifications

Once the GigaVUE HC Series or GigaVUE TA Series SNMP server is enabled, you can enable the sending of SNMP notifications from the SNMP through the SNMP page shown in [Figure 31SNMP Settings Page](#).

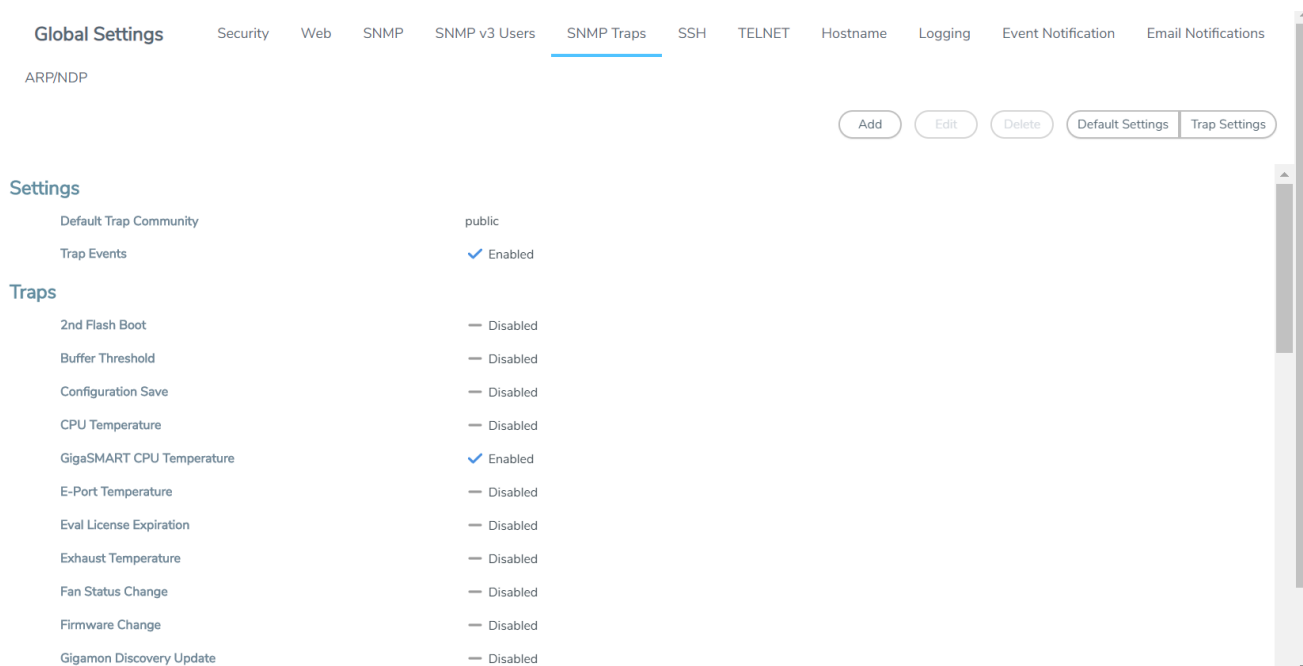


Figure 31 *SNMP Settings Page*

The GigaVUE HC Series and GigaVUE TA Series SNMP server is enabled so that management stations can poll the node remotely using standard SNMP commands (**Get**, **GetNext**, and **Walk**). The GigaVUE HC Series and GigaVUE TA Series nodes support MIB polling using the standard MIB-II OIDs.

Delete a Destination for SNMP Notifications

To delete a destination for SNMP notifications, do the following:

1. Select **Settings > Global Settings > SNMP Traps**.
2. Scroll to the bottom of the SNMP Traps page, and select the destination to delete under Remote Log Sinks. In [Figure 32 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 32 *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 HC Series node's MIB is available for download from the [Gigamon Documentation Library](#). The name of the MIB is GIGAMON-SNMP-MIB. Contact Technical Support for details.

Once you have received a copy of the MIB, you can compile it into your SNMP Management software to view intelligible descriptions of the OIDs included in the notifications.

View Associated Log Messages

SNMP events have log messages associated with them. The following table shows the log messages for each SNMP event.

