



GigaVUE-OS H-VUE Administration Guide

GigaVUE-OS 5.6.00

Document Version: 3.0 (*Change Notes*)

COPYRIGHT

Copyright © 2019 Gigamon Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without Gigamon's written permission.

TRADEMARK ATTRIBUTIONS

Copyright © 2019 Gigamon Inc. All rights reserved. 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.

DOCUMENT REVISION – 5/9/2019

Change Notes

When a document is updated, the document revision number on the cover page will indicate a new revision number, the Document Revision date is updated on the title page, and this table will describe what changed.

Rev	Date	Change
rev 1	03/29/2019	Original release of document with the 5.6.00 release.
rev 2	04/12/2019	As part of effort to streamline the documentation set, the GigaVUE-OS CLI User's Guide has been transformed into the GigaVUE-OS CLI Reference Guide. Detailed feature descriptions that were previously provided in the GigaVUE-OS CLI User's Guide are now incorporated into the GigaVUE-OS HVUE Administration Guide. Added the following sections: <ul style="list-style-type: none">• Monitoring Utilization on page 185
rev 3	05/09/2019	5.6.00.02 Update: Updated the FIPS and Common Criteria sections of the Configuring Security Options chapter and removed the list of supported browsers as this information is now maintained in the Release Notes.

Contents

PART 1: Getting Started	9
1 Introducing the GigaVUE Nodes	11
About the GigaVUE H Series and TA Series	11
GigaVUE H Series Features and Benefits	15
The Gigamon Visibility Platform	15
Features and Benefits	16
2 Navigating H-VUE	19
Home	20
Overview	20
Traffic	21
Ports	21
Maps	22
GigaSMART	22
Inline Bypass	23
Active Visibility	23
System	24
Chassis	24
Roles and Users	25
Settings	25
Support	27
Getting Started	27
Help Topics	27
About	27
Quick View	27
Table View Customization	28
Using Search	28
Searching	29
Advanced Searching	30
3 Accessing H-VUE From GigaVUE-FM	33
4 GigaVUE H-VUE Overview	35
Overview Page	36
Systems	36
Ports Down	38

Ports with Packet Drops	38
Traffic	39
Over-Utilized Ports	40
Traffic Pages	41
Ports	41
Maps	42
GigaSMART	42
Inline Bypass	42
System Pages	43
Chassis	43
Roles and Users	43
5 Getting Started with GigaVUE H-VUE	45
Logging In to GigaVUE-OS H-VUE	46
Initial User Account Configuration (Optional)	47
Changing Passwords and Setting Up Basic Accounts	47
Changing the admin Account Password	47
Setting Up Some Basic Accounts	48
Adding a New Monitor User	51
Enabling/Disabling a User Accounts	52
Account Status	52
GigaVUE-OS Password Policies	53
Resetting Password on GigaVUE Nodes	55
Password Expiry	55
Configuring the Host Name	55
Configuring Time Options	55
Setting Time Manually	56
Using NTP Time Server for Clock Synchronization	57
Performing One-Time NTP Server Synchronization	58
Configuring Logging	59
External Syslog Servers and Clustered Nodes	60
Deleting an External Syslog Server	60
Packet Format for Syslog Output	60
Configuring Automatic Email Notifications	61
Configuring the Email Server Settings	61
Configuring the Event Settings	62
Adding Email Notification Recipients	63
Using a Custom Banner	63
Viewing Information About the Node	65
About	65
Interface	66
DNS	69
Cluster Safe and Limited Modes	69
Safe Mode	70
Limited Mode	71
Enabling SNMP Trap for Safe Mode and Limited Mode	72
Collecting Information for Technical Support	72
Supported Browsers	73

Configuring Internet Explorer for Use with H-VUE	73
6 Configuring Security Options	75
About Security and Access	76
Management Port Security	77
About Role-Based Access	78
Configuring Role-Based Access: A Summary	79
About Locks and Lock Sharing	80
Configuring Authentication and Authorization (AAA)	81
Overview of the AAA Page	82
Authentication Priority	82
User Mapping	82
Password	83
Lockout	83
Non Local User Authentication	84
FAQ for Logins and Passwords	84
Do Passwords Expire?	84
What Happens After Unsuccessful Logins?	84
Can a User be Forced to Change Their Password?	84
Are Passwords Displayed?	84
Who Creates Users and Passwords?	84
Configuring AAA Authentication Options	85
Remote Authentication Only	87
Authorization of User Account	88
Next Steps	88
Granting Roles with External Authentication Servers	88
Assigning Role in AAA Servers	90
Creating Users for AAA and Remote Authentication Server	90
Configuring AAA Authorization	91
Example	92
Adding AAA Servers to the Node's List	94
Adding a RADIUS Server	94
Adding a TACACS+ Server	95
Adding an LDAP Server	97
Setting the LDAP Server Default Settings	97
Configuring Roles in External Authentication Servers	101
Configuring Cisco ACS: RADIUS Authentication	101
Configuring Cisco ACS: TACACS+ Authentication	103
Configuring LDAP Authentication	105
Supported Clients	107
Default Ports	108
FIPS 140-2 Compliance	109
UC APL Compliance	110
Configuring UC APL	110
Accepting DoD Web Server Certificates	110
Enabling Login Failure Tracking	110
Displaying Unsuccessful Login Attempts	111
Common Criteria	112
Configuring Common Criteria	112

Configuring Secure Cryptography Mode	113
Enabling Secure Cryptography Mode	113
Disabling Secure Cryptography Mode	113
Ciphers to Use with Secure Cryptography Mode	114
Cryptographic Algorithms	114
Status of Secure Cryptography Mode	115
Configuring Secure Passwords Mode	115
Managing Blank Passwords	116
Encrypting Syslog Audit Data	118
Encryption Procedure	119
Displaying Logging Information	120
GigaVUE-OS Security Hardening	121
SHA1-Based Signature in TLS/SSL Server X.509 Certificate	121
ICMP Timestamp Response	122
TCP Timestamp Response	122
Non-Standard SNMP Community Name	123
Best Practices for Security Hardening	123
Using Telnet is Not Recommended	123
Using SNMPv1 and SNMPv2 are Not Recommended	123
Using Self-Signed Certificates are Not Recommended	124
Using FTP and TFTP are Not Recommended	124
Using Secure Cryptography Mode to Run Scans is Recommended	124
Changing the Password on admin Account	124
Messages Associated with Changing the admin Account Password	124
Best Practices for Passwords	125
7 Licensing GigaVUE TA Series	127
Perpetual GigaVUE TA Series Licenses	128
Applying Licenses for GigaVUE TA Series	128
Moving a License between GigaVUE TA Series	130

PART 2: System..... 131

8 Chassis	133
Chassis View	133
Chassis View + Transceiver View	135
Chassis View + Port View	136
Line Card and Module Numbering	137
Table View	138
Actions Menu	140
Reloading a GigaSMART Line Card or Module	140
Change Mode	141
Configuring the Card Mode on a GigaVUE-TA1 or GigaVUE-TA10	141
Change Port Mode	143
Enabling Advanced Fabric Hashing	145
Fabric Advance Hashing	146

9	Managing Roles and Users	149
	About Role-Based Access	149
	Role-Based Access and Flow Mapping	149
	Locks and Lock Sharing	149
	Role-Based Access: Rules and Notes	150
	User Management	150
	Role Management	150
	Port Ownership	151
	Configuring Role-Based Access and Setting Permissions in H-VUE	151
	Adding Users	151
	Creating Roles	152
	Associating Roles with Port Permissions	153
	Setting Locks and Lock-Shares	154
	Removing a Lock from a User's Port	154
	Removing a User's Lock-Share	154
	Locking a Port for a User	155
	Setting Map-Sharing Permission Levels	155
10	Reboot and Upgrade Options	157
	Rebooting Nodes	157
	Upgrading Software	158
	Working with Configuration Files in the Configurations Page	163
11	Backup and Restore	167
	What Is Saved In a Configuration File	167
	Saving a Configuration File	168
	Sharing Configuration Files with Other GigaVUE H Series Nodes	171
12	Using SNMP	173
	SNMP and Clusters	173
	Configuring SNMP Notifications	173
	Configuring the SNMP Server and Notification Destinations	174
	Configuring SNMP v3 Users	175
	Enabling Notifications	175
	Deleting a Destination for SNMP Notifications	176
	Enabling or Disabling Events for SNMP Notifications	177
	Receiving Traps	178
	Viewing Associated Log Messages	178
	Enabling the SNMP Server	180
	Configuring Other SNMP Server Settings	181
	Recommendations for Vulnerabilities	182
	Available SNMP Statistics for Data Ports	182
	SNMP Statistics	183
13	Monitoring Utilization	185
	Viewing System Health Information	185
	Displaying the System Health Statistics	186
	Enabling the System Health Threshold Notification	189

Configuring the System Health Threshold	190
Viewing the System Health Events	192
Enabling System Health Events for SNMP Notifications	192
Viewing the System Health Diagnostics	192
Configuring Packet Capture	193
Packet Capture Limitations	195
Working with Port Utilization Measurements.	196
Port Utilization Availability by Port Type	196
Viewing Port Utilization	196
Format of show port utilization Output.	196
Examples.	197
Port Utilization Thresholds	197
Utilization Alarm/SNMP Notification Generation	197
Configuring Port Utilization Thresholds and Notifications	198
Configuring Alarm Buffer Thresholds	200
Setting Alarm Buffer Thresholds	201
Configuration Example	202
Buffer Usage Alarm	203
Additional Sources of Information	205
Documentation	205
Documentation Feedback	206
Contacting Technical Support	206
Contacting Sales	206
The Gigamon Community	206

Getting Started

This section covers the following topics to help get you started with GigaVUE-OS H-VUE:

- [Introducing the GigaVUE Nodes](#) on page 11
- [Accessing H-VUE From GigaVUE-FM](#) on page 33

1 Introducing the GigaVUE Nodes

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

- [About the GigaVUE H Series and TA Series](#) on page 11
- [GigaVUE H Series Features and Benefits](#) on page 15



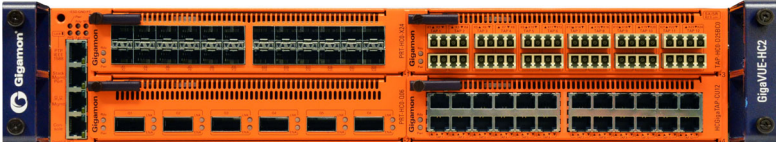
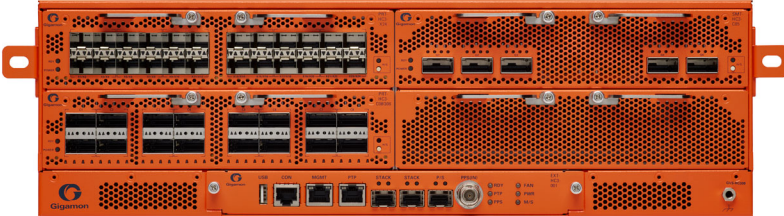
About the GigaVUE H Series and TA Series

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

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

- GigaVUE-HB1
- GigaVUE-HC1
- GigaVUE-HC2
- GigaVUE-HC3
- GigaVUE-HD4
- GigaVUE-HD8
- GigaVUE-TA1
- GigaVUE-TA10
- GigaVUE-TA40
- GigaVUE-TA100
- GigaVUE-TA100-CXP
- GigaVUE-TA200
- Certified Traffic Aggregation White Box

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

<p>GigaVUE-HB1</p>	<ul style="list-style-type: none"> • 1RU Footprint • Built-in GigaSMART Functionality • Standard GigaVUE-OS CLI and H-VUE GUI • Cluster with GigaVUE H Series and GigaVUE TA Series Nodes 	
<p>GigaVUE-HC1</p>	<ul style="list-style-type: none"> • 1RU Footprint • Built-in GigaSMART functionality • Standard GigaVUE-OS CLI and H-VUE GUI • Cluster with GigaVUE H Series and GigaVUE TA Series Nodes 	
<p>GigaVUE-HC2</p>	<ul style="list-style-type: none"> • 2RU Footprint • Four front-facing bays for port, TAP, BPS, and GigaSMART front modules • One rear bay for a GigaSMART rear module • Standard GigaVUE-OS CLI and H-VUE GUI • Cluster with GigaVUE H Series and GigaVUE TA Series Nodes 	
<p>GigaVUE-HC3</p>	<ul style="list-style-type: none"> • 3RU Footprint • Four Module Slots (Bays) • Internal Control Card • Extension Board • Dedicated Cluster Management Port • Standard GigaVUE-OS CLI and H-VUE GUI • Supports all GigaVUE-HC3 Modules • Cluster with GigaVUE H Series and GigaVUE TA Series Nodes 	

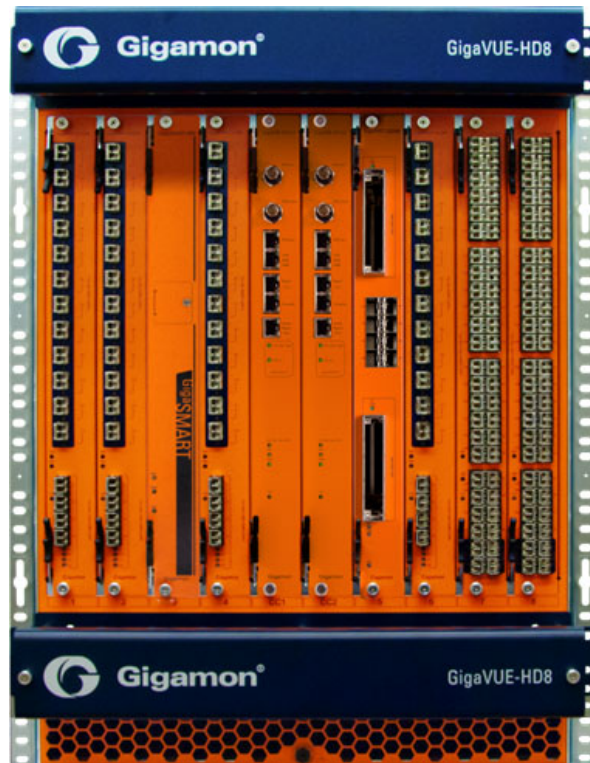
GigaVUE-HD4

- 5RU Footprint
- Four Line Card Slots
- Single Control Card
- Dedicated Cluster Management Port
- Supports all GigaVUE HD Series Line Cards
- Standard GigaVUE-OS CLI and H-VUE GUI
- Cluster with GigaVUE H Series and GigaVUE TA Series Nodes



GigaVUE-HD8







- 14RU Footprint
- Eight Line Card Slots
- Dual Control Cards
- Dedicated Cluster Management Port
- Supports all GigaVUE HD Series Line Cards
- Standard GigaVUE-OS CLI and H-VUE GUI
- Cluster with GigaVUE H Series and GigaVUE TA Series Nodes



GigaVUE-TA1

- 1RU Footprint
- Flexible 10Gb/40Gb Modes for 40Gb Ports
- Standard GigaVUE-OS CLI and H-VUE GUI
- Cluster with GigaVUE H Series and GigaVUE TA Series Nodes



GigaVUE-TA10	<ul style="list-style-type: none"> • 1RU Footprint • Flexible 10Gb/40Gb Modes for 40Gb Ports • Standard GigaVUE-OS CLI and H-VUE GUI • Cluster with GigaVUE H Series and GigaVUE TA Series Nodes 	
GigaVUE-TA40	<ul style="list-style-type: none"> • 1RU Footprint • Flexible 10Gb/40Gb Modes for 40Gb Ports • Standard GigaVUE-OS CLI and H-VUE GUI • Cluster with GigaVUE H Series and GigaVUE TA Series Nodes 	
GigaVUE-TA100	<ul style="list-style-type: none"> • 1RU Footprint • 32 x 100Gb/40Gb Ports • Standard GigaVUE-OS CLI and H-VUE GUI • Cluster with GigaVUE H Series and GigaVUE TA Series Nodes 	
GigaVUE-TA100 CXP	<ul style="list-style-type: none"> • 1RU Footprint • 20 100Gb CXP Ports, 8 100Gb QSFP28 Ports • Standard GigaVUE-OS CLI and H-VUE GUI 	
GigaVUE-TA200	<ul style="list-style-type: none"> • 2RU Footprint • 64x 100Gb/40Gb Ports • Standard GigaVUE-OS CLI and H-VUE GUI • Cluster with GigaVUE H Series and GigaVUE TA Series Nodes 	
Certified Traffic Aggregation White Box	<ul style="list-style-type: none"> • 1RU Footprint • 10Gb/40Gb Ports • Standard GigaVUE-OS CLI and H-VUE GUI • Cluster with GigaVUE H Series and GigaVUE TA Series Nodes 	

Notes on TA Series Nodes

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

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

GigaVUE H Series Features and Benefits

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

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

Any Packet, Any Destination

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

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

The Gigamon Visibility Platform

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

The Visibility Platform addresses many common network management issues, including security, compliance, forensics review, application performance, and VoIP QoS, among others. Once data is acquired from multiple SPAN ports or TAPs, it can be

multicast to multiple tools, aggregated to a few consolidated tools, and filtered or divided across many instances of the same tools.