Table 8: Log messages Associated with SNMP Event

SNMP Event	Description	Log Message
2ndflashboot	Secondary flash boot notification (for GigaVUE-TA100, GigaVUE-TA100-CXP, GigaVUE-HC1, and GigaVUE-HC3)	/gv/snmp/events/SecondFlashBoot
bufferoverusage	Buffer usage threshold crossing notification	/gv/snmp/events/buffer_threshold
gigasmartcputemp	GigaSMART engine temperature (for GigaVUE-HC1)	/gv/snmp/events/GigaSMARTCPUTemp
configsave	Configuration saved notification	
cputemp	CPU temperature notification (for GigaVUE-TA100, GigaVUE-TA100-CXP, GigaVUE-HC1, and GigaVUE-HC3)	/gv/snmp/events/CPUTemp
eporttemp	GigaSMART CPU (e1/e2 port) temperature notification (for GigaVUE-HC3)	/gv/snmp/events/EPortTemp
evallicensereminder	Evaluation license expiration notification	/gv/snmp/events/EvalLicenseReminder
exhausttemp	Exhaust temperature notification (for GigaVUE-TA100, GigaVUE-TA100-CXP, GigaVUE-HC1, and GigaVUE-HC3)	/gv/snmp/events/ExhaustTemp
fanchange	Fan status change notification	/gv/snmp/events/ResetSystem
firmwarechange	Firmware change notification	/gv/snmp/events/FirmwareChange
gdpupdate	GDP update notification	/gv/snmp/events/GdpUpdate
gscpuutilization	GigaSMART CPU utilization crossing threshold notification	/gv/snmp/events/CpuUtilization
gspacketdrop	GigaSMART packet drop notification	/gv/snmp/events/GsPacketDrop
gsresourceutilization	GigaSMART resource utilization notification	/gv/snmp/events/GsIsslResourceUtilization
ibstatechange	Inline bypass forwarding state change notification	/gv/snmp/events/IbStateChange
inlinetoolrecovery	Inline tool recovery notification	/gv/snmp/events/InlineToolRecovery

SNMP Event	Description	Log Message
linkspeedstatuschange	Port link status or port speed change notification	/gv/snmp/events/LinkSpeedStatusChange
lowportutilization	Port utilization low threshold crossing notification	/gv/snmp/events/BelowThreshold
modulechange	Module change notification	/gv/snmp/events/ModuleChange
operationmode	Operational mode change notification	/gv/snmp/events/SystemModeChange
opticstemp	Optics (transceiver) temperature notification (for GigaVUE-TA100, GigaVUE-TA100-CXP, and GigaVUE-HC3)	/gv/snmp/events/OpticsTemp
packetdrop	Packet drop notification	/gv/snmp/events/PacketDrop
policytrigger	Policy triggered notification	/gv/snmp/events/PolicyTriggered
portutilization	Port utilization high threshold crossing notification	/gv/snmp/events/OverThresholdChange
powerchange	Power supply status change notification	/gv/snmp/events/PowerChange
processcputhreshold	Process CPU threshold notification	/gv/snmp/events/CcProcessCpuThreshold
processmemthreshold	Process memory threshold notification	/gv/snmp/events/CcProcessMemThreshold
rxtxerror	Packet receive (RX) or transmit (TX) error	/gv/snmp/events/RxTxError
switchcputemp	Switch CPU temperature notification (for GigaVUE-TA100, GigaVUE-TA100-CXP, GigaVUE-HC1, and GigaVUE-HC3)	/gv/snmp/events/SwitchCPUTemp
syscputhreshold	System CPU threshold notification	/gv/snmp/events/CcSystemCpuThreshold
sysmemthreshold	System memory threshold notification	/gv/snmp/events/CcSystemMemThreshold
systemreset	System reset notification	/gv/snmp/events/ResetSystem
tunnelstatus	Tunnel status notification	/gv/gs/snmp/events/TunnelGwStatusChange
tunneldesstatus	Tunnel destination status notification	/gv/gs/snmp/events/TunnelDestStatusChange
unexpectedshutdown	Unexpected system shut down notification	/gv/snmp/events/UnexpectedShutdown

SNMP Event	Description	Log Message
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-hc3-144-20150506-150207/messages.1:May 6 14:26:33 hc3-144 mgmtd
[1829]: [mgmtd.INFO]: EVENT: /gv/snmp/events/LinkSpeedStatusChange
```

Enable the SNMP Server

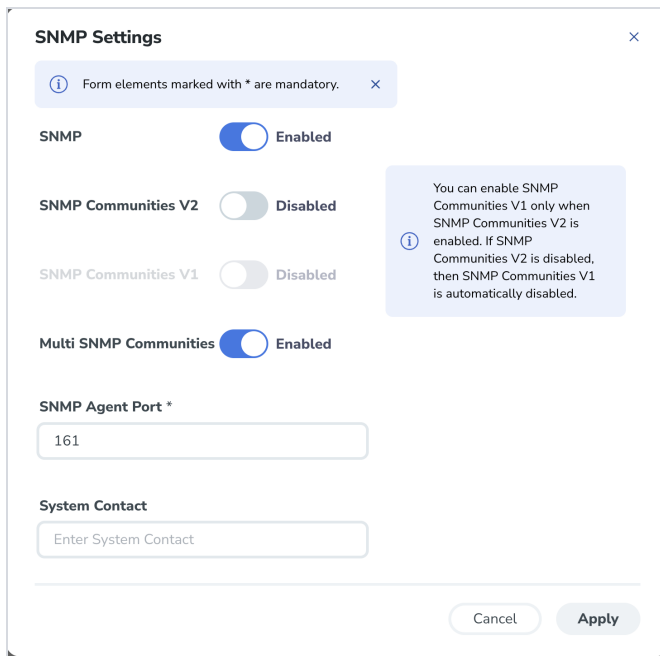
You can enable the GigaVUE HC Series or GigaVUE TA Series SNMP server so that the SNMP management side can send SNMP requests by using **Get**, **GetNext**, and **GetBulk** SNMP commands to poll the node. The GigaVUE HC Series and GigaVUE TA Series supports public MIBs, including partial MIB-II (ifTable and ifXTable).

The GigaVUE HC Series and GigaVUE TA Series SNMP server is enabled so that management stations can poll the node remotely using standard SNMP commands (**Get**, **GetNext**, and **Walk**). The GigaVUE HC Series and GigaVUE TA Series nodes support MIB polling using the standard MIB-II OIDs. You can retrieve statistics for any of the data ports. For a sample of ifIndex numbers, as well as a list of the supported statistics from the ifTable and ifXTable, refer to [Available SNMP Statistics for Data Ports](#).

You can also load Gigamon's MIB to view private MIB values.

To enable the SNMP server:

1. Select **Settings > Global Settings > SNMP**.
2. On the SNMP page, click **Settings**. The SNMP Settings page displays as shown in [Figure 33 SNMP Settings Page](#)



The image shows the 'SNMP Settings' configuration window. At the top, there is a header 'SNMP Settings' and a close button 'X'. Below the header is a message bar: 'Form elements marked with * are mandatory.' with an information icon 'i' and a close button 'X'. The settings are as follows:

- SNMP**: Enabled (toggle switch)
- SNMP Communities V2**: Disabled (toggle switch)
- SNMP Communities V1**: Disabled (toggle switch)
- Multi SNMP Communities**: Enabled (toggle switch)
- SNMP Agent Port ***: 161 (text input field)
- System Contact**: Enter System Contact (text input field)

At the bottom right, there are 'Cancel' and 'Apply' buttons. A blue information box on the right side contains the following text: 'You can enable SNMP Communities V1 only when SNMP Communities V2 is enabled. If SNMP Communities V2 is disabled, then SNMP Communities V1 is automatically disabled.'

Figure 33 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 or 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 HC Series and GigaVUE TA Series node, it provides MIB-II statistics for all data (network and tool) ports. Data ports are numbered sequentially with ifIndex numbers starting from the leftmost slot (slot 1) and proceeding sequentially through all slots. Within a slot, ports are numbered sequentially starting with the 10Gb ports and then the 10/100/1000 ports. For example, on a PRT-H00-X12G04 line card, ports number sequentially from 1/1/x1..1/1/x12 and then g1..g4.

You can use the **ifDescr** OID to correlate an ifIndex with a data port number on the GigaVUE HC 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 HC 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 OID	Value for a PRT-H00-X12G04 in Slots 1/2
ifDescr.5; Value (OctetString)	1/1/x5
ifDescr.6; Value (OctetString)	1/1/x6
ifDescr.7; Value (OctetString)	1/1/x7
ifDescr.8; Value (OctetString)	1/1/x8
ifDescr.9; Value (OctetString)	1/1/x9
ifDescr.10; Value (OctetString)	1/1/x10
ifDescr.11; Value (OctetString)	1/1/x11
ifDescr.12; Value (OctetString)	1/1/x12
ifDescr.13; Value (OctetString)	1/1/g1
ifDescr.14; Value (OctetString)	1/1/g2
ifDescr.15; Value (OctetString)	1/1/g3
ifDescr.16; Value (OctetString)	1/1/g4
ifDescr.17; Value (OctetString)	1/2/x1
ifDescr.18; Value (OctetString)	1/2/x2
ifDescr.19; Value (OctetString)	1/2/x3
ifDescr.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
- ifHCOctets
- ifHCOUcastPkts
- ifHCOMulticastPkts
- ifHCOBroadcastPkts

Monitor Utilization

This chapter describes how to monitor the system health information and port utilization on the GigaVUE HC Series and GigaVUE TA Series nodes. It also provides commands to enable the system health threshold checks and set the buffer thresholds for port utilization. Refer to the following sections for details:

- [View System Health Information](#)
- [Work with Port Utilization Measurements](#)
- [Configure Alarm Buffer Thresholds](#)

View System Health Information

You can view the system health information for a specified node or for each node in a cluster by displaying the system health statistics. The system health statistics provide visibility into the CPU and memory usage, and the processes that are consuming the largest amount of CPU and memory resources in the node.