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



Figure 1-1: The Gigamon Visibility Platform

Features and Benefits

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

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

Benefit	Descriptions
CLI Management	Configure the operations of the GigaVUE H Series node using a command-line interface, the GigaVUE-OS: <ul style="list-style-type: none"> • Local access over the serial console port on control card. • Remote network access using Telnet or 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 H Series node evolves with network speeds, including line cards with 40Gb and 100Gb support for data centers and service providers.
Cluster Support	Connect multiple GigaVUE H Series nodes in a self-healing, intelligent cluster. When you create a cluster of GigaVUE H Series nodes, available ports appear as a unified fabric, with ingress ports able to send packets to any egress port, regardless of its physical chassis. Nodes are connected through stack links consisting of one or more 10Gb, 40Gb, or 100Gb ports. Cluster management traffic can be carried out-of-band on its own network or inband on stack links.
Share SPAN Ports	Connect a SPAN port to a network port on the GigaVUE H Series node and multicast that traffic to multiple different tool ports, giving multiple different tools access to the same data. Use flow mapping to send specific traffic to different tool ports, ensuring that each tool sees the data that best suits its individual strengths. You can move, add, and reconfigure tools at will without affecting production networks.
Aggregate Links	Send the data from multiple different network ports to one or more tool ports, allowing you to combine traffic from multiple access points into a single stream for analysis.
Flow Mapping	The GigaVUE H Series Flow Mapping features let you direct traffic arriving on network ports to one or more tool ports based on different packet criteria, including VLAN IDs, IP addresses, port ranges, protocols, bit patterns, and so on. You can drop some traffic intentionally using drop rules and also create a shared-collector destination for any packets not matching the maps configured on a shared set of network ports.
GigaVUE-FM Support	Deploy Gigamon's umbrella fabric management system, GigaVUE-FM to manage all of your GigaVUE H Series, GigaVUE TA Series, and G Series nodes. The GigaVUE H Series is fully compatible with GigaVUE-FM, allowing you to centralize deployment of images, configuration backups, and alert management.
Role-Based Access	Role-based access makes it easy to share the Gigamon Visibility Platform between different groups of users with different needs. Administrators can assign egress ports to different groups of users. Users can then select the traffic they need to see from shared ingress ports. Administrators adjust map priority to ensure that each packet is delivered to the correct destination.
Cisco-Style CLI	The GigaVUE H Series node's CLI offers a similar style to the familiar Cisco interface, minimizing relearning for IT professionals.
Command Abbreviation	Type only as many letters of a command as are needed to positively differentiate from other available commands. For example, you only need to type co t to enter Configure mode, not the full configure terminal command (although that works, too!).
SNMP Support	Rely on secure SNMP v3 access to the onboard SNMP agent as well as v1/v2 SNMP traps.
Email Notifications	Use email alerts for proactive notification of a wide variety of GigaVUE events, helping you keep tabs on system status in real time.

Benefit	Descriptions
Modularized Design	Hot-pluggable line cards, power supplies, and fan trays allow for flexibility and future growth. The HD line cards are interchangeable between the GigaVUE-HD8 and GigaVUE-HD4 nodes. For GigaVUE-HC1, GigaVUE-HC2, and GigaVUE-HC3, the modules are interchangeable between the front bays of each chassis type, but not with each other, due to form and factor.
Flexible 10Gb/1Gb Support	All 10Gb ports in GigaVUE H Series line cards can be used with 1Gb Ethernet media by inserting a copper or optical SX/LX SFP instead of an SFP+. Interoperability and support are ensured by purchasing SFPs from Gigamon – transceivers purchased from other vendors are not supported.

2 Navigating H-VUE

H-VUE displays the Navigation panel and the **Overview** page when you first log in as shown in [Figure 2-1](#).

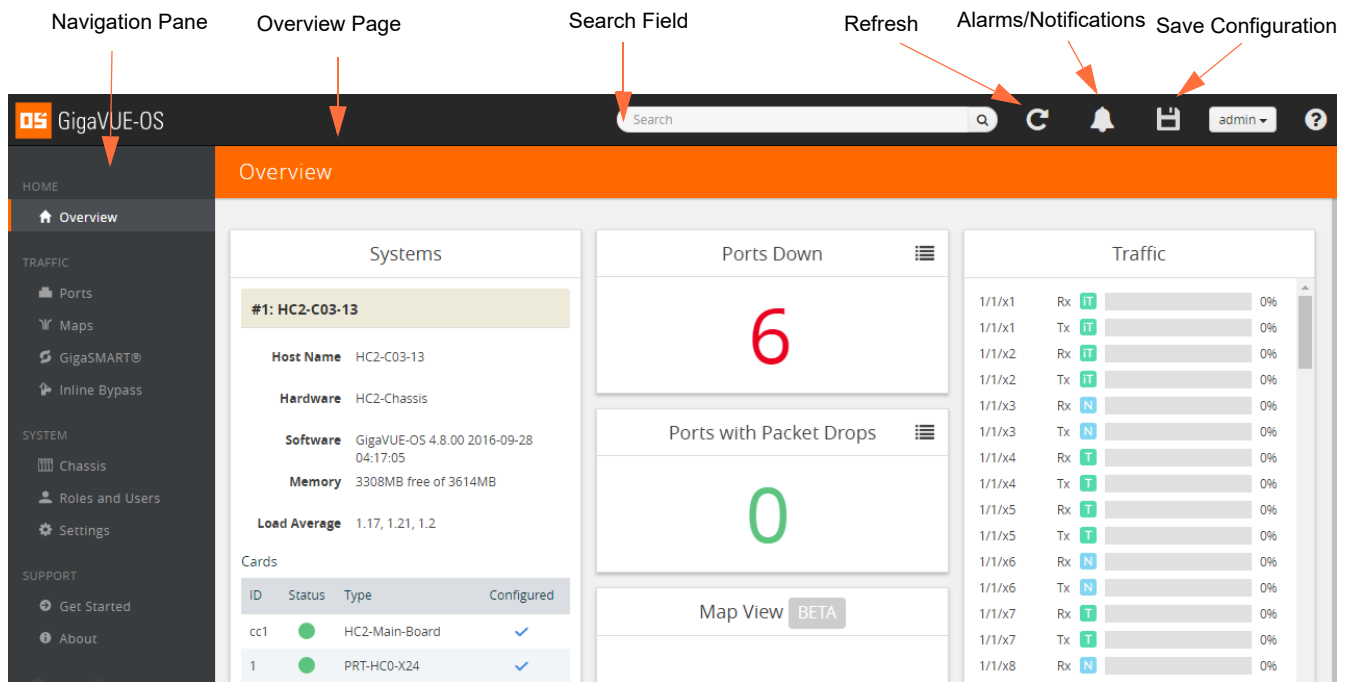


Figure 2-1: Main Navigation Panel and Overview Page

The header at the top of the page has the following features:

- Use the search field to find items within GigaVUE-OS H-VUE quickly, such as particular port or map. For more information about the search feature, refer to [Using Search](#) on page 28.
- Click the Refresh button to update the current page.
- Click the Alarms/Notification button to view a list of the current notifications or alarms. If there are any alarms/notifications, the current number of items displays next to the button.
- Click the Save Configuration button to save any current changes made to a node's configuration.
- Click the Help button to open the online documentation for H-VUE.

The Navigation panel provides links to various first level pages and fall into four categories. This chapter describes the Navigation links in the following sections:

- [Home](#) on page 20
- [Traffic](#) on page 21
- [System](#) on page 24
- [Support](#) on page 27

Also, on each page, you can open a Quickview. For more information about Quickviews, refer to [Quick View](#) on page 27.

Home

Home navigation links provide a link to the **Overview** page.

Overview

The Overview page shows panes that provide a quick visual overview of data for System, Ports Down, Over-Utilized Ports, Packets Dropped, Traffic, and a Map View. [Figure 2-2](#) shows an example of the Overview page.

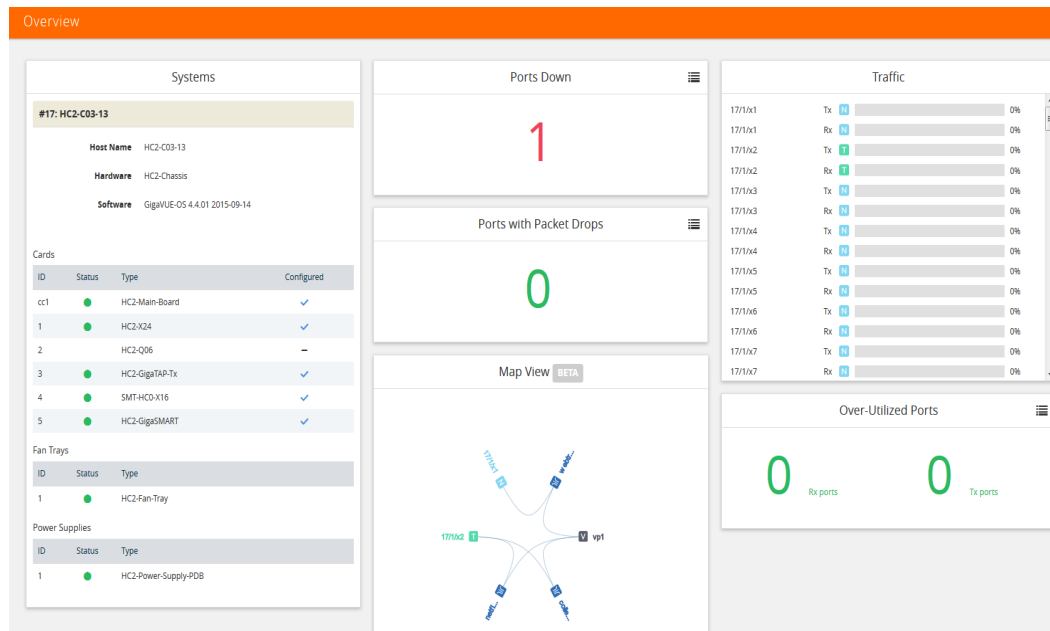


Figure 2-2: Overview Page

The Overview page displays the following widgets:

Widget	Description
Systems	The Systems widget displays general information about the specific node that you selected. This pane gives you a quick status if any issues are present in any of the nodes through the color indicators

Widget	Description
Ports Down	The Ports Down widget displays the current number of ports that are down.
Ports with Packet Drops	The Ports with Packet Drops widget displays the current number of ports with dropped packets.
Traffic	The Traffic widget displays the current utilization of each port as a bar and a percentage value for the transmit (Tx) and receive (Rx) traffic on each port.
Over-Utilized Ports	The Over-Utilized Ports widget displays the current number of receive (Rx) and transmit (Tx) ports that are experiencing over utilization.

Traffic

Traffic navigation links take you to pages for ports, maps, and GigaSMART. The following sections list the pages and navigation paths to get traffic information:

- [Ports](#) on page 21
- [Maps](#) on page 22
- [GigaSMART](#) on page 22
- [Inline Bypass](#) on page 23
- [Active Visibility](#) on page 23

Ports

The following table lists the pages you can navigate to with the **Ports** link in the Navigation panel:

Page	Navigation Path
All Ports (default)	Ports > All Ports
Port Discovery	Ports > Ports Discovery
Statistics	Ports > Statistics
Port Groups	Port Groups > All Port Groups
GigaStream	Port Groups > GigaStream
Statistics	Port Groups > Statistics
Tunnel Ports	Tunnel Ports > Tunnel Ports
Tunnel Endpoints	Tunnel Ports > Tunnel Endpoints
Statistics	Tunnel Ports > Statistics
Port Pairs	Ports > Port Pairs
Tool Mirrors	Ports > Tool Mirrors
Stack Links	Ports > Stack Links

Maps

The following table lists the pages you can navigate to with the **Maps** link in the Navigation panel:

Page	Navigation Path
Maps	Maps > Maps
Map Groups	Maps > Map Groups
Statistics	Maps > Statistics
Map Templates	Maps > Map Templates
Filter Templates	Maps > Filter Templates

GigaSMART

The following table lists the pages that you can access when you select **GigaSMART** in the Navigation panel.

Page	Navigation Path
GigaSMART Operations (GSOP)	GigaSMART > GigaSMART Operations (GSOP) > GigaSMART Operation
Statistics	GigaSMART > GigaSMART Operations (GSOP) > Statistics
GigaSMART Groups	GigaSMART > GigaSMART Groups
Statistics	GigaSMART > GigaSMART Groups > Statistics
Report	GigaSMART > GigaSMART Groups > Report
Virtual Ports	GigaSMART > Virtual Ports
Statistics	GigaSMART > Virtual Ports > Statistics
Records	GigaSMART > Netflow / IPFIX Generation > Records
Exporters	GigaSMART > Netflow / IPFIX Generation > Exporters
Monitors	GigaSMART > Netflow / IPFIX Generation > Monitors
Exporter Statistics	GigaSMART > Netflow / IPFIX Generation > Exporter Statistics
Monitor Statistics	GigaSMART > Netflow / IPFIX Generation > Monitor Statistics
SSL Profiles	GigaSMART > Inline SSL > SSL Profiles
Key Store	GigaSMART > Inline SSL > Key Store
Signing CA	GigaSMART > Inline SSL > Signing CA
Trust Store	GigaSMART > Inline SSL > Trust Store
Global Defaults	GigaSMART > Inline SSL > Global Defaults
Network Access	GigaSMART > Inline SSL > Network Access
Cache Persistence	GigaSMART > Inline SSL > Cache Persistence
Session Statistics	GigaSMART > Inline SSL > Session Statistics

Page	Navigation Path
Key Store	GigaSMART > Passive SSL > Key Store
SSL Services	GigaSMART > Passive SSL > SSL Services
Application Session Filtering	GigaSMART > Application Session Filtering
Whitelist	GigaSMART > Whitelist

Inline Bypass

The following table lists the pages you can navigate to with the **Inline Bypass** link in the Navigation panel.

Page	Navigation Path
Inline Networks	Inline Bypass > Inline Networks
Inline Network Groups	Inline Bypass > Inline Network Groups
Inline Tools	Inline Bypass > Inline Tools
Inline Tool Groups	Inline Bypass > Inline Tool Groups
Inline Serial Tools	Inline Bypass > Inline Serial Tools
Heartbeats	Inline Bypass > Heartbeats
Statistics	Inline Bypass > Heartbeats > Statistics
Redundancies	Inline Bypass > Redundancies

Active Visibility

The following table lists the pages you can navigate to with the **Active Visibility** link in the Navigation panel.

Page	Navigation Path
Policies	Active Visibility > Policies
Conditions	Active Visibility > Conditions
Actions	Active Visibility > Actions

System

The **System** navigation links take you to pages for the chassis, roles and users, and system settings. The following sections list the pages and navigation paths to get system information:

- [Chassis](#) on page 24
- [Roles and Users](#) on page 25
- [Settings](#) on page 25

Chassis

The **Chassis** navigation link provide access to the **Chassis** page. You can open different views of the chassis by clicking either the Chassis View button to display the Chassis View shown in [Figure 2-3](#) or the Table View button to display the Table View.



Figure 2-3: Chassis View Page

The following are brief descriptions of the different views. For more details information refer to [Chassis](#) on page 133.

- **Chassis View**

When you click the Chassis View button, the page shows the node. Placing the pointer over a component in the graphic displays information about that component, such as a slot or a fan tray. When the Chassis View is active, the following buttons are available:

- **Ports**

When selected, the page shows the port locations and types on the node.

- **Transceiver**

When select, the page shows the node with all line card and module LEDs displayed.

- Table View

When you click the Table View button, the page shows information about the chassis in table format. Clicking on the title bar of the tables collapses and expands the table rows. In Table View, you have the following options:

- **Actions**—in Table View, you can select a card to by clicking the check box next to the card, which enables the Actions menu for changing the configuration of the chassis or cards installed in the chassis. For details, refer to [Chassis](#) on page 133.
- **Change Port Mode**—Sets the port breakout mode on certain node models and line cards. For details, refer to [Chassis](#) on page 133.
- **Enable Fabric Hash**—Enable Fabric Hash option is used to enable advanced fabric hashing for improving packet distribution on PRT-H00-Q02X32 and PRT-HD0-Q08 line cards. For example, if traffic comes into two PRT-HD0-Q08 line cards and then is sent out to four GigaSMART engines on two GigaSMART cards, configuring advanced fabric hashing on both the PRT-HD0-Q08 line cards improves GigaSMART performance.

Roles and Users

The following tables lists the pages that you can access when you select **Roles and Users** in the Navigation panel.

Page	Navigation Path
Roles	Roles > Roles
Users	Roles > Users

Settings

The following tables lists the pages that you can access when you select **Settings** in the Navigation panel.

Page	Navigation Path
Date and Time	Settings > Data and Time
NTP	Settings > Date and Time > NTP
NTP Keys	Settings > Date and Time > NTP Keys
PTP	Settings > Date and Time > PTP
Timestamp	Settings > Date and Time > Timestamp
Security	Settings > Global Settings > Security
Web	Settings > Global Settings > Web
SNMP	Settings > Global Settings > SNMP
SNMP v3 Users	Settings > Global Settings > SNMP v3 Users
SNMP Traps	Settings > Global Settings > SNMP Traps

Page	Navigation Path
SSH	Settings > Global Settings > SSH
TELNET	Settings > Global Settings > TELNET
Hostname	Settings > Global Settings > Hostname
Logging	Settings > Global Settings > Logging
Email Notifications	Settings > Global Settings > Email Notifications
Debug	Settings > Global Settings > Debug
AAA	Settings > Authentication > AAA
RADIUS	Settings > Authentication > RADIUS
TACACS+	Settings > Authentication > TACACS+
LDAP	Settings > Authentication > LDAP
Interface	Settings > Interface > Interface
DNS	Settings > Interface > DNS
Configurations	Settings > Config and Licenses > Configurations
Licenses	Settings > Config and Licenses > Licenses
Reboot	Settings > Reboot and Upgrade > Reboot Reboot—Reboots the system. Shutdown—Shuts down the system.
Images	Settings > Reboot and Upgrade > Images
PLD and Uboot	Settings > Reboot and Upgrade > PLD and Uboot

Support

The **Support** navigation links provide take you to the following support information.

- [Getting Started](#) on page 27
- [Help Topics](#) on page 27
- [About](#) on page 27

Getting Started

Starts a short animation that provides an overview of the features in H-VUE.

Help Topics

Opens a page with links to various help topics.

About

The About page provides basic information about H-VUE.

Quick View

A Quick View provides a quick overview information when clicking on an item on a page. For example, [Figure 2-4](#) shows the Quickview for port 1/1/x1 when it is select on the **Ports** page. Also, you can close the Quickview or expand it as indicated in [Figure 2-4](#).