The **show system-health** command displays the CPU and memory utilization percentage for different time intervals, hence providing historical trends for CPU and memory utilization.

Optional SNMP notifications are triggered when the aggregate system CPU or memory usage exceeds the pre-defined threshold values.

Refer to the following sections for details:

- [Display the System Health Statistics](#)
- [Enable the System Health Threshold Notification](#)
- [Configure the System Health Threshold](#)

Display the System Health Statistics

Use the **show system-health** command to display the system CPU and memory statistics for all of the nodes in the cluster.

Use the **show system-health box-id <box id>** command to display the system CPU and memory statistics for a specified node in the cluster.

The CPU utilization statistics display the CPU load average over the last 1 minute, 5 minute, and 15 minute intervals. The CPU usage is displayed over the last 5 secs, 1 minute, and 5 minutes. In addition, all the processes running in the cluster or a specified node in the cluster display the CPU utilization for the last 5 second, 1 minute, and 5 minute intervals. The process consuming the largest amount of CPU is displayed at the top.

The memory usage statistics display the total, used, and free amount of physical and swap memory available, as well as the memory usage for all the processes, with the process consuming the largest amount of memory displayed at the top.

[Table 9: Statistics for CPU Utilization](#) describes the statistics for CPU utilization:

Table 9: 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 10: 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
syssth                 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
syscth	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.

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_mgmd	process cpu (mgmd)	>= 98% (600 sec)	syslog, snmp trap
rule_proc_mem_mgmd	process mem (mgmd)	>= 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_liscd	process cpu (liscd)	>= 98% (600 sec)	syslog, snmp trap
rule_proc_mem_liscd	process mem (liscd)	>= 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_syssth	process cpu (syssth)	>= 98% (600 sec)	syslog, snmp trap
rule_proc_mem_syssth	process mem (syssth)	>= 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, SCP, SFTP

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

Work with Port Utilization Measurements

The GigaVUE HC Series and GigaVUE TA Series nodes include the port utilization features summarized in the following table:

Feature	CLI Command
View Port Utilization Percentage You can view the percentage utilization measurement over the last second for one or more ports. Refer to View Port Utilization.	<pre>show port utilization all box-id <box ID> port-list <port list> slot <slot ID></pre>
Configure Percentage Utilization You can configure the utilization percentage at which the GigaVUE HC 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.	<pre>port <port list> alarm low-utilization-threshold <percentage>port <port list> alarm high- utilization-threshold <percentage></pre>

Port Utilization Availability by Port Type

You can view port utilization for all network, tool, hybrid, and stack link ports on the GigaVUE HC Series or GigaVUE TA Series node.

View Port Utilization

Use the **show port utilization** command to view the percentage utilization measurement over the last second for one or more ports.

If you use the **show port utilization** command without any arguments, the last measured utilization values for all ports in the node (or cluster, if configured) are shown.

Format of show port utilization Output

The **show port utilization** command lists the utilization for all requested ports with the port number, port type, port speed, receive (rx) utilization percentage (network and stack ports), transmit (tx) utilization percentage (tool, hybrid, and stack ports), alarm threshold (high and low), and the last time the threshold was exceeded on either the transmit or receive direction.

The following table shows sample output for a **show port utilization port 13/1/x1** command.

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/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 HC 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 HC Series node will log an alarm for the specified ports. By default, the thresholds are 0 , which means disabled.

NOTE: Network ports always use an Rx threshold; tool ports always use Tx. Stack ports and hybrid ports use both Rx and Tx; the same threshold is used for each.

Utilization Alarm/SNMP Notification Generation

Utilization alarms are written to syslog and forwarded to all SNMP management stations configured as notification destinations. For SNMP notifications to be generated, forwarded, and displayed correctly in your SNMP management station, all of the following must be true:

Requirement	Description
SNMP Enabled	Use the snmp-server enable options to turn on the node's SNMP functionality and enable notifications.
SNMP Destinations Configured	Use the snmp-server host options in the CLI to specify the IP addresses for SNMP notification destinations.
SNMP Notifications Enabled for Utilization Alarms	Use the portutilization argument for the snmp-server notify event command to enable high utilization notifications. For example: (config) # snmp-server notify event portutilization Use the lowportutilization argument for the snmp-server notify event command to enable low utilization notifications. For example: (config) # snmp-server notify event lowportutilization Refer to Configure Port Utilization Thresholds and Notifications.
GigaVUE MIB Compiled at Management Station	You can obtain Gigamon's latest private MIB file by contacting support@gigamon.com .

Refer to [Use SNMP](#) for information on configuring the GigaVUE HC 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 portutilization and lowportutilization.

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 portutilization 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 lowportutilization 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 lowportutilization 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 portutilization alarm is enabled, it will be sent. If the high utilization threshold is then disabled, a clear notification will be sent.

Configure Alarm Buffer Thresholds

Often network ports are utilized at rates below 50%. If several network ports are aggregated, there is a risk of oversubscribing the tool ports. Alarm buffer thresholds are used to monitor the congestion within the GigaVUE node caused by microbursts or by oversubscription of tool ports.

The buffer usage on any port remains at zero until the maximum line rate of the port is reached. When the usage crosses 100% either instantaneously, in the microburst case, or prolonged, in the oversubscription case, there is congestion.

The internal buffer on the GigaVUE node can absorb a certain number of packet bursts. During congestion, packets are buffered in the chassis and the buffer usage is reported on the corresponding ports and in the corresponding direction: rx (ingress) and tx (egress).

Reporting the buffer usage provides a trend of how the microbursts are causing congestion, so more tool ports can be added before packets are dropped. Buffer usage is measured in intervals of 5 seconds. The peak buffer usage within a 5-second interval is reported. Use the **show profile** commands to see trends of buffer usage over time.

When buffer usage is less than or equal to zero, there is no congestion, so no packets are dropped due to buffer unavailability.

When buffer usage is greater than zero, there is congestion. When buffer usage is greater than zero on any port in any direction, there is a chance that the packets (that caused the buffer usage to increase) are dropped due to unavailable buffers. However, it is unlikely to see packet drops due to buffer unavailability when the buffer usage on a port is less than 5%.

The buffer usage feature is supported on all ports and module types on the GigaVUE-HC3.

Refer to the following sections for configuring buffer thresholds and for configuring a notification that can be sent when a threshold is exceeded:

- [Set Alarm Buffer Thresholds](#)
- [Configuration Example](#)
- [Buffer Usage Alarm](#)

Set Alarm Buffer Thresholds

Use the **card slot <slot id> alarm buffer-threshold** command to set an alarm buffer threshold on the slots of a GigaVUE node.

The card level threshold indicates usage levels of the node.

The following table describes the arguments:

Argument	Description
card slot <slot ID>	Specifies the slot.
alarm buffer-threshold <0-100%>	Sets the alarm buffer threshold for a slot, as a percentage. By default, the threshold is set to 0, which disables the threshold. NOTE: On the GigaVUE-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
-----
12/1/x5    41      N/A    2014/07/01 17:30:07.371  N/A      30
N/A12/1/x6    39      N/A    2014/07/01 17:30:07.378  N/A      32
N/A12/1/x2    35      N/A    2014/07/01 17:30:07.384  N/A