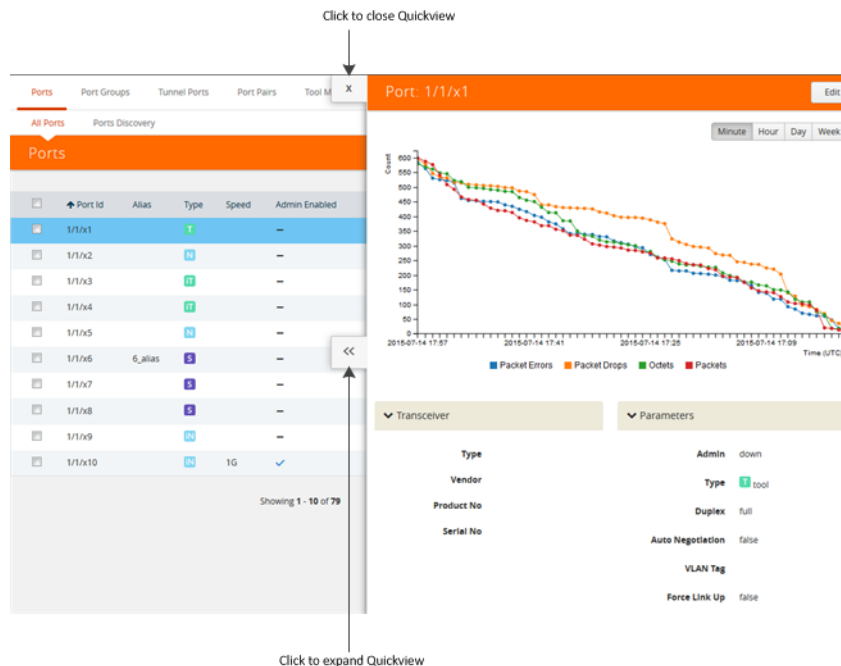


Figure 2-4: A Port Quickview

Table View Customization

GigaVUE-FM enables you to customize the appearance of table views, such as those found on Physical Nodes, Alarms/Events, Ports, Fabric Statistics, and Maps. In these pages, you can choose the columns you want to show and hide in the table. You can also choose the order in which you want to view the columns in the table.

The customized column settings are preserved for the user profile. When you log out and log back in, the tables display the same customized columns.

To select the columns to show or hide, click the table menu icon on the top left edge of the table.

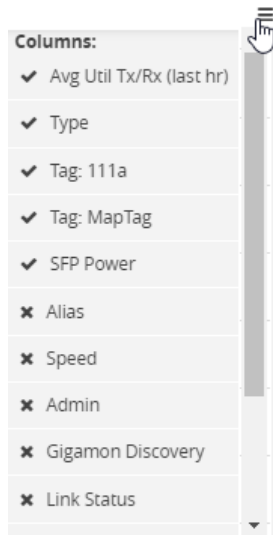


Figure 2-5: Table menu to configure columns

Click on a column to change the show/hide setting. A check mark indicates the columns to show and an X indicates the columns to hide. To rearrange the columns in the table, select a column heading and drag it to the new location. Your customizations are automatically saved.

Tables have scroll bars on the left to scroll through long lists of data or at the base to scroll through columns that extend past the window. Each page can show up to 100 rows of data per view. To navigate between multiple pages, use the arrows at the lower left edge of the table.



Figure 2-6: Table page navigation

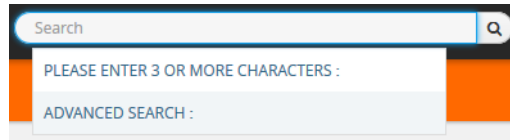
Using Search

A Search is available from the main title bar in H-VUE. Search makes it possible to quickly find a specific, such as a particular port or map, instead of using the Navigation panel links.

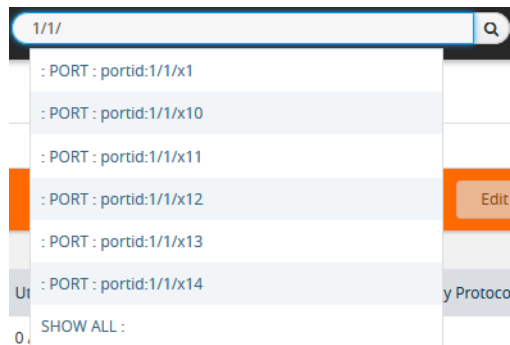
Searching

To search for an item, do the following:

1. Click in the Search field.



2. Enter the item that you want to find. For example port 1/1/x9. As you enter text, H-VUE shows a list of possible choices as shown in the following figure.



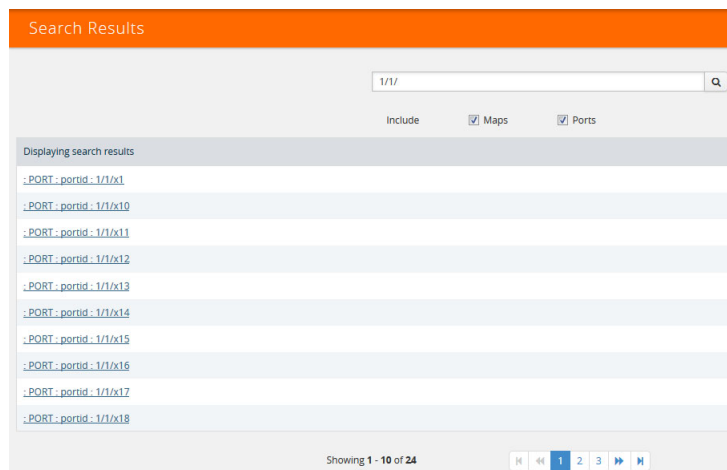
3. Select an item from the list, select **SHOW ALL**, or complete your entry.

If you select an item from the list, the page for that item displays.

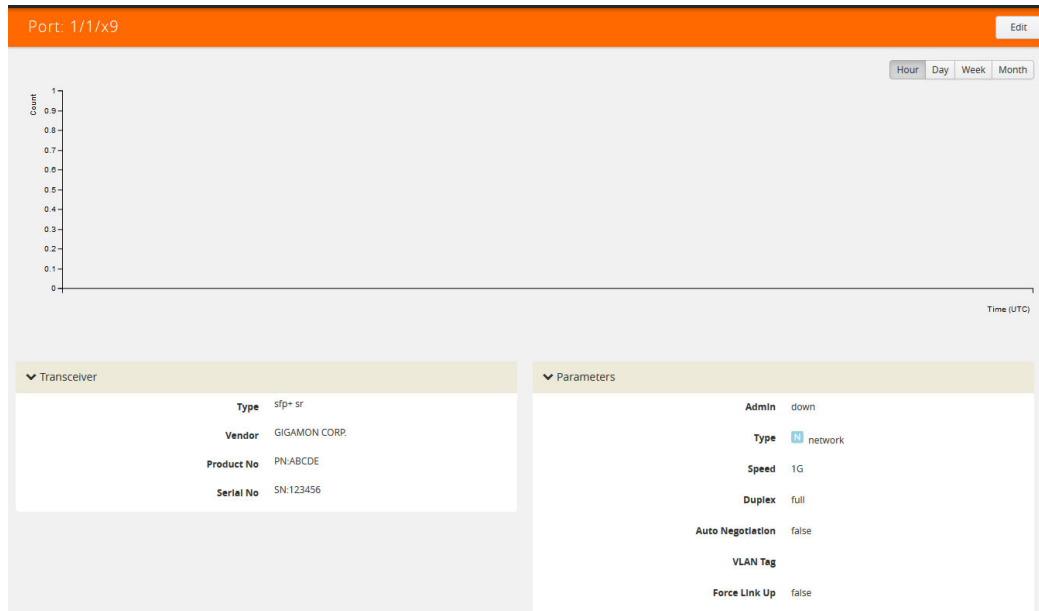
If you complete your entry, a single search result displays as shown in the following figure.



If you select SHOW ALL, a Search Results page displays.



4. Select the search result. The relevant page displays. For example, the Port page for port 1/1/x9 as shown in the following figure.



Advanced Searching

When you start typing in the Search field, an **ADVANCED SEARCH** option displays, which takes you to the **Search Results** page shown in [Figure 2-7](#).

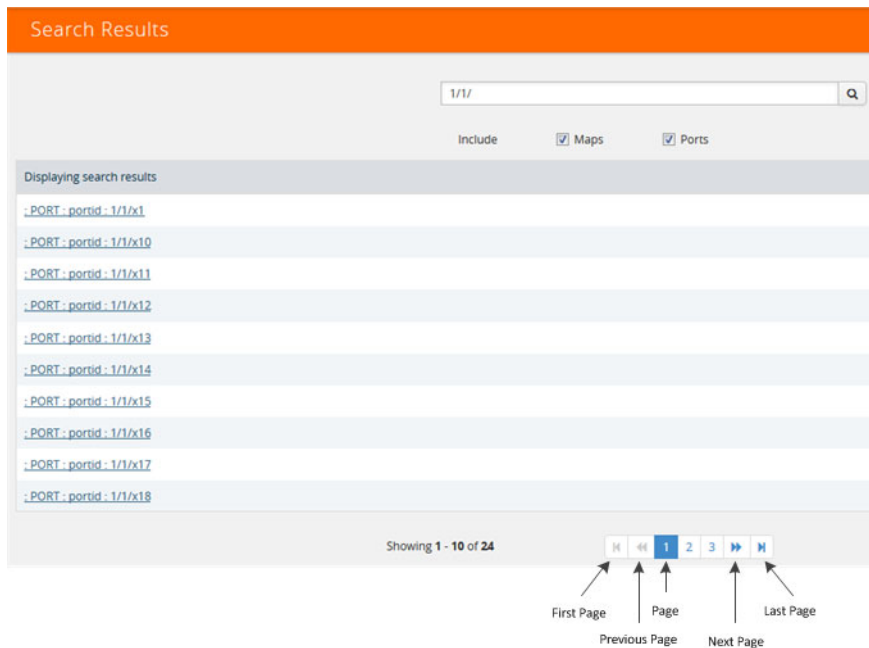


Figure 2-7: Search Results Page

On the Search Results page, you can do the following:

- Click a link under **Displaying search results**.
- Include or exclude maps in the results by selecting or clearing the **Maps** check box, respectively.

- Include or exclude ports in the results by selecting or clearing the **Ports** check box, respectively.
- Use the page controls at the bottom of the page to see additional search results.

3 Accessing H-VUE From GigaVUE-FM

You can access H-VUE from within GigaVUE-FM, by accessing a device that has been added to FM from the GigaVUE-FM interface.

To access H-VUE from the GigaVUE-FM interface:

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

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

Refer to:

- [Chassis](#) on page 133 for a detailed snapshot of a selected GigaVUE node.
- [Managing Roles and Users](#) on page 149 to manage roles and users in H-VUE and to assign access permissions.
- [Reboot and Upgrade Options](#) on page 157 to upload and upgrade images on the GigaVUE node.
- [Backup and Restore](#) on page 167 to learn how to back up and restore the configuration of the GigaVUE node.
- [Using SNMP](#) on page 173 to learn how to use the SNMP features on the GigaVUE node.

4 GigaVUE H-VUE Overview

When you login to GigaVUE-OS H-VUE, the Overview page is displayed by default. You can return to the page by selecting **Overview** from Navigation pane while viewing another page.

This chapter describes each of the panes displayed on the Overview page. Refer to the following sections for details:

- [Overview Page](#) on page 36
- [Systems](#) on page 36
- [Ports Down](#) on page 38
- [Ports with Packet Drops](#) on page 38
- [Traffic](#) on page 39
- [Over-Utilized Ports](#) on page 40

NOTE: All TA Series nodes are treated as H Series nodes in H-VUE. Therefore, you will see the same information displayed for all TA Series nodes including the white boxes with GigaVUE-OS.

Overview Page

The **Overview** link is the only link in the Home section of the Navigation pane and opens the Overview page. The Overview page displays widgets that provide a quick visual overview of data for the specific H Series node. These widgets are System, Ports Down, Over-Utilized Ports, Packets Dropped, Map View, and Traffic.

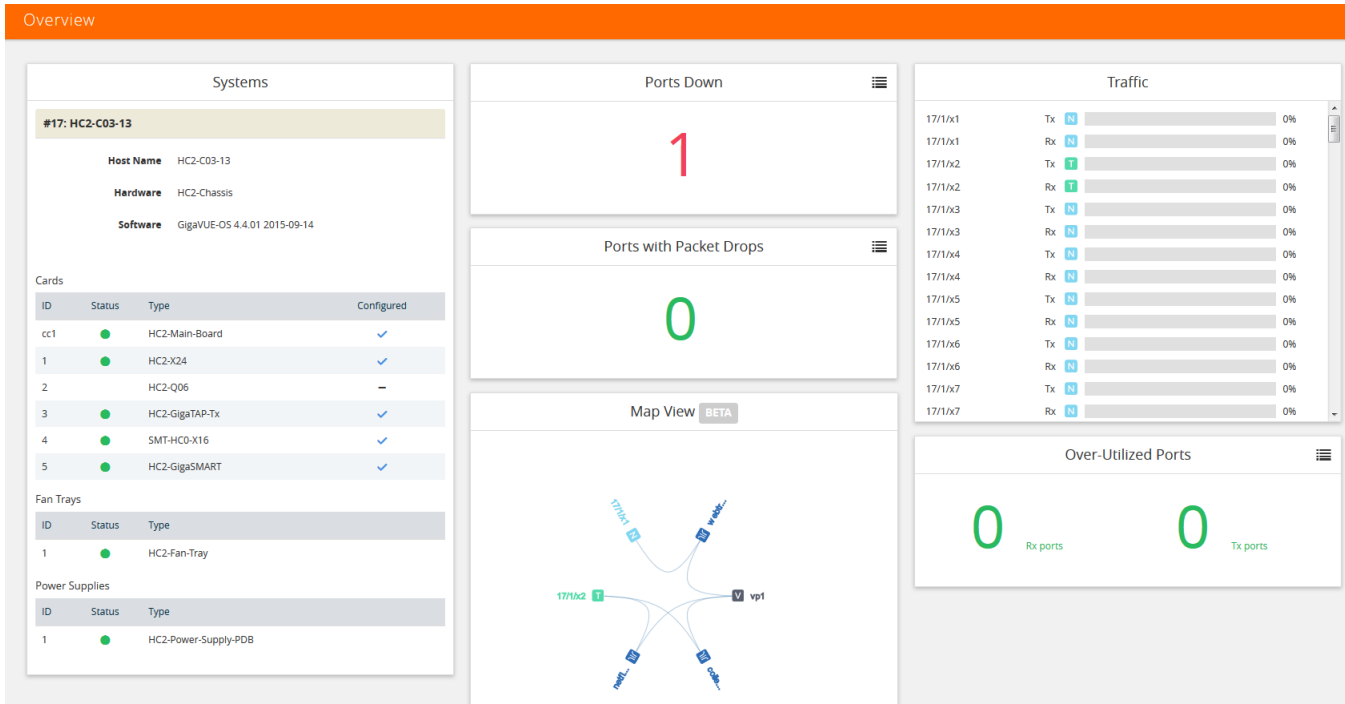


Figure 4-1: Overview Page

Systems

The **Systems** widget displays general information about the specific node that you selected. This widget gives you a quick status if any issues are present in any of the nodes through the following color indicators:

- green (running)
- amber (warning)
- red (alert)

A red alert appears for cards not present. Figure 4-2 shows an example of a Systems pane.

If node is in Safe or Limited mode, the **Systems** widget displays a banner, indicating that it is in Safe for Limited mod. For details, refer to [Cluster Safe and Limited Modes](#) on page 69.

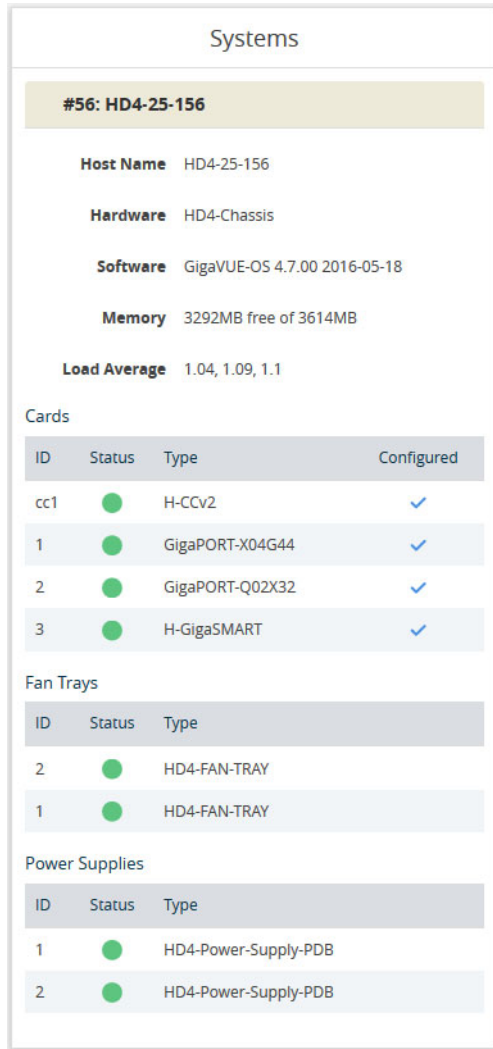


Figure 4-2: Systems Pane

Table 4-1 describes all the data points of the node displayed on the System widget.

Table 4-1: Parameters Highlighted in System Pane

Field	Description
Host Name	The host name of the box.
Hardware	The hardware type, (i.e., GigaVUE-HD8 or GigaVUE-TA1).
Software	The version of the software running on the node.
Memory	Shows the amount of used and free memory.
Load Average	The average load on the system over the last 1 minute, 5 minutes, and 15 minutes.
Cards	Displays all slots for the specific hardware type including its slot number and the type of card it contains or not. Note: When you hover over the card slot, the temperature is displayed.

Table 4-1: Parameters Highlighted in System Pane

Field	Description
Power Supply	Indicates that the power supply is On or Absent.
Fans	Indicates that the Fans are On or Off.

Ports Down

The Ports Down widget displays the current number of ports that are down. Clicking on the List icon in the upper right-hand corner changes to the panel from a counter to a table that lists the down ports and their aliases. Click the Arrow icon to return the panel to a counter. The different views are shown in [Figure 4-3](#) and [Figure 4-4](#).

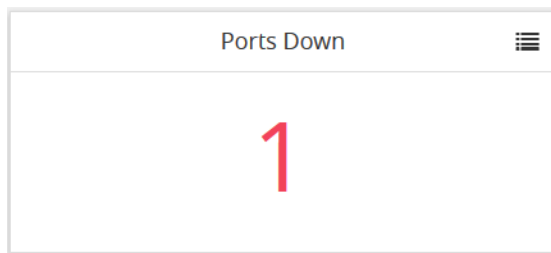


Figure 4-3: Ports Down Pane with Counter

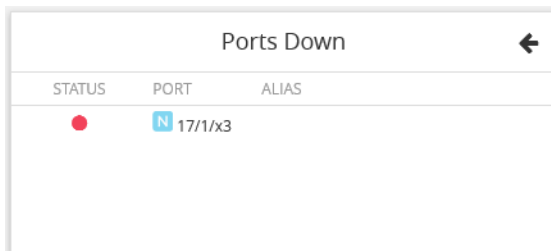


Figure 4-4: Ports Down Pane with Table

Ports with Packet Drops

The Ports with Packet Drops widget displays the current number of ports with dropped packets. Clicking on the List icon in the upper right-hand corner changes to the panel from a counter to a table that lists each ports and shows the number of packets dropped on that port. Click the Arrow icon to return the panel to a counter. The different views are shown in [Figure 4-4](#) and [Figure 4-5](#).