```

Use the following command to display the current buffers:

(config) # show profile current buffer all

```

12/1/x2 counters  value-----
      RX: 0      TX: 37      RX Config: 0      TX
Config: 35Last Time Exceeding: 2014/07/01 17:30:07.384
12/1/x5 counters  value-----
      RX: 41      TX: 0      RX Config: 30      TX
Config: 0Last Time Exceeding: 0
12/1/x6 counters  value-----

```

```

RX: 39 TX: 0 RX Config: 32 TX
Config: 0Last Time Exceeding: 0

```

Use the following command to display the last minute of buffer history for a specific port:

(config) # show profile history buffer 12/1/x5 min

```

=====Port: 12/1/x5 minute history
report=====
Counter Name      0 sec ago      5 secs ago      10 secs ago      15 secs ago
=====
RX:              44              44              44              44
TX:              0              0              0              0
RX Config:       30              30              30              30
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
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
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.

Web

This section provides the steps required to configure the GigaVUE HC Series node's web server used for GigaVUE-FM access to the node. GigaVUE-FM is Gigamon Web-based GUI for the GigaVUE HC Series node, providing graphical user interface configuration.

To access the Web page of the node:



1. On the left navigation pane, click  under **Physical** select **Nodes**. This displays the list of Devices/Cluster Nodes managed by this instance of GigaVUE-FM.
2. Click the Cluster ID of any node to open the node.
3. Once you are in the node, click **Settings > Global Settings > Web**.
4. Select or enter the following details:

Field	Description
Setting	
HTTP Port	HTTP port.
HTTPS	Use the toggle option to enable and disable HTTPS.
HTTPS Port	HTTPS port number.
Auto Logout Timeout	The maximum duration of user inactivity before a Web session is logged out automatically.
Web Session Renewal	Specifies the length of time before a session expires that the Web server will issue a new cookie and renew the session. This should be set at least as long as the auto-logout setting so that sessions do not expire before they have a chance to be renewed.
Session Timeout	
Web Proxy Settings	
Web Proxy Address	Web proxy address. This can be either IPv4 or IPv6 address.
Web Proxy Port	Web proxy port. If you do not specify a port, the default is 1080.
Authentication Type	Can be either basic or none.
Basic Auth Username	Basic authentication username.
Basic Auth Password	Basic authentication password.

Click **Apply** to save the configuration.

Refer to [Configure TLS Parameters](#).

Enabled TLS Cipher Suites

TLS 1.2 Ciphers

Classic mode

GigaVUE-OS supports the commonly-supported TLS 1.2 ciphers. The following ciphers are supported in TLS 1.2:

- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256

FIPS mode

The following Secure (FIPS) mode ciphers are supported in TLS 1.2:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384

Crypto mode

The following Secure (Crypto) mode ciphers are supported in TLS 1.2:

- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384

Curves

The following Curves are supported:

- secp521r1
- secp384r1
- prime256v1

TLS 1.3 Ciphers

Classic mode

GigaVUE-OS supports the commonly-supported TLS 1.3 ciphers. The following ciphers are supported in TLS 1.3:

- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256

FIPS mode

The following Secure (FIPS) mode ciphers are supported in TLS 1.3:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384

Crypto mode

The following Secure (Crypto) mode ciphers is supported in TLS 1.3:
TLS_AES_256_GCM_SHA384

Groups

The following groups are supported:

- secp521r1
- secp384r1
- prime256v1

Rules and Notes - Limitations

Keep in mind the following rules and notes when working with TLS ciphers:

- TLS configuration is available only if all managed physical devices are running version 6.14 or above. Devices on lower versions must be upgraded to 6.14 to access TLS configuration settings.
- When adding any device running version 6.14 or above, all configured TLS ciphers on the device will be replaced by the Global FM cipher configuration. Similarly, when upgrading the device to version 6.14 or above, these ciphers will be applied to the device.
- **Certification:** When selecting ECDSA and RSA-based ciphers, the device must have the corresponding ECDSA and RSA certifications installed, respectively.
- **Default TLS ciphers:** On fresh GigaVUE-FM 6.14 installs, all supported TLS ciphers are selected by default in the global TLS configuration and pushed to 6.14 devices.
- **CLI: web server ssl min-version** command is deprecated in 6.14; use **system tls min-version <tlsversion>**
- **UI:** In GigaVUE-FM 6.14 and above, TLS minimum version controls; configuration must be done via the  > **Settings** > **System** > **Cipher**.
- To view which TLS configuration settings, go to **Inventory**  > **Physical** > **Nodes** in GigaVUE-FM and navigate to the  > **Settings** > **System** > **Global Settings** > **TLS tab**.

- **Legacy mode:** The behavior of existing configurations remains unchanged with the introduction of the new feature.

System Warnings

- **Error – No Common Ciphers:**
 - On the GigaVUE-FM global TLS configuration page, if the selected ciphers do not include any from the common cipher set, an error is displayed and saving the configuration is blocked. The common ciphers are consistent across version 6.14 and above, and apply to all three modes: Classic, FIPS, and Crypto.
 - An informational banner is displayed listing the common TLS ciphers between GigaVUE-FM and the selected device(s), helping you quickly identify and select valid options when no common cipher has been chosen.
- **General Behavior:** When a device with CLI-configured ciphers is upgraded / mode-changed and managed by GigaVUE-FM, the global TLS selection is pushed, removing any CLI-only ciphers. This may break TLS connections with third-party servers.

Exceptions

- If TLS ciphers are edited outside the GigaVUE-FM global configuration via device CLI and none overlap with the GigaVUE-FM global selection, GigaVUE-FM and device TLS connections will fail and GigaVUE-FM cannot manage the device until a common cipher is restored.
- Devices on versions earlier than 6.13 do not support TLS 1.3 and may see connection disruptions when TLS 1.3 is configured in GigaVUE-FM.
- Configuring ciphers directly via CLI can cause mismatches between CLI and GigaVUE-FM views until the next config sync/apply realigns the device with the GigaVUE-FM global template.
- GigaVUE-FM supports TLS cipher configuration only via the global TLS template — no UI or REST API exists for per-node/per-device configuration. Per-device customization must be done via CLI.

NOTE: When upgrading from version 6.12.02 or 6.13.00 to 6.14 or above device, the TLS ciphers configured in GigaVUE-FM will be retained. These ciphers will then be pushed to applicable devices (6.14 and above) and managed through GigaVUE-FM.

Refer to [System](#) for tls commands.

About

To view the About page (refer to the following figure):

1. On the left navigation pane, go to **Inventory**  and select **Physical > Nodes**.
2. Click on a node listed in the page.
3. In the Node Overview page, select **About** (under support).

The **About** provides the following information:

- Product Name—The name of the product, GigaVUE-OS.
- Version—The current version running. For example, 4.8.00.
- Build ID and Build Date—Information about when the current build was created.
- Version Summary—A detailed description of the currently installed version.
- Git Hash—Additional build information.
- U-Boot Version—The currently installed u-boot version.
- CPLD Version—System information.
- TS Version—System information. This field displays information only when a timestamp card is inserted in the chassis.
- Model—The node model. For example, GigaVUE-HC1-Plus.
- Serial Number—Serial number of the node.
- Host Name—The host name assigned to the node. For information about setting the host name, refer to [Configure the Host Name](#)
- Host ID—Host id of the node.
- Start-up time—The date that the current version was installed and the number of hours, minutes, and seconds that the node has been running.

GigaVUE-OS Information

Name	Information
Product Name	GigaVUE-OS
Version	6.4.00.02
Build ID	413960
Build Date	Debug 2023-10-12
Version Summary	GigaVUE-OS 6.4.00.02 Build 413960 Debug 2023-10-12 21:36:51 x86_64 gihc3 root@jenkins-slave601:git:9bc89e4b4ede
Git Hash	9bc89e4b4ede9556cab35b3bfcd22f811ba95366
U-Boot Version	N/A
Ts Version	—
Model	HC3
Serial Number	JD39A
Host Name	gigamon-a0d39a
Host ID	eaf72ba0d39a

© 2023 Gigamon Inc. All Rights Reserved.

Figure 34 About Page

Additional Sources of Information