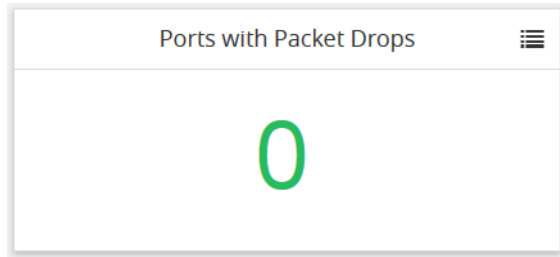


Figure 4-5: Packet Drops Counter

A rectangular widget with a white background and a light gray border. At the top, the text "Packet Drops" is centered, followed by a back arrow icon on the right. Below the title is a table with three columns: "STATUS", "PORT", and "PACKET DROPS". The table body contains a single row with the text "No packets dropped." centered across all three columns.

STATUS	PORT	PACKET DROPS
No packets dropped.		

Figure 4-6: Packet Drops Table

Traffic

The Traffic widget displays up to 20 of the most-utilized ports. The ports are ordered by traffic count. Each displayed port is labeled with its location, whether it is a transmitting or receiving port, and its percentage of utilization. [Figure 4-7](#) shows an example of the Traffic pane.

NOTE: The Traffic pane is view-only. It reflects traffic activity with port ID at the time of discovery and does not immediately refresh.

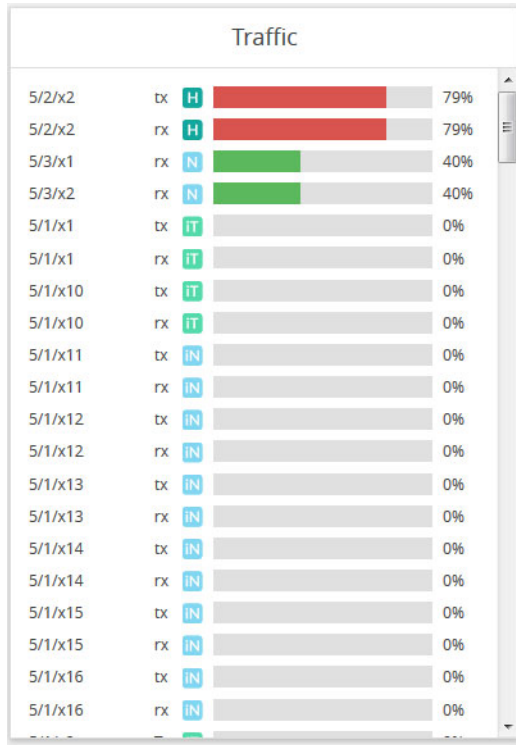


Figure 4-7: Traffic View Pane

Over-Utilized Ports

The Over-Utilized Ports widget displays the current number of receive (Rx) and transmit (Tx) ports that are experiencing over utilization. Click on the List icon in the upper right-hand corner to change the panel to a table that lists each over utilized port with its status, type, and alias.

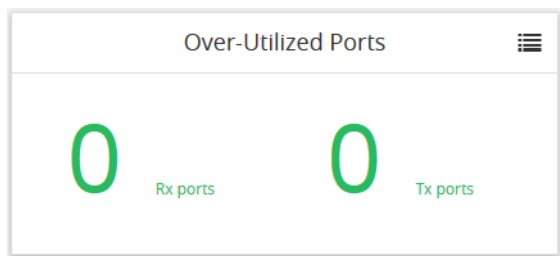


Figure 4-8: Over-Utilized Ports Counter

Over-Utilized Ports			
STATUS	PORT	TYPE	ALIAS
No over-utilized ports.			

Figure 4-9: Over-Utilized Ports Table

Traffic Pages

The Traffic section of the Navigation pane provides links to pages for creating and configuring the following:

- Ports
- Maps
- GigaSMART
- Inline Bypass

Ports

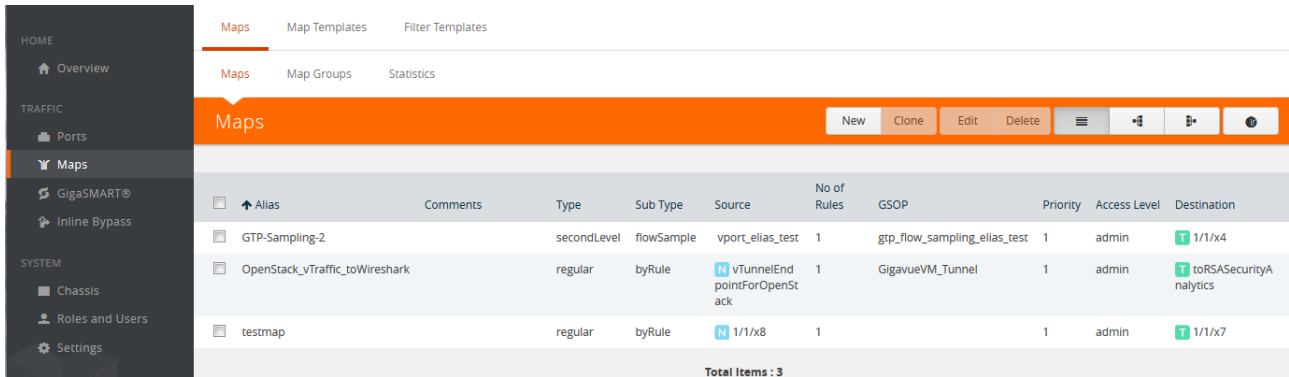
When you select **Ports** from the Navigation pane the default ports page displayed is the **All Ports** page shown in Figure 4-10. Other pages that you can access are Port Groups, Tunnel Ports, Port Pairs, Tool Mirrors, and Stack Links.

Port Id	Alias	Type	Speed	Admin Enabled	Link Status	Transceiver Type	Utilization (Tx/Rx)	Port Filter	Discovery Protocol
1/1/x1	ColaSoft_Dedicated_Link_ESX12	1G	1G	✓	up	sfp cu	0 / 0	—	Off
1/1/x2	WireShark_Dedicated_Link_ESX12	1G	1G	✓	up	sfp cu	0 / 0	—	Off
1/1/x3	TunnelPort_From_ESX12	1G	1G	✓	up	sfp cu	0 / 0	—	Off
1/1/x4		1G	1G	—	down		0 / 0	—	Off
1/1/x5	RSA_Decoder_Dedicated_NIC	10G	10G	✓	down	sfp+ sr	0 / 0	—	Off
1/1/x6	GigamonITFeed_TA01_to_HD4TME_to_HC2TME	10G	10G	✓	up	sfp+ sr	0 / 0	—	Off
1/1/x7		1G	1G	—	down		0 / 0	—	Off
1/1/x8		1G	1G	—	down		0 / 0	—	Off
1/1/x9		1G	1G	—	down		0 / 0	—	Off

Figure 4-10: All Ports Page

Maps

When you select **Maps** from the Navigation pane the default page displayed is the **Maps** page shown in [Figure 4-11](#). The other pages that you can access are Maps Templates and Filter Templates. The Map pages are used to configure flow mapping from the H-VUE UI.



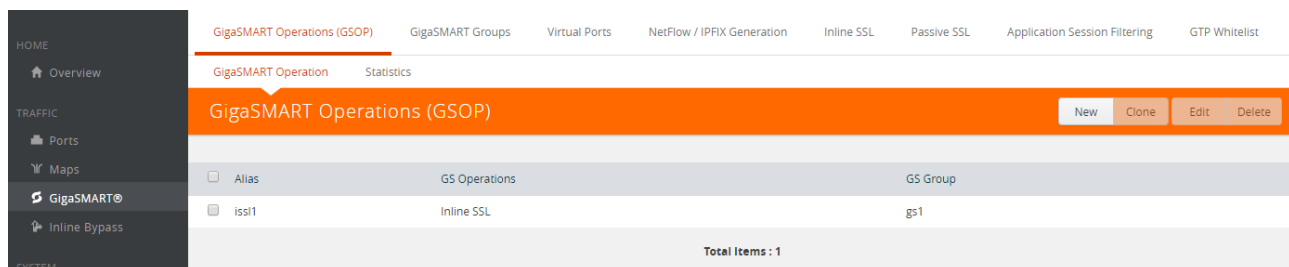
<input type="checkbox"/>	Alias	Comments	Type	Sub Type	Source	No of Rules	GSOP	Priority	Access Level	Destination
<input type="checkbox"/>	GTP-Sampling-2		secondLevel	flowSample	vport_elias_test	1	gtp_flow_sampling_elias_test	1	admin	T 1/1/x4
<input type="checkbox"/>	OpenStack_vTraffic_toWireshark		regular	byRule	N vTunnelEnd pointForOpenStack	1	GigavueVM_Tunnel	1	admin	T toRSA Security Analytics
<input type="checkbox"/>	testmap		regular	byRule	N 1/1/x8	1		1	admin	T 1/1/x7

Total Items : 3

Figure 4-11: Maps Page

GigaSMART

When you select **GigaSMART** from the Navigation pane the default page displayed is the **GigaSMART Operation** page shown in [Figure 4-12](#). GigaSMART operations are special packet modification features available for use with maps. Other pages that you can access from the GigaSMART link in the Navigation pane are GigaSMART Groups, Virtual Ports, NetFlow/IPFIX Generation, Inline SSL, Passive SSL, Application Session Filtering and GTP Whitelist.



<input type="checkbox"/>	Alias	GS Operations	GS Group
<input type="checkbox"/>	issi1	Inline SSL	gs1

Total Items : 1

Figure 4-12: GigaSMART Operation Page

Inline Bypass

When you select **Inline Bypass** from the Navigation pane the default page displayed is the **Inline Networks** page shown in [Figure 4-12](#). Other pages that you can access from the **Inline Bypass** link are Inline Network Groups, Inline Tools, Inline Tool Groups, Inline Serial Tools, Heartbeats, and Redundancies. These pages are used to create inline bypass solutions that place the Gigamon node inline between two sides of a network.

Alias	Comment	Type	Forwarding State	Link Propagation	Physical Bypass	Traffic Path
InLineNet2		protected	physicalBypass	true	enabled	Bypass
InLineNet1		protected	physicalBypass	true	enabled	Bypass
cu1		unprotected	disconnected	true	disabled	To Inline Tool
cu2		unprotected	disconnected	true	disabled	Bypass With Monitoring
inline_network_1_3_2		protected	physicalBypass	true	enabled	To Inline Tool

Total Items : 5

Figure 4-13: Inline Networks Page

System Pages

The System section of the Navigation pane provides links to pages for viewing detailed information about the physical node's chassis, managing roles and users, and configuring settings for the node. The links under System are:

- Chassis
- Roles and Users
- Settings

Chassis

The **Chassis** link opens the Chassis page shown in [Chassis View](#) on page 43. The Chassis page provides a detailed snapshot of a selected H Series node, allowing you to view cards, control cards, and ports, fan trays, and power modules on the chassis. For a detailed description of the Chassis page and views, refer to [Chassis](#) on page 133.

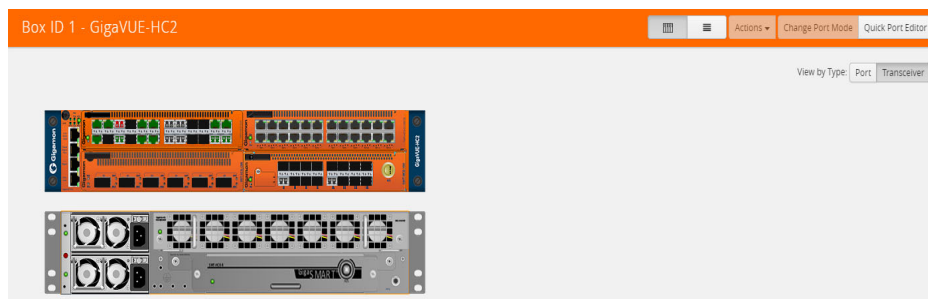


Figure 4-14: Chassis View

Roles and Users

The **Roles and Users** link provides access the Roles and User Setup pages. The Roles page shown in [Figure 4-15](#) is where you view and create the roles that can be assigned to users to control their level of access to the system.

<input type="checkbox"/>	User Group	Description
<input type="checkbox"/>	admin	--
<input type="checkbox"/>	Default	--
<input type="checkbox"/>	monitor	--

Total Items : 3

Figure 4-15: Roles Page

The User Setup page shown in [Figure 4-16](#) is where you view and create the user that have access to the system.

<input type="checkbox"/>	Full Name	Username	User Group	Enabled	Account Status
<input type="checkbox"/>	System Administrator	admin	admin	true	Password Set
<input type="checkbox"/>	System Monitor	monitor	monitor	true	No Password
<input type="checkbox"/>	System Operator	operator	--	true	Account Locked Out

Total Items : 3

Figure 4-16: User Setup Page

The Roles and User pages form the basis creating Role Based Access and Control (RBAC). For more detailed information about roles and users, refer to [Managing Roles and Users](#) on page 149.

5 Getting Started with GigaVUE H-VUE

This chapter describes the tasks you will want to do the first time you login to GigaVUE H-VUE. This chapter assumes that you have already installed, connected and configured the node as described in the GigaVUE H Series or TA Series *Hardware Installation Guide*. This includes running the jump-start script and enabling the Web server with the **web enable** command, which allows you to use H-VUE with the GigaVUE H Series node.

This chapter describes the following configuration tasks that you can complete from the CLI or from H-VUE:

- [Initial User Account Configuration \(Optional\)](#) on page 47
- [Configuring the Host Name](#) on page 55
- [Configuring Time Options](#) on page 55
- [Configuring Logging](#) on page 59
- [Configuring Automatic Email Notifications](#) on page 61
- [Using a Custom Banner](#) on page 63
- [Viewing Information About the Node](#) on page 65
- [Cluster Safe and Limited Modes](#) on page 69
- [Supported Browsers](#) on page 73
- [Configuring Internet Explorer for Use with H-VUE](#) on page 73

Logging In to GigaVUE-OS H-VUE

GigaVUE-OS H-VUE opens with the login page shown in [Figure 5-1](#). The login page provides information about the physical node beside the username and password login field. The login page shows the following information:

- The current version of GigaVUE-OS running on the node
- Hostname assigned to the node
- A login banner.

The login banner is customizable. For the steps to customize the login banner, refer to [Using a Custom Banner](#) on page 63.

For the initial login, enter the admin in the username field and the password assigned during the configuration jump-start.

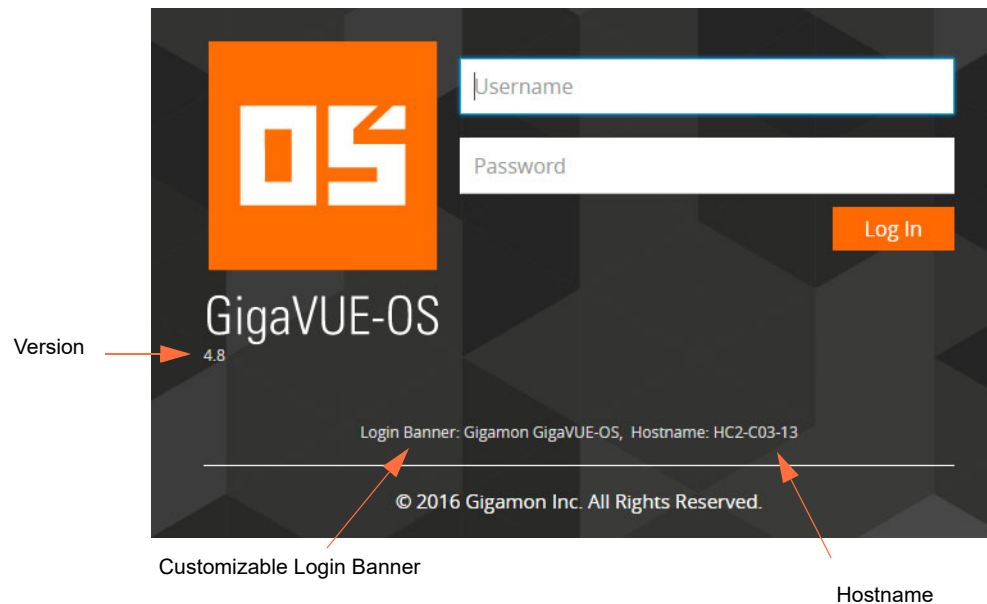


Figure 5-1: GigaVUE-OS H-VUE Login Page

Initial User Account Configuration (Optional)

Before you start mapping traffic, you must change the password for the default admin account and a few other accounts for use by different level users. You may have already used the jump-start script to change the password for the admin account.

Changing Passwords and Setting Up Basic Accounts

This section describes the steps for changing the account password for the admin and setting up some basic accounts. See also [GigaVUE-OS Password Policies](#) on page 53.

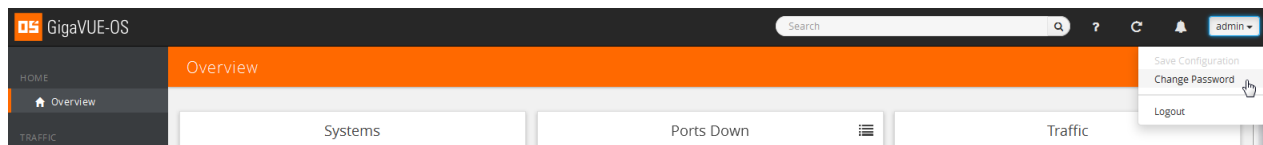
Starting in software version 4.7, the default password admin123A! is no longer allowed. If the node is upgraded to version 4.8 and above through the **configuration-jumpstart** command, the password for the admin user is required to be set, which will be the password when the admin user logs into H-VUE after the upgrade.

If the node is upgraded through GigaVUE-FM, H-VUE does require the default password to be reset. However, you should change the admin default password after upgrading to software version 4.8 and above or prior to an upgrade from GigaVUE-FM.

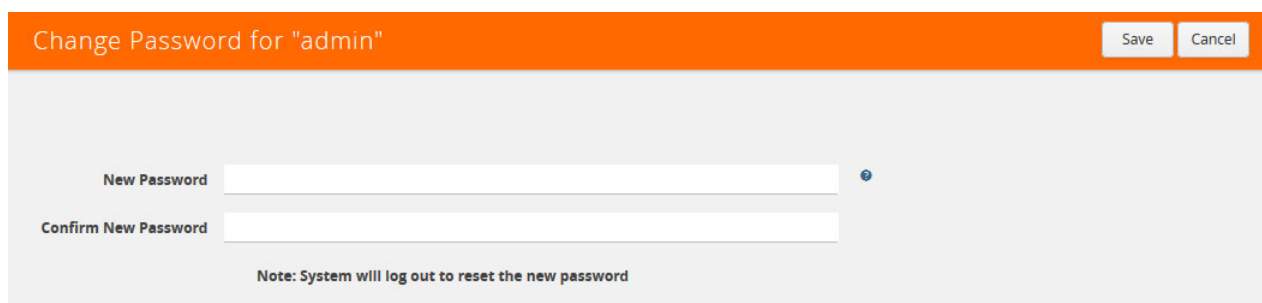
Changing the admin Account Password

To change the password for the admin account from H-VUE, do the following:

1. Click the **admin** button in the top right corner of the H-VUE UI as shown in the following figure.



2. Select **Change Password**. The Change Password page opens as shown in the following figure.

A screenshot of the "Change Password for 'admin'" page in the H-VUE UI. The page has an orange header with the title "Change Password for 'admin'" and two buttons: "Save" and "Cancel". Below the header, there are two input fields: "New Password" and "Confirm New Password". A note at the bottom of the form states: "Note: System will log out to reset the new password".

3. Enter a new password in the **New Password** field.

For a description of the password standards, refer to [GigaVUE-OS Password Policies](#) on page 53.

4. Re-enter the password in the **Confirm New Password** field.
5. Click **Save**.

The system will log out to reset the new password.

6. Log in to H-VUE with the admin user name and the new password.

Setting Up Some Basic Accounts

After resetting the admin password, you will probably want to set a few user accounts with different access levels.

The GigaVUE node has a local account database that can optionally integrate with an LDAP, RADIUS, or TACACS+ server for authentication. Any account you want to authenticate using an external AAA server must have a matching account name in the local database.

Authentication, user levels, and roles are discussed in detail in the GigaVUE-OS CLI User's Guide and in [Managing Roles and Users](#) on page 149. For now, however, it is easiest to create a few basic user account with different privilege levels. In general, user privileges are as follows:

- **Admin** users have access to all command modes, including Standard, Enable, and Configure. They also have full permissions for all network, tool, and stack ports.
- **Operator** users have access to all command modes, including Standard, Enable, and Configure. However, they only have access to the network and tool ports associated with their user group.
- **Monitor** users have access to the Standard and Enable command modes. They cannot configure packet distribution (or any other global GigaVUE node options).

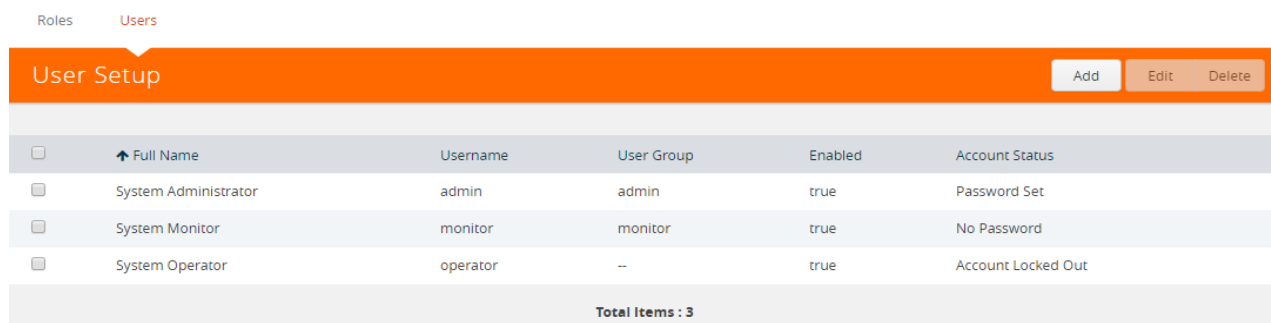
Once you have configured these basic user accounts, review your settings on the User Set Up page.

The following procedures add a new **admin** user, a new **operator** user, and a new monitor user.

Adding a New admin user

Use the following steps to create a new **admin** user:

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



<input type="checkbox"/>	Full Name	Username	User Group	Enabled	Account Status
<input type="checkbox"/>	System Administrator	admin	admin	true	Password Set
<input type="checkbox"/>	System Monitor	monitor	monitor	true	No Password
<input type="checkbox"/>	System Operator	operator	--	true	Account Locked Out

Total Items : 3

2. Click **Add**. The New User page displays.

Add New User Save Cancel

Account Details

User Name User Name

Name Name

Password Password

Confirm Password Confirm Password

User Role Select user Groups

Enabled

3. Add the account details for the new user.
 - a. Enter a user name for this account in the **User Name** field.
 - b. Enter the users actual name in the **Name** field.
 - c. Enter a password in the **Password** field.
For a description of the password standards, refer to [GigaVUE-OS Password Policies](#) on page 53.
 - d. Re-enter the password in the **Confirm Password** field.
 - e. Click in the **User Role** field and select **admin**.
 - f. Select **Enable** to enable the user’s account.
4. Click **Save**.

Adding a New operator User

Use the following steps to create a new **operator** user:

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

Roles Users

User Setup Add Edit Delete

<input type="checkbox"/>	Full Name	Username	User Group	Enabled	Account Status
<input type="checkbox"/>	System Administrator	admin	admin	true	Password Set
<input type="checkbox"/>	System Monitor	monitor	monitor	true	No Password
<input type="checkbox"/>	System Operator	operator	--	true	Account Locked Out

Total Items : 3

2. Click **Add**. The New User page displays.

The screenshot shows the 'Add New User' form. It features an orange header bar with the text 'Add New User' on the left and 'Save' and 'Cancel' buttons on the right. Below the header, the form is titled 'Account Details'. It contains several input fields: 'User Name' (with placeholder text 'User Name'), 'Name' (with placeholder text 'Name'), 'Password' (with placeholder text 'Password' and a small blue icon to its right), 'Confirm Password' (with placeholder text 'Confirm Password'), and 'User Role' (a dropdown menu with the text 'Select user Groups'). At the bottom of the form, there is an 'Enabled' checkbox which is checked.

3. Add the account details for the new user.
 - a. Enter a user name for this account in the **User Name** field.
 - b. Enter the users actual name in the **Name** field.
 - c. Enter a password in the **Password** field.
For a description of the password standards, refer to [GigaVUE-OS Password Policies](#) on page 53.
 - d. Re-enter the password in the **Confirm Password** field.
 - e. Leave the User Role field empty.
New user's are automatically created with **Default** operator level privileges, so there s no need to grant an additional role.
 - f. Select **Enable** to enable the user's account.
4. Click **Save**.

The new user with displays on the User Setup page assigned to the Default user group. In the following example, the user TME has been added and assigned to the default user group.

The screenshot shows the 'User Setup' page. It has an orange header with 'User Setup' and 'Add', 'Edit', and 'Delete' buttons. Below the header, there is a table with the following data:

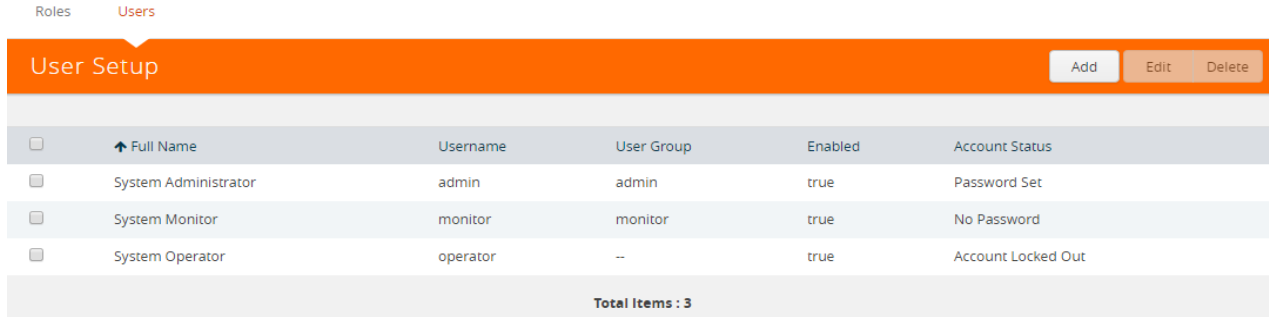
<input type="checkbox"/>	Full Name	Username	User Group	Enabled	Account Status
<input type="checkbox"/>	System Administrator	admin	admin	true	Password Set
<input type="checkbox"/>	System Monitor	monitor	monitor	true	No Password
<input type="checkbox"/>	System Operator	operator	--	true	Account Locked Out
<input type="checkbox"/>	TME	Operator-2	Default	true	Password Set

At the bottom of the table, it says 'Total Items : 4'.

Adding a New Monitor User

Use the following steps to create a new **monitor** user:

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

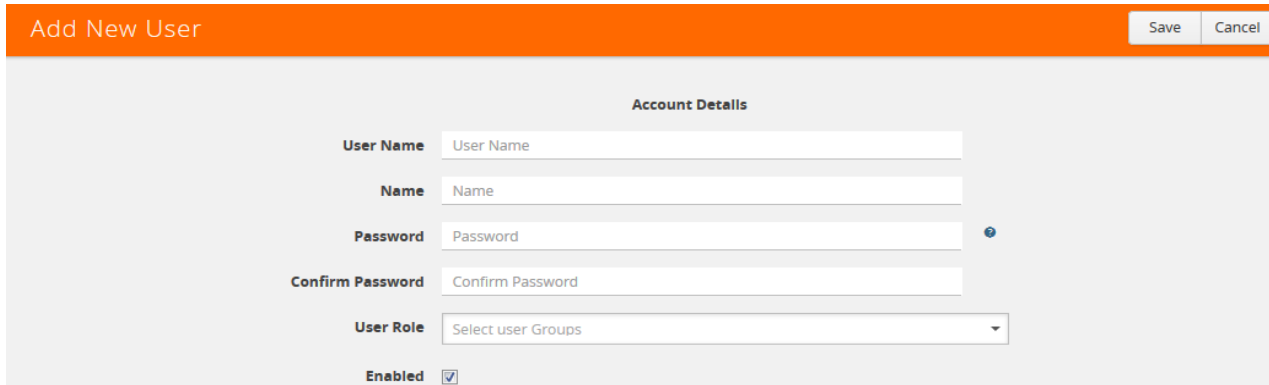


The screenshot shows the 'User Setup' page with a table of existing users. The table has columns for checkboxes, full name, username, user group, enabled status, and account status. There are three users listed: System Administrator, System Monitor, and System Operator. The System Monitor user is highlighted in blue.

<input type="checkbox"/>	↑ Full Name	Username	User Group	Enabled	Account Status
<input type="checkbox"/>	System Administrator	admin	admin	true	Password Set
<input type="checkbox"/>	System Monitor	monitor	monitor	true	No Password
<input type="checkbox"/>	System Operator	operator	--	true	Account Locked Out

Total Items : 3

2. Click **Add**. The New User page displays.



The screenshot shows the 'Add New User' page with a form for account details. The form includes fields for User Name, Name, Password, Confirm Password, User Role, and an Enabled checkbox. The User Role dropdown is set to 'Select user Groups'.

Account Details

User Name:

Name:

Password:

Confirm Password:

User Role:

Enabled:

3. Add the account details for the new user.
 - a. Enter a user name for this account in the **User Name** field.
 - b. Enter the users actual name in the **Name** field.
 - c. Enter a password in the **Password** field.
For a description of the password standards, refer to [GigaVUE-OS Password Policies](#) on page 53.
 - d. Re-enter the password in the **Confirm Password** field.
 - e. Click in the **User Role** field and select **monitor**.
 - f. Select **Enable** to enable the user's account.

4. Click **Save**.

The new user with monitor role displays on the User Setup page. In the following example, the user TME has been added and assigned to the monitor user group.

Roles **Users**

User Setup Add Edit Delete

<input type="checkbox"/>	Full Name	Username	User Group	Enabled	Account Status
<input type="checkbox"/>	System Administrator	admin	admin	true	Password Set
<input type="checkbox"/>	System Monitor	monitor	monitor	true	No Password
<input type="checkbox"/>	System Operator	operator	--	true	Account Locked Out
<input type="checkbox"/>	TME	monitor-user-1	monitor	true	Password Set

Total Items : 4

Enabling/Disabling a User Accounts

To enable an existing user account, do the following:

1. Select **Roles & Users > Users**.
2. On the User Setup page, select the user and click **Edit**.
3. Enter a new password in the **Password** field and re-enter in the Confirm **Password** field.
4. Select **Enable**.
5. Click **Save**.

After saving the user account, Account Disabled will display in the Account Status field. For information about account statuses, refer to [Account Status](#) on page 52.

To disable a existing user account, do the following:

1. Select **Roles & Users > Users**.
2. On the User Setup page, select the user and click **Edit**.
3. Enter a new password in the **Password** field and re-enter in the Confirm **Password** field.
4. Clear the **Enable** check box.
5. Click **Save**.

After saving the user account, Password Set will display in the Account Status field. For information about account statuses, refer to [Account Status](#) on page 52.

Account Status

Each user's account has status that is displayed in the Account Status column on the User Setup page. The account status can be one of the following:

- Password Set—the user's password is set and can log in.
- No Password—The user does not have a password (that is the password is blank). However, the user can still login. Only Monitor user accounts created prior to the current release may have blank passwords. Blank passwords are no longer allowed when creating a user account.
- Account Locked Out—the user's account is enabled but cannot log in.

- Account Disabled—the user’s account is has been disabled. Refer to [Enabling/Disabling a User Accounts](#) on page 52 for more information.

NOTE: A users with the Monitor role only sees the account status for their account, which is Password Set.

GigaVUE-OS Password Policies

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

Policy	Description
Password Standards	<p>Passwords must meet the following standards:</p> <ul style="list-style-type: none"> • 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)
Password Recommendations	<p>The following are password recommendations:</p> <ul style="list-style-type: none"> • 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 in length, 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 <p>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.</p>
Password Change Rights	<p>Only admin users can change the passwords of other users.</p>

Policy	Description
Password on Default admin Use	<p>Starting in software version 4.7, the password on the default admin account must be changed during initial configuration using configuration jump-start.</p> <p>If the following message is displayed, the system administrator must change the default password on the admin account:</p> <pre>ATTENTION: Admin account default password must be changed for security.</pre> <p>If the system administrator tries to change the password to the default, it will not be allowed and the following message will be displayed:</p> <pre>Default password is not allowed.</pre> <p>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:</p> <pre>Admin account password must be changed via the CLI to a non-default value for security purposes.</pre>

Resetting Password on GigaVUE Nodes

Passwords can only be reset from the CLI. For the procedures for resetting the password on GigaVUE nodes, refer to the *GigaVUE-OS CLI User's Guide*.

Password Expiry

When the password on GigaVUE nodes expires, a new password can be set using the CLI commands. For setting the password on GigaVUE nodes, refer to the *GigaVUE-OS CLI User's Guide*.

Configuring the Host Name

It is generally a good idea to configure the GigaVUE node's name, date, and time as part of your initial configuration. For information on setting options related to time and date, refer to [Configuring Time Options](#) on page 55. The Hostname is shown on the Hostname page, which is shown in [Figure 5-2](#).

To set the host name, do the following:

1. Select **Settings > Global Settings > Host Name**.
2. Click **Edit**.
3. Enter a name in the **Hostname** field.
4. Click **Save**.

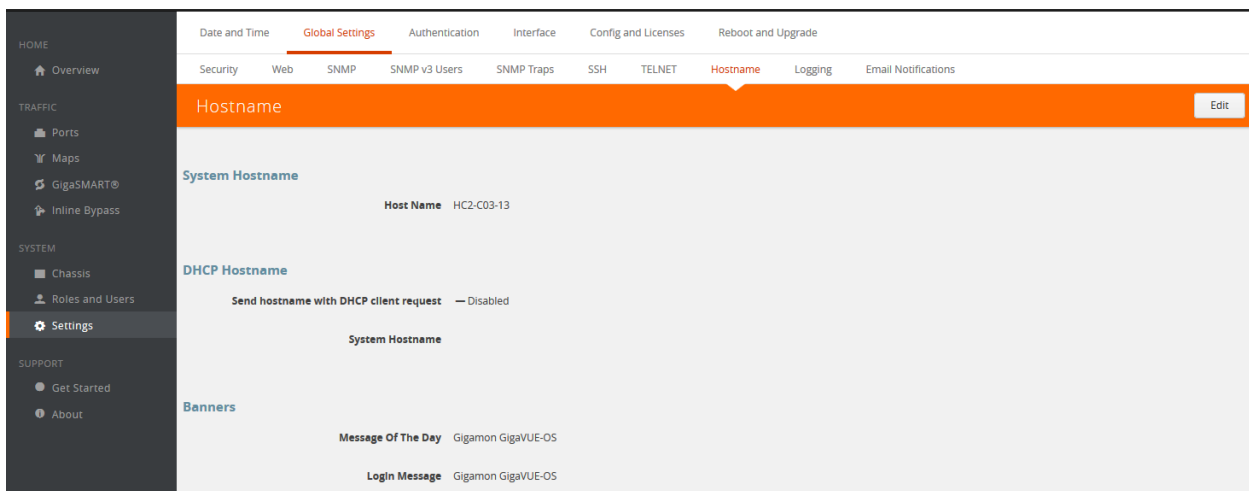


Figure 5-2: Hostname Page

Configuring Time Options

The GigaVUE node includes a variety of features for setting the time. By default, the GigaVUE H Series node is configured to use its local clock, as configured with on the Date and Time page by selecting **Settings > Date and Time**. The following table

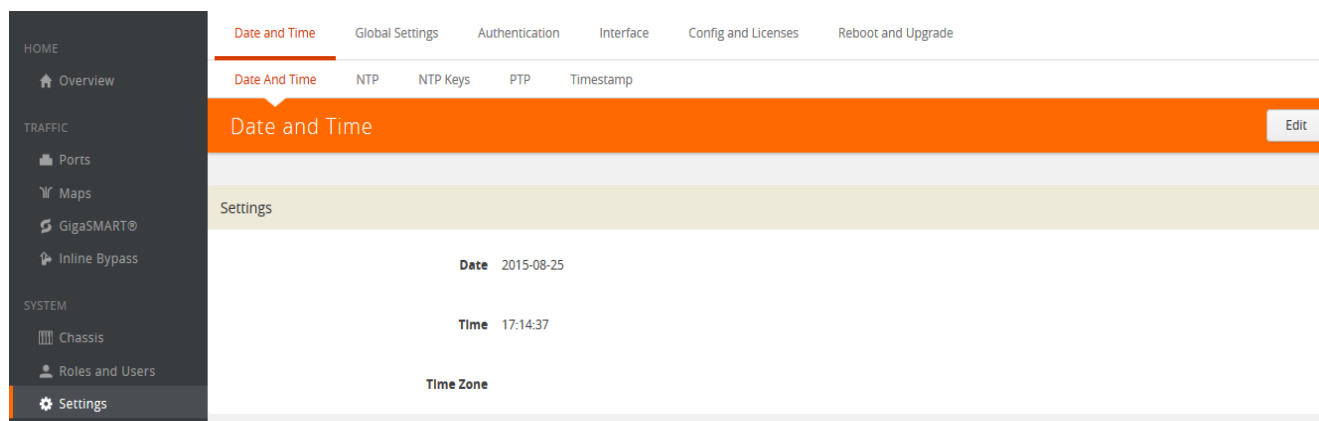
provides references to information about the various methods available for setting the time.

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

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

Setting Time Manually

The easiest way to set the GigaVUE 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. [Figure 5-3](#) shows an example where the date and time is set to May 13, 2016 at 10:07:08am for time zone America/Los Angeles. If you are using NTP, use UTC for the timezone.
4. Click **Save** to update the date and time settings.

Figure 5-3: Date, Time, and Time Zone Set

Using 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 displays.

3. Specify the address of the time server in the Server IP/Host Name field.
You can specify an IPv4, IPv6, or hostname. To use IPv6 addresses, IPv6 must be enabled through the CLI. For more information, refer to the *GigaVUE-OS CLI User's Guide*.
NOTE: There are many public NTP servers available on the Internet.
4. Select the NTP version in the **Version** field.
5. Select **Enable** to enable the server.
6. Click **Save**.

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

Performing 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 shown in [Figure 5-4](#).
3. On the Edit NTP Settings page, select **Enabled**.
4. Click **Save**.

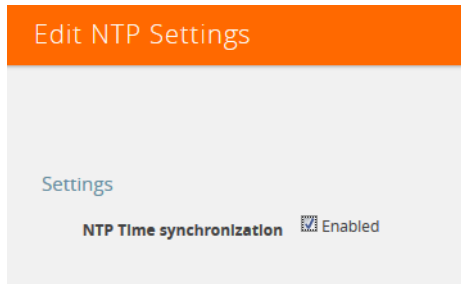


Figure 5-4: NTP Time Synchronization Enabled

Configuring Logging

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

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

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

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

For UDP, do the following:

- a. Enter the external server's IP address in the **IP Address** field.
- b. Select the logging level from the **Log Level** list. For a description of the logging levels, refer to [Table 5-1 on page 59](#).

For TCP, do the following:

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

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

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

- b. Select the logging level from the **Log Level** list. For a description of the logging levels, refer to [Table 5-1 on page 59](#).
- c. Enter the port number in the TCP Port field.

For SSH, do the following:

- a. Enter the external server's IP address in the **IP Address** field.
- b. Select the logging level from the **Log Level** list. For a description of the logging levels, refer to [Table 5-1 on page 59](#).
- c. Enter the port number in the TCP Port field.
- d. Enter the user name for logging in to the SSH server in the **Username** field.

Table 5-1: 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.

Table 5-1: Logging Levels

Log-Level	Description
error	Error conditions.
warning	Warning conditions.
notice	Normal but significant condition.
info	Informational messages.
debug	Debug-level messages. Authorized for factory use only.

External Syslog Servers and Clustered Nodes

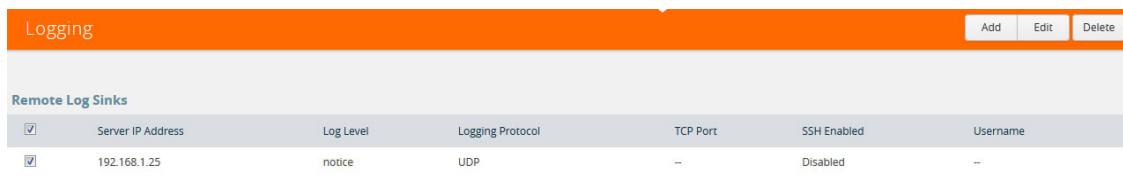
When working with clustered nodes, set up logging individually for each clustered node.

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

Deleting an External Syslog Server

Remove a logging server by doing the following:

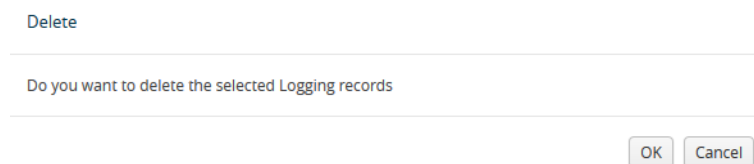
1. Select **Settings > Global Settings > Logging**.
2. Select the external server on the Logging page as shown in [Table 5-5](#)



Logging							Add	Edit	Delete	
Remote Log Sinks										
<input checked="" type="checkbox"/>	Server IP Address	Log Level	Logging Protocol	TCP Port	SSH Enabled	Username				
<input checked="" type="checkbox"/>	192.168.1.25	notice	UDP	--	Disabled	--				

Figure 5-5: Logging Server Selected for Delete

3. Click **Delete**.
4. Delete message shown in the following figure displays. Click **OK** to delete the server.



Packet Format for Syslog Output

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

Keep in mind the following about this packet format:

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

Configuring Automatic Email Notifications

The GigaVUE 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.

Configuring the Email Server Settings

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

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

The Email Notifications page (refer to [Figure 5-6](#)) shows the current server settings, the events enabled for notification, and the recipients for the notifications.

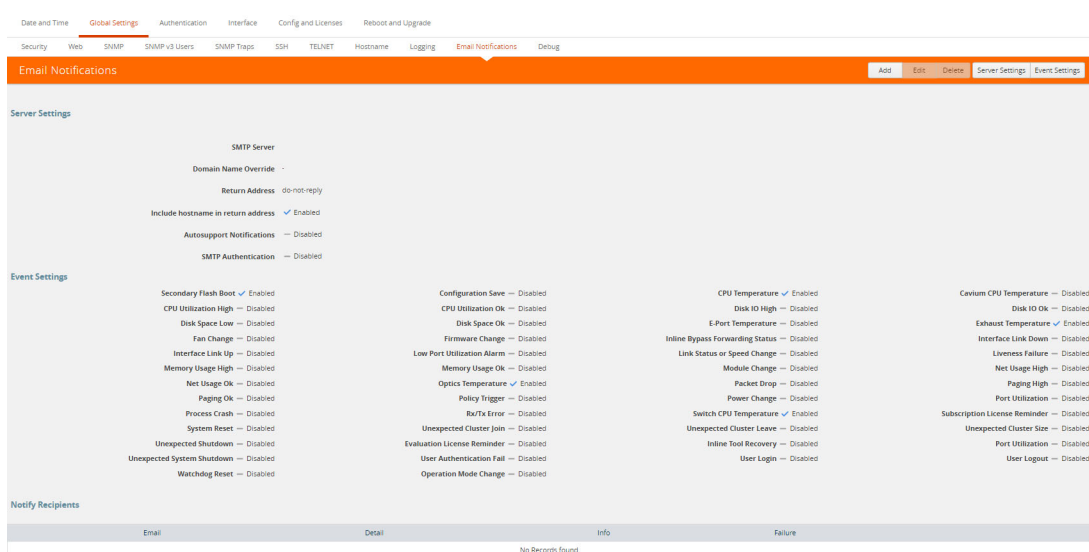


Figure 5-6: Email Notifications Page

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

Figure 5-7: Email Server Settings

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

Configuring the Event Settings

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

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

Figure 5-8: Email Event Settings

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

Adding Email Notification Recipients

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

1. Select **Settings > Global Settings > Email Notifications**, and then click **Add**.
2. Enter the recipient's email address in the **Email Address** field. You can add more than one email address, separating each address with a comma.
3. Set the level of notification to be sent to the recipient by selecting one or more of the following:
 - **Send Detail Notification** — send a detailed description about the event. Use detail notification to specify whether summarized 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.
4. (Optional) Click **Send Test Email** to send an test email to the recipient or recipients specified in [Step 2](#).
5. Click **OK**.

Using a Custom Banner

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

To set the custom banner:

1. Select **Settings > Global Settings > Host Name**.
2. Click **Edit**. The Edit Hostname page displays a shown in [Figure 5-9](#).
3. Enter the custom banner in the Login Message field.
4. Click **OK**.

Edit Hostname Save Cancel

▼ System Hostname

Hostname

▼ DHCP Hostname

Send hostname with DHCP client request Enabled

System Hostname Use System hostname (currently HC2-C03-13)

Use alternate hostname for DHCP

▼ Banners

Message Of The Day

Login Message

Figure 5-9: Edit Host Name Page

Viewing Information About the Node

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

About

To view the About page (refer to [Figure 5-10 on page 66](#)), select **About** in the main navigation pane. 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 on which H-VUE is running. For example, GigaVUE-HC2.
- Host Name—the host name assigned to the node. For information about setting the host name, refer to [Configuring the Host Name](#) on page 55
- Uptime—the date that the current version was installed and the number of hours, minutes, and seconds that the node has been running.

About GigaVUE-OS

Product Name	GigaVUE-OS
Version	4.8.00
Build ID	28102
Build Date	2016-10-17 04:18:51
Version Summary	GigaVUE-OS 4.8.00 Build 28102 2016-10-17 04:18:51 ppc_gvhc2.root@jenkins-slave017.git:fceb0029b05a
Git Hash	fceb0029b05a8d7384a10041f5ced19c83be4fd9
U-Boot Version	2011.06.7 (Oct 17 2016 - 04:20:36)
CPLD version	CPLD: 24
TS version	
Model	GigaVUE-HC2
Host Name	HC2-C03-13
Host ID	85a2463a784f
Uptime	2016-10-17T18:23:40

Figure 5-10: About Page

Interface

The Interface page (refer to [Figure 5-11 on page 68](#)) shows status information about the various interfaces. To access the interface page, select **Settings > interface > Interface**. The page provides the following information:

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

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

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

- Autoconf enabled
- Autoconf privacy
- IPv6 addresses
- Dhcp enabled
- Speed
- IP address
- Netmask
- Type
- ifindex
- IPv6 enabled
- Autoconf route
- DHCPv6 running
- IPv6 address

Date and Time Global Settings Authentication **Interface** Config and Licenses Reboot and Upgrade

Interface DNS

Interface

eth0

Admin Status ✓	Speed auto
Link Status ✓	IP address 10.115.152.53
Duplex auto	Netmask /21
MTU 1500	Type ethernet
HW addr 00:1D:AC:12:00:38	Ifindex 3
IfSource physical	IPv6 enabled yes
Autoconf enabled no	Autoconf route yes
Autoconf privacy no	DHCPv6 running no
IPv6 addresses -	IPv6 address -
Dhcp enabled no	

eth1

Admin Status —	Speed -
Link Status —	IP address -
Duplex -	Netmask -
MTU 1500	Type ethernet
HW addr 00:1D:AC:13:00:38	Ifindex 4
IfSource physical	IPv6 enabled no
Autoconf enabled no	Autoconf route no
Autoconf privacy no	DHCPv6 running no
IPv6 addresses -	IPv6 address -
Dhcp enabled no	

Figure 5-11: Interface Page

DNS

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

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

Cluster Safe and Limited Modes

Starting in software version 4.7, safe and limited modes are introduced to safeguard critical provisioning errors for both standalone nodes and nodes in a cluster.

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

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

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

When a node is in safe mode, H-VUE displays the Safe Mode banner as shown in [Figure 5-12](#).

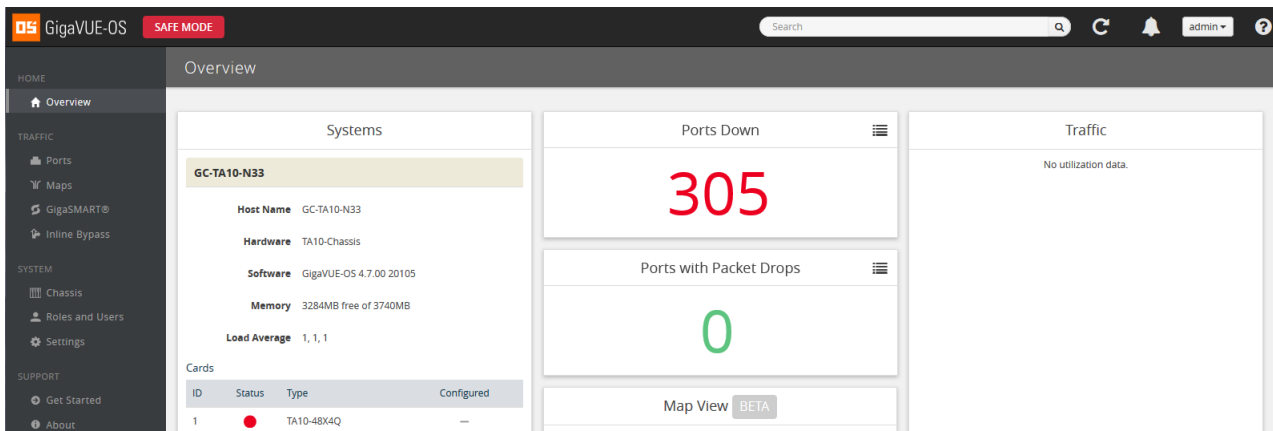


Figure 5-12: Node in Safe Mode

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.

Figure 5-13 shows the message displayed in safe mode.

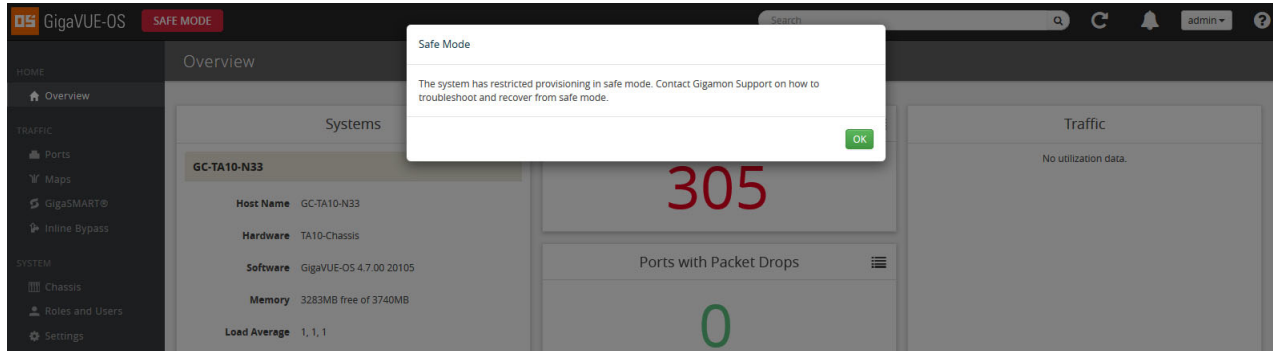


Figure 5-13: Safe Mode Message

Safe Mode

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

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

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

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

A node will automatically enter safe mode.

When a node is in safe mode:

- The node displays a banner indicating it is in safe mode. (Refer to [Figure 5-12 on page 69.](#))
- An SNMP trap is sent to notify the user when the mode changes.
- Configured traffic continues to be forwarded.
- Traffic provisioning is not allowed on the affected node. Any other configuration remains as is.
- If the standby node in the cluster is in safe mode, it can still become the master if the current master fails or switches over, but the database on the standby node may

not be in sync, so it is not recommended to continue in that state. Instead, take immediate action to recover the node.

- In safe mode, the non-master nodes in the cluster do not process any incoming traffic configuration from the cluster master.

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 [Figure 5-13 on page 70](#).

When safe mode has been detected, collect information and report it Gigamon Technical Support. Refer to [Collecting Information for Technical Support](#) on page 72. 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. [Figure 5-14](#) shows a node in limited mode.

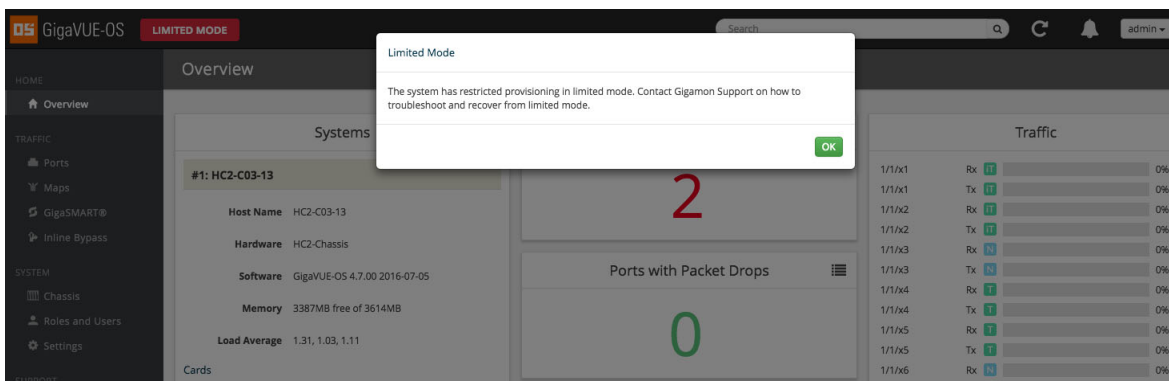


Figure 5-14: Node in Limited Mode

When limited mode has been detected, collect information and report it to Gigamon Technical Support. Refer to [Collecting Information for Technical Support](#) on page 72.

Enabling SNMP Trap for Safe Mode and Limited Mode

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

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

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

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

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

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

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

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

Collecting 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
- CLU or H-VUE screen captures
- SNMP captures

To contact technical support, refer to [Contacting Technical Support](#) on page 206.

Supported Browsers

GigaVUE-OS HVUE supports the following browsers:

Browser	Version
Mozilla Firefox™	• Version 49.00 and higher
Windows® Internet Explorer®	• Version 11 and higher
Apple® Safari®	• Version 9.1 and higher
Google® Chrome®	• Version 54.0 and higher

NOTE: IE 11 Compatibility view mode is not supported.

Configuring Internet Explorer for Use with H-VUE

H-VUE works best in Internet Explorer when the browser is configured to check for newer versions of stored pages every time pages are visited. Enable this option as follows:

1. Open Internet Explorer.
2. Select the **Tools > Internet Options** command.
3. In the **General** tab, locate the **Browsing history** section and click its **Settings** button.
4. Set the **Check for newer version of stored pages:** option to **Every time I visit the webpage**.
5. Click **OK** on the Temporary Internet Files and History Settings dialog.
6. Click **OK** on the Internet Options dialog.

6 Configuring 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](#) on page 76
- [About Role-Based Access](#) on page 78
- [Configuring Authentication and Authorization \(AAA\)](#) on page 81
 - [Configuring AAA Authentication Options](#) on page 85
 - [Granting Roles with External Authentication Servers](#) on page 88
 - [Adding AAA Servers to the Node's List](#) on page 94
 - [Configuring Roles in External Authentication Servers](#) on page 101
- [Supported Clients](#) on page 107
- [Default Ports](#) on page 108
- [FIPS 140-2 Compliance](#) on page 109
- [UC APL Compliance](#) on page 110
- [Common Criteria](#) on page 112
- [GigaVUE-OS Security Hardening](#) on page 121
- [Best Practices for Security Hardening](#) on page 123

About Security and Access

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

Security Tools	Description
Roles/Groups	<p>Roles specify which users have access to a given port. The following built-in roles are provided:</p> <ul style="list-style-type: none">• 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 <p>Administrators create additional custom <i>roles</i> and assign them to users together with the Default role. For example, if you create a role named Security_Team and assign it to tool port 5/1/x2, users assigned the Security_Team role will be able to access tool port 5/1/x2. Conversely, users without a role that gives them some access to tool port 5/1/x2 will not even be able to see it in H-VUE or the CLI. Users can have multiple assigned roles, allowing administrators to fine-tune access to the Visibility Platform.</p>
Permissions	<p>Administrators assign Permissions to specify what users can do with a port to which they have access. You can assign the following permission levels:</p> <ul style="list-style-type: none">• 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. <p>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).</p> <p>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.</p>
Port Locking/ Sharing	<p>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.</p> <p>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.</p> <p>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.</p>

Security Tools	Description
Authentication	<p>The GigaVUE H Series node can authenticate users against a local user database or against the database stored on an external authentication server (LDAP, RADIUS, or TACACS+).</p> <p>Admin users can specify the authentication methods used for logins using AAA Authentication.</p> <p>NOTE: The serial console port always retains local authentication as a fallback option to prevent unintended lockouts.</p>

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 User's Guide*.

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

About Role-Based Access

GigaVUE nodes use role-based access control to manage access to the Gigamon Visibility Platform, providing different groups of users with different analysis needs full access to the packets they need for their tools. Figure 6-1 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 6-1 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.

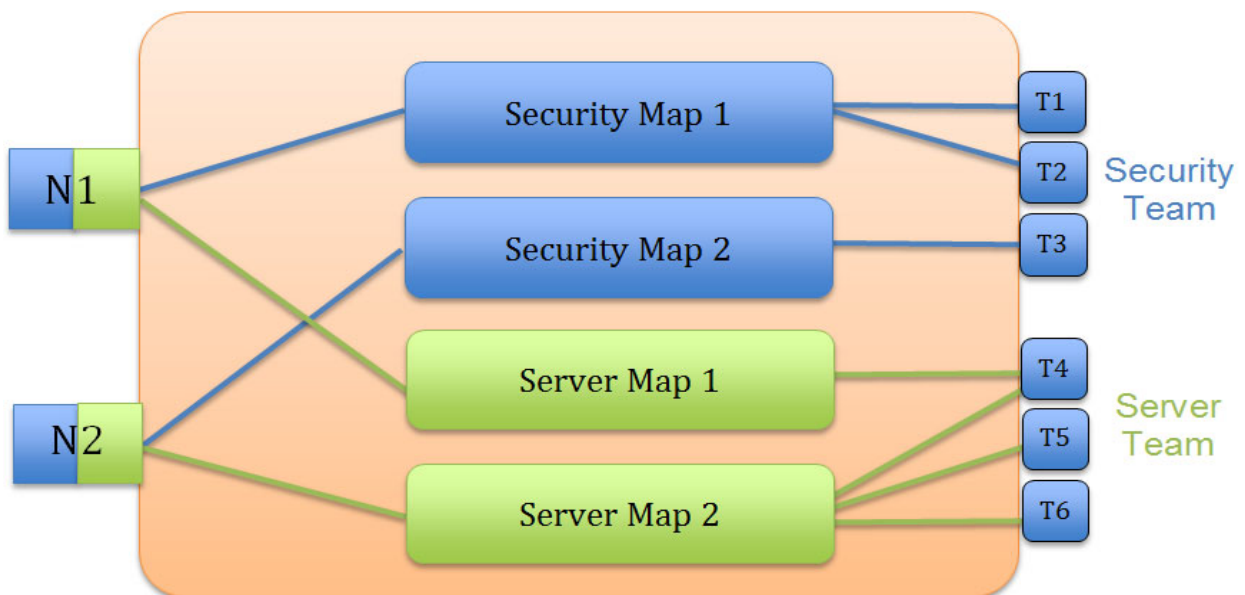


Figure 6-1: Role-Based Access in Action

Configuring Role-Based Access: A Summary

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

Step	Description
Configure Roles	<p>Administrators use the Roles page to create roles.</p> <p>At first, roles are empty containers. You can create as many as you need to share the Visibility Platform effectively. For example, if you have an IT organization with six different groups (Security, Desktop, Application Performance Management, Server, Archive, and so on), each with different packet needs, you may want to create separate roles for each of them and assign them to different sets of tool ports.</p> <p>NOTE: The built-in “Default” role has no access to unassigned ports.</p>
Create Users with Roles Assigned	<p>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.</p> <p>Keep in mind that admin-level users automatically have access to all roles. Administrators assign roles to default-level users.</p>
Associate Roles with Ports and Permissions	<p>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.</p>
Restriction for Removing a Role	<p>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.</p>
Fine Tune and Evolve	<p>The Visibility Platform evolves as your needs change. You can continue to add new roles and tweak assigned ports and permissions to achieve the sharing results needed for different groups to get the packets they need</p>

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 6-2](#)

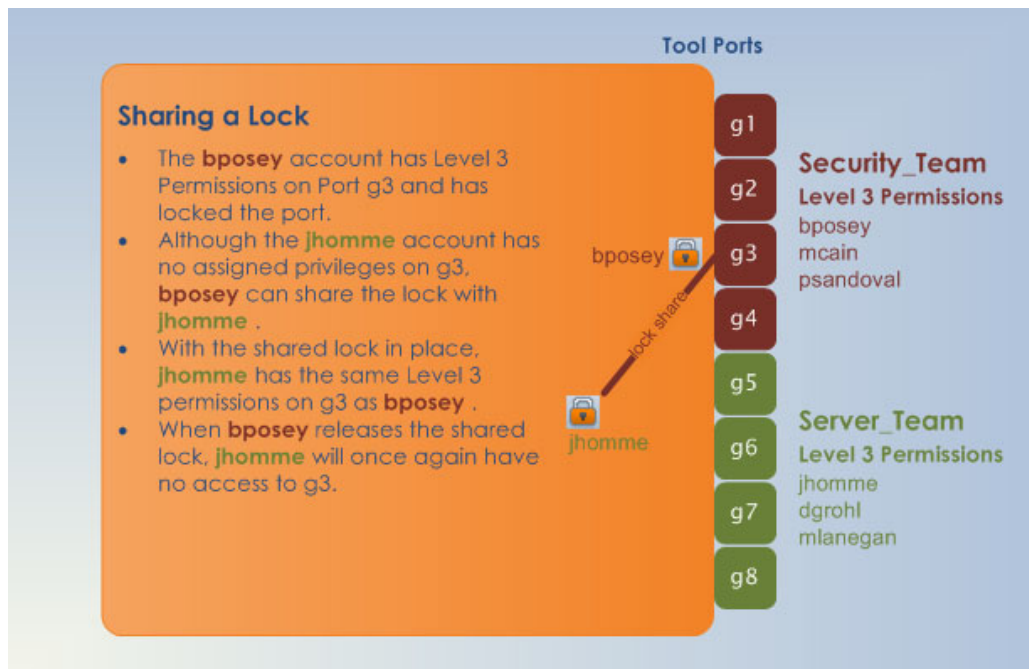


Figure 6-2: Sharing Locks

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.

Configuring Authentication and Authorization (AAA)

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

To open the AAA page, which is shown in [Figure 6-3](#), select **Settings > Authentication > AAA**.

Refer to the following sections for details:

- [Configuring AAA Authentication Options](#) on page 85
- [Granting Roles with External Authentication Servers](#) on page 88
- [Adding AAA Servers to the Node's List](#) on page 94

The screenshot displays the 'Authentication' configuration page. At the top, there are navigation tabs: 'Date and Time', 'Global Settings', 'Authentication' (selected), 'Interface', 'Config and Licenses', and 'Reboot and Upgrade'. Below these are sub-tabs: 'AAA', 'RADIUS', 'TACACS+', and 'LDAP'. The main content area is titled 'Authentication' and is divided into several sections:

- Authentication Priority:** Four dropdown menus for 'First Priority' (Local), 'Second Priority' (None), 'Third Priority' (None), and 'Fourth Priority' (None). A note below states: '* You are currently unauthorized to authenticate against: Local'.
- User Mapping:** Two dropdown menus: 'Map Order' (Remote First) and 'Map Default User' (operator).
- Password:** An 'Enabled' checkbox (unchecked) and a 'Duration' spinner set to 90 Days.
- Lockout:** Four checkboxes: 'Track Authentication Failures' (checked), 'Enable Lockout' (checked), 'Enable Admin Lockout' (unchecked). Three spinners: 'Lock time' (0 Seconds), 'Unlock time' (15 Seconds), and 'Maximum Failure' (5).
- Non local user Authentication:** Two checkboxes: 'Track Authentication Failures' (checked) and 'hashUsername' (checked).

Figure 6-3: Authentication and Authorization Page

Overview of the AAA Page

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

Authentication Priority

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

- Local
- TACACS+
- RADIUS
- LDAP

For details about setting the login methods, refer to [Configuring AAA Authentication Options](#) on page 85.

User Mapping

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

- **Remote First**—Maps externally authenticated logins in the following order:
 - a. Mapped to the matching local account name, if present.
 - b. If there is no matching local account, the local user mapping attribute provided by the AAA server is used.
 - c. If the local user mapping attribute is not present or does not specify a valid local user account, the account name specified by the **Map Default User**.
This is the default.
- **Local Only**—Maps all externally authenticated logins to the user specified by **Map Default User**.
- **Remote Only**—Maps externally authenticated logins in the following order:
 - a. Mapped to the matching local account name, if present.
 - b. If there is no matching local account, the local user mapping attribute provided by the AAA server is used.
 - c. If the local user mapping attribute is not present or does not specify a valid local user account, no further mapping is attempted.

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

Password

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

Lockout

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

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

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

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

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

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

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

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

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

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

Non Local User Authentication

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

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

FAQ for Logins and Passwords

This section answers frequently asked questions for logins and passwords.

Do Passwords Expire?

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

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

What Happens After Unsuccessful Logins?

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

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

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

Can a User be Forced to Change Their Password?

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

Are Passwords Displayed?

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

Who Creates Users and Passwords?

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

Configuring AAA Authentication Options

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

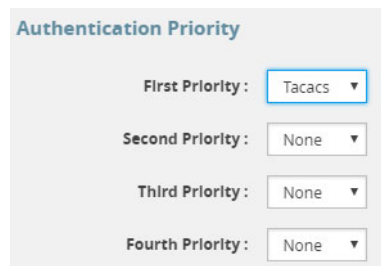
The valid authentication the authentication methods are:

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

For example, you configure the Mgmt port to authenticate with TACACS+, then local. If a user does not exist in the TACACS+ database, the user will be rejected from TACACS+, but then will be authenticated against local. Therefore, the user will be able to log on to the node.

You can enable any of or all of the authentication methods ((TACACS+, RADIUS, LDAP, and local) at the same time. If you enable more than one method, the GigaVUE H Series node uses the methods in the same order in which they are specified, falling back as necessary. If all servers using the first method are unreachable, the GigaVUE H Series node will fall back to the secondary method, and so on.

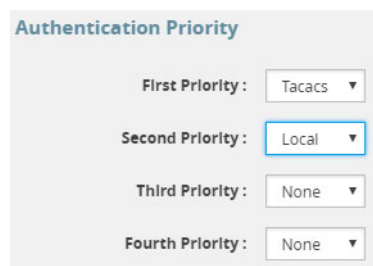
In the following example, if local is not included as one of the methods, the node will be authenticated exclusively by the TACACS+ server:



The screenshot shows the 'Authentication Priority' configuration interface. It contains four rows, each with a label and a dropdown menu:

- First Priority: Tacacs
- Second Priority: None
- Third Priority: None
- Fourth Priority: None

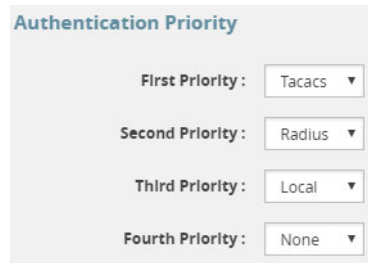
Access is only given to one method at a time. In the following example, if the TACACS+ server is reachable, the local method will not be checked. Only if the TACACS+ server becomes unreachable will the method fall back to local.



The screenshot shows the 'Authentication Priority' configuration interface. It contains four rows, each with a label and a dropdown menu:

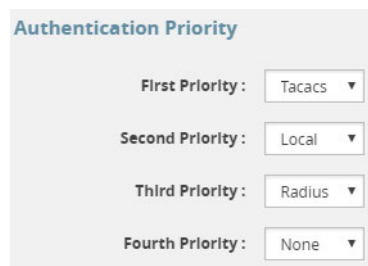
- First Priority: Tacacs
- Second Priority: Local
- Third Priority: None
- Fourth Priority: None

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



The screenshot shows a configuration panel titled "Authentication Priority" with four rows of dropdown menus. 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.

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



The screenshot shows a configuration panel titled "Authentication Priority" with four rows of dropdown menus. 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 "Radius" selected. The fourth row is "Fourth Priority:" with "None" selected.

To prevent lockouts, it is recommended that you include **local** as one of the methods. However, the **local** method is optional. Refer to *Remote Authentication Only* on page 568.

For example, you could use an external authentication server as your primary authentication method with local authentication as a fallback (Figure 6-4). The fallback is used when an authentication server is unreachable.

NOTE: If a server responds to a login attempt with an authentication reject, no further servers using that method are tried. Instead, the next method is tried until either the user's login is granted or all specified methods are exhausted.

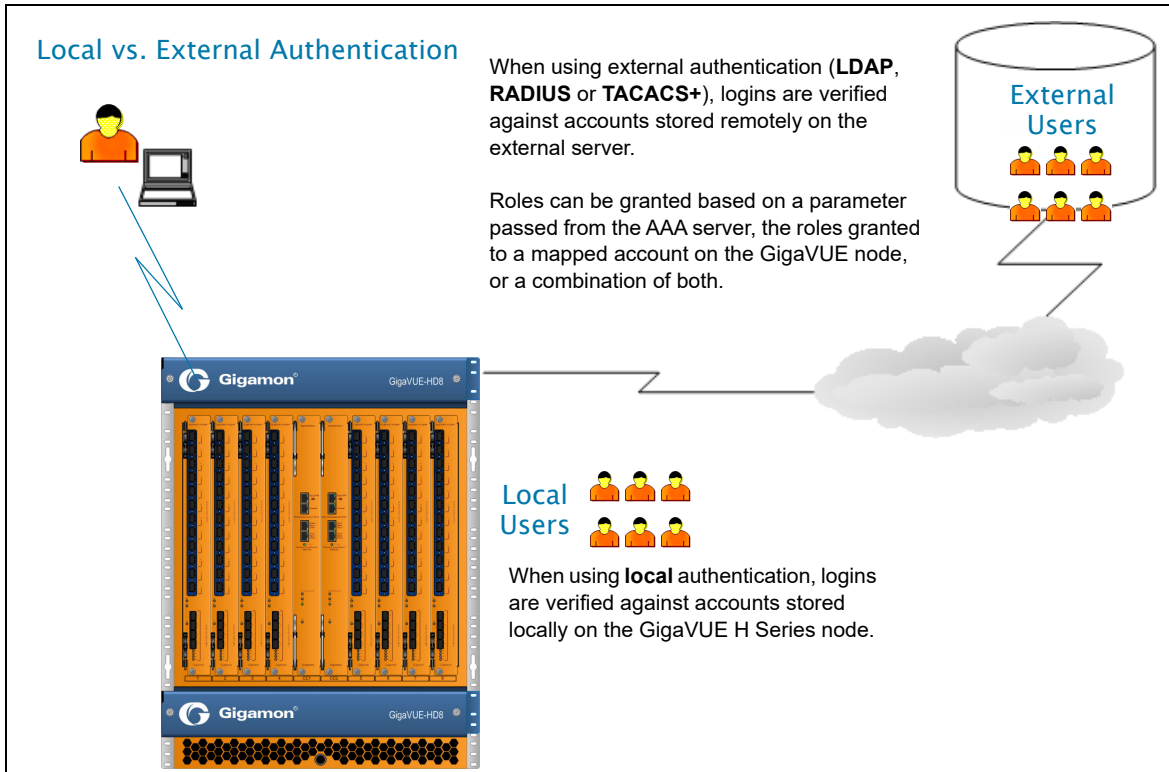


Figure 6-4: Local vs. External Authentication

Remote Authentication Only

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

Authentication Priority

First Priority: Tacacs ▼

Second Priority: None ▼

Third Priority: None ▼

Fourth Priority: None ▼

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

User Mapping

Map Order: Remote Only ▼

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

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

If this happens, the only option is to use a password recovery process which requires a reboot of the node. Refer to [Contacting Technical Support](#) on page 206.

Authorization of User Account

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

Next Steps

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

- Add the RADIUS, TACACS+, or LDAP server to the GigaVUE H Series node's list using the corresponding **RADIUS**, **TACACS+**, or **LDAP** pages. Refer to [Adding AAA Servers to the Node's List](#) on page 94.
- Set up GigaVUE H series nodes and users within the external authentication server itself. Depending on your authorization model, you can grant privileges to externally authenticated users based on the roles assigned to a corresponding account on the local node, the roles passed from the AAA server, or a combination of both. Refer to [Granting Roles with External Authentication Servers](#) on page 88 for details.

Granting Roles with External Authentication Servers

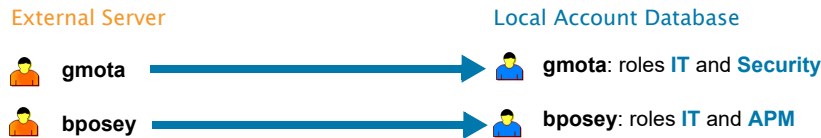
Roles are configured on the GigaVUE H Series node itself. Roles consist of a set of ports and permission levels specifying what a user with the role assigned can do on the port.

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

- [Using Local Role Assignments](#) on page 88
- [Using AAA Server Role Assignments](#) on page 89
- [Using Combination of Local and AAA Role Assignments](#) on page 89

Using Local Role Assignments

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



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

Using 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.



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

Using 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.



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

- **gmota** is mapped to local user **mcain**. He receives both the role configured in the AAA server (**IT**) and the role locally assigned to **mcain** (**Security**).
- **bposey** is mapped to local user **psandoval** with no additional roles specified. He receives only the roles locally assigned to the **psandoval** account (**IT** and **APM**).

Assigning Role in AAA Servers

Refer to [Configuring Roles in External Authentication Servers](#) on page 101 for instructions on how to set up users with local-user-name attributes in RADIUS, TACACS+, and LDAP AAA servers.

Creating Users for AAA and Remote Authentication Server

To create users for AAA and the remote authentication server:

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

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

Authentication

Authentication Priority

First Priority: Tacacs ▼

Second Priority: None ▼

Third Priority: None ▼

Fourth Priority: None ▼

* You are currently unauthorized to authenticate against: Local

User Mapping

Map Order: Remote Only ▼

Map Default User: networker ▼

Password

Enabled:

Duration: 90 Days

The settings in the example configuration are as follows:

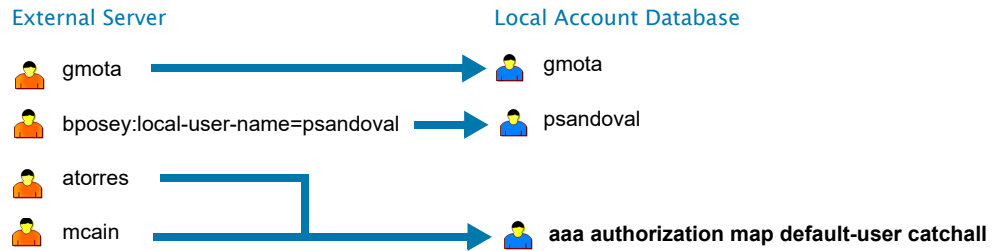
- AAA authorization:
 - Map Order: Remote Only means the user has a local account matching the external username account.
 - Map Default User: networker is a common user member of internal netops role and TACACS+ netops group.
- Authentication method(s):
 - Tacacs means that TACACS+ is the only authentication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

Configuring AAA Authorization

For details on the AAA authorization command, refer to [Overview of the AAA Page](#) on page 82.

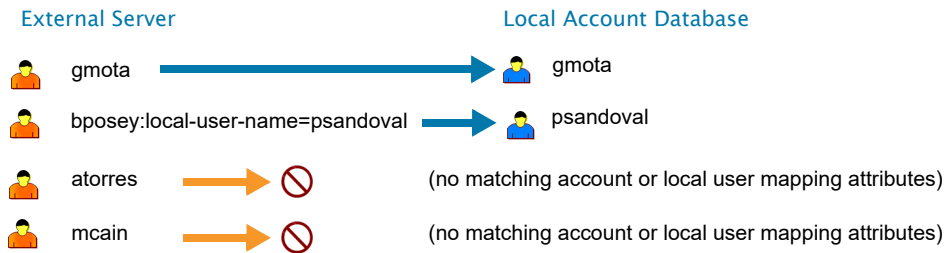
map order = remote-first

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 **mcaim** 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).

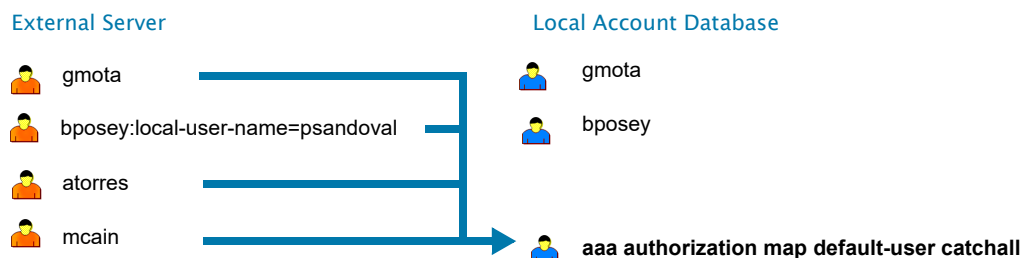


Figure 6-5: How the **map order** Argument Works

Example

The following steps demonstrate how to set up authentication using RADIUS with a fallback to local if no RADIUS server is available.

1. **Select Settings > Authentication > AAA.**
2. 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.

3. Add a RADIUS Server.

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

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

4. Allow the RADIUS server to include additional roles for a remotely authenticated user in the response. Refer to [Granting Roles with External Authentication Servers](#) on page 88.

Adding 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:

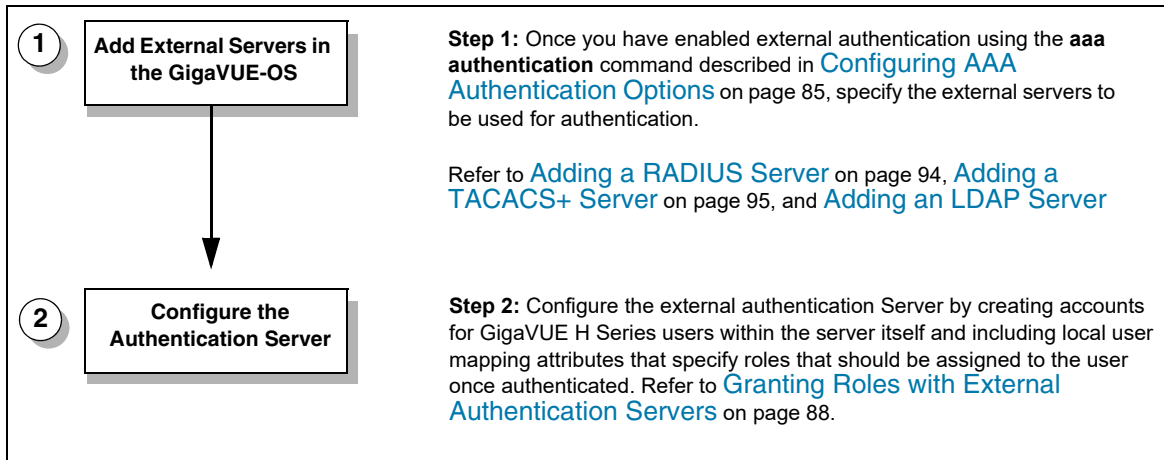


Figure 6-6: Steps to Use the Node with an External Authentication Server

Adding a RADIUS Server

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

To Add a RADIUS server, do the following:

1. Select **Settings > Authentication > RADIUS**.
2. Click **Add**.
3. Enter the RADIUS information on the ADD Radius page. For an example, refer to [Figure 6-7](#).

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

4. Click **Save**.

Figure 6-7: Adding a Radius Server

Deleting a RADIUS Server

To delete a RADIUS server, do the following:

1. Select **Settings > Authentication > RADIUS**.
2. Select the RADIUS server to delete as shown in [Figure 6-8](#).
3. Click **Delete**.

Server IP	Auth Port	Timeout	Retransmit	Enabled
<input type="checkbox"/> 10.10.10.100	120	0	0	No
<input checked="" type="checkbox"/> 10.10.10.121	1024	0	0	No

Figure 6-8: Selecting a RADIUS Server

Adding a TACACS+ Server

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

To Add a RADIUS server, do the following:

1. Select **Settings > Authentication > TACACS+**.
2. Click **Add**.
3. Enter the RADIUS information on the ADD TACACS Server page. For an example, refer to [Figure 6-9](#)
4. Click Save.

Enabled: Yes

Server IP: IP Address

Auth Port: 1-65535

Auth Type: pap

Use defaults for following

Key: *****

Timeout: 3

Retransmit: 1

Figure 6-9: Adding a TACACS Server

Deleting a TACACS+ Server

To delete a RADIUS server, do the following:

1. Select **Settings > Authentication > TACACS+**.
2. Select the TACACS+ server to delete. [Figure 6-10](#) shows an example, where the server with IP address 10.10.10.100 is selected.
3. Click **Delete**.

AAA RADIUS TACACS+ LDAP

TACACS Servers Add Edit Delete Default Settings

	Server IP	Auth Port	Timeout	Retransmit	Enabled
<input checked="" type="checkbox"/>	10.10.10.100	1001	0	0	No

Figure 6-10: Selecting a TACACS+ Server

Configuring 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 User's Guide*.

Adding 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 as shown in [Figure 6-11](#).
4. Click Save.

For Common Criteria, specify SHA password hashing when configuring the remote LDAP server. For details on Common Criteria, refer to [Common Criteria](#) on page 112.

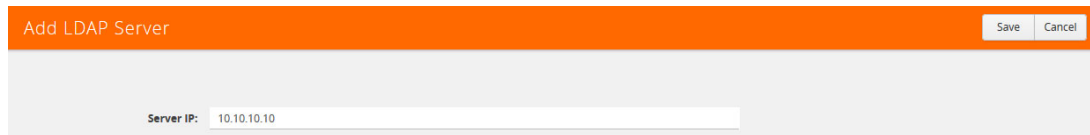
The image shows a web form titled "Add LDAP Server" with an orange header bar. In the top right corner of the header, there are "Save" and "Cancel" buttons. Below the header, there is a text input field labeled "Server IP:" containing the value "10.10.10.10".

Figure 6-11: Adding an LDAP Server

Setting 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 as shown in [Figure 6-12](#).

Date and Time		Global Settings	Authentication	Interface	Config and Licenses	Reboot and Upgrade		
AAA		RADIUS	TACACS+	LDAP				
LDAP Servers				Add	Delete	Default Settings		
Server IP	User Base DN	Search Scope	Login	Group Base DN	Group Attributes	Timeout	Bind DN	Port
<input checked="" type="checkbox"/> abcd	ou=users,dc=example,dc=com	subtree	uid		uniqueMember	5		389
<input type="checkbox"/> hq82.gigamon.com	ou=users,dc=example,dc=com	subtree	uid		uniqueMember	5		389
<input type="checkbox"/> x.x.3.4	ou=users,dc=example,dc=com	subtree	uid		uniqueMember	5		389
<input type="checkbox"/> x.x.x.4	ou=users,dc=example,dc=com	subtree	uid		uniqueMember	5		389

Figure 6-12: Selecting an LDAP Server

3. Click **Default Settings**.
4. 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 6-1](#)

Table 6-1: LDAP Default Settings

Default Setting	Description
User Base DN	Identifies the base distinguished name (location) of the user information in the LDAP server's schema. Specify this by identifying the organizational unit (ou) in the base DN. Provide the value as a string with no spaces. For example: ou=People,dc=mycompany,dc=com This is a global setting. It cannot be configured on a per-host basis.
User Search Scope	Specifies the search scope for the user under the base distinguished name (dn): <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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.

Table 6-1: LDAP Default Settings

Default Setting	Description
Group Base DN	<p>Specifies that membership in the named Group Base DN is required for successful login to the GigaVUE H Series node.</p> <p>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.</p> <p>This is a global setting. It cannot be configured on a per-host basis.</p>
Bind DN	<p>Specifies the distinguished name (dn) on the LDAP server with which to bind. By default, this is left empty for anonymous login.</p> <p>This is a global setting. It cannot be configured on a per-host basis.</p>
Group Login Attr	<p>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:</p> <ul style="list-style-type: none"> • custom attribute • member • uniqueMember <p>This is a global setting. It cannot be configured on a per-host basis.</p>
LDAP Version	<p>Specifies the version of LDAP to use. The default is version 3, which is the current standard. Some older servers still use version 2.</p> <p>This is a global setting. It cannot be configured on a per-host basis.</p>
Port	<p>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.</p> <p>This is a global setting. It cannot be configured on a per-host basis.</p>
Timeout	<p>Specifies how long the GigaVUE H Series node should wait for a response from an LDAP server to a bind request before declaring a timeout failure.</p> <p>The valid range is 0-60 seconds. The default is 5 seconds.</p>
Extra Roles	<p>When Yes is selected, enables the GigaVUE H Series node to accept user roles assigned in the LDAP server. The default is No.</p>
SSL Mode	<p>Enables SSL or TLS to secure communications with LDAP servers as follows:</p> <ul style="list-style-type: none"> • 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.
SSL Port	<p>Configures LDAP SSL port number.</p>
SSL Cert Check	<p>Enables LDAP SSL/TLS certificate verification. Use Off to disable.</p>
SSL ca-list	<p>Configures LDAP to use a supplemental CA list. Set to default Ca list to use the CA list configured with the Secure Cryptography (refer to Configuring Secure Cryptography Mode on page 113). Set to None if you do not want to use a supplemental list.</p>

Deleting an LDAP Server

To delete an LDAP Server, do the following:

1. Select **Settings > Authentication > LDAP**.

2. Select the LDAP server to delete on the LDAP Server page. For an example, refer to [Figure 6-6](#).
3. Click **Delete**.

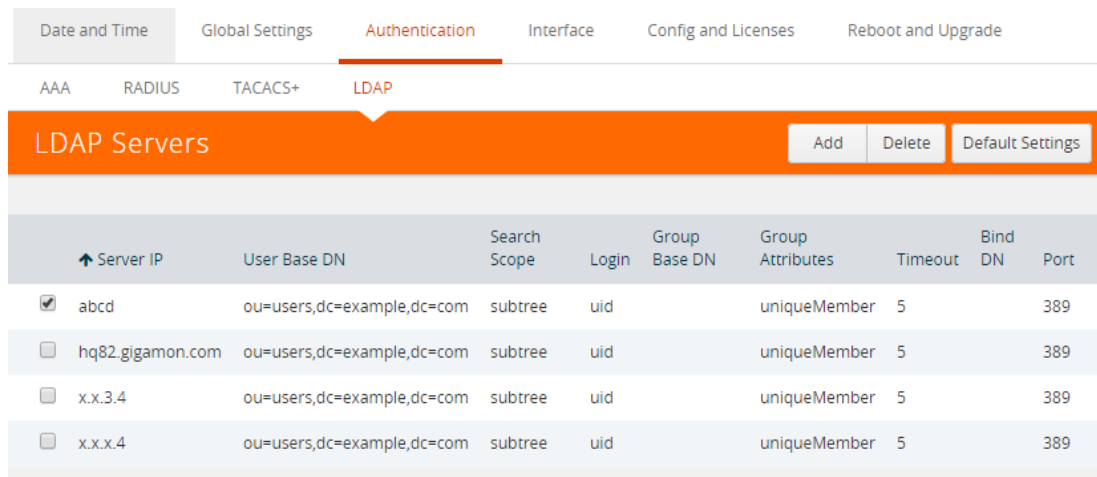


Figure 6-13: Deleting an LDAP Server

Configuring an IPv6 Address

To configure an IPv6 address for a LDAP server, enter the IPv6 address in the Server IP field 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 User's Guide*.

Configuring 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 details:

- [Granting Roles with External Authentication Servers](#)
- [Configuring Cisco ACS: RADIUS Authentication](#)
- [Configuring Cisco ACS: TACACS+ Authentication](#)
- [Configuring LDAP Authentication](#)

Configuring Cisco ACS: RADIUS Authentication

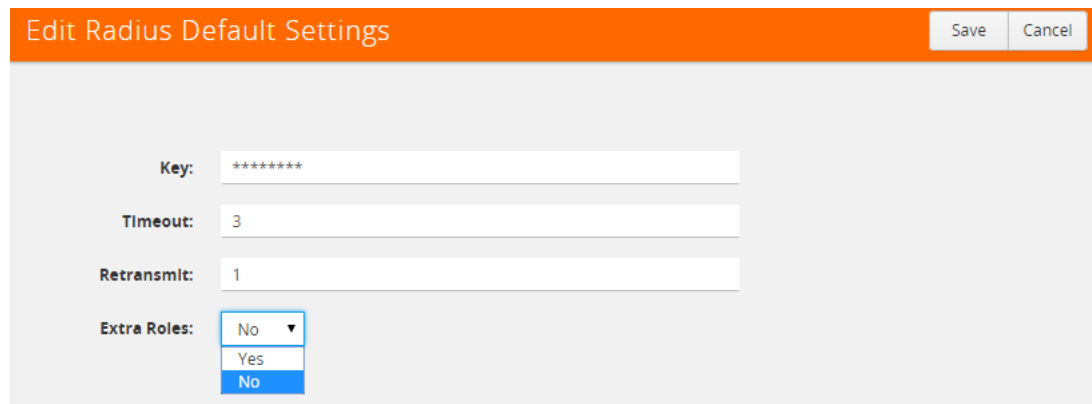
Use the following steps to configure Cisco ACS 5.x (RADIUS) to grant extra roles to externally authenticated users on the GigaVUE H Series node.

Enable Extra Roles for RADIUS on the GigaVUE Node

1. Use the following command to enable the GigaVUE H Series node to accept extra roles in the response from the AAA server:

Settings > Authentication > RADIUS > Default Settings

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



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

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

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

Buttons: Add, Edit, Replace, Delete

Dictionary Type: RADIUS-IETF

RADIUS Attribute: Class (Select)

Attribute Type