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

- [How to Download Software and Release Notes from My Gigamon](#)
- [Documentation Feedback](#)
- [Contact Technical Support](#)
- [Contact Sales](#)
- [The VUE Community](#)

Documentation

©This table lists all the guides provided for GigaVUE software and hardware. The first row provides an All-Documents Zip file that contains all the guides in the set for the release.

NOTE: In the online documentation, view [What's New](#) to access quick links to topics for each of the new features in this Release; view [Documentation Downloads](#) to download all PDFs.

Table 1: Documentation Set for Gigamon Products

GigaVUE 6.14 Hardware and Software Guides	
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing Edit > Advanced Search from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.	
Hardware	how to unpack, assemble, rackmount, connect, and initially configure ports the respective GigaVUE devices; reference information and specifications for the respective GigaVUE devices
GigaVUE-HC1 Hardware Installation Guide	
GigaVUE-HC3 Hardware Installation Guide	
GigaVUE-HC1-Plus Hardware Installation Guide	
GigaVUE-HCT Hardware Installation Guide	
GigaVUE-TA25 Hardware Installation Guide	
GigaVUE-TA25E Hardware Installation Guide	
GigaVUE-TA100 Hardware Installation Guide	
GigaVUE-TA200 Hardware Installation Guide	
GigaVUE-TA200E Hardware Installation Guide	
GigaVUE-TA400 Hardware Installation Guide	

GigaVUE 6.14 Hardware and Software Guides
GigaVUE-TA400E Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliances Guide
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE-Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
GigaVUE Application Intelligence Solutions Guide
GigaVUE Inline Solutions Guide(NEW) (previously included in the GigaVUE Fabric Management Guide)
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Applications Guide
GigaVUE Cloud Suite Deployment Guide - AWS
GigaVUE Cloud Suite Deployment Guide - Azure
GigaVUE Cloud Suite Deployment Guide - OpenStack
GigaVUE Cloud Suite Deployment Guide - Nutanix
GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
Universal Cloud TAP - Container Deployment Guide
Gigamon Containerized Broker Deployment Guide

GigaVUE 6.14 Hardware and Software Guides

GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions

GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions

Reference Guides

GigaVUE-OS CLI Reference Guide

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

GigaVUE-OS Security Hardening Guide

GigaVUE Firewall and Security Guide

GigaVUE Licensing Guide

GigaVUE-OS Cabling Quick Reference Guide

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

GigaVUE-OS Compatibility and Interoperability Matrix

compatibility information and interoperability requirements for Gigamon devices

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

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

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

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

Release Notes

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

new features, resolved issues, and known issues in this release ;
important notes regarding installing and upgrading to this release

Note: Release Notes are not included in the online documentation.

Note: Registered Customers can log in to [My Gigamon](#) to download the Software and Release Notes from the Software and Docs page on to [My Gigamon](#). Refer to [How to Download Software and Release Notes from My Gigamon](#).

In-Product Help

GigaVUE-FM Online Help

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

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

Documentation Feedback Form		
About You	Your Name	
	Your Role	
	Your Company	

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The VUE Community

The [VUE 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 VUE Community site to:

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

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

Register today at community.gigamon.com

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

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

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

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

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

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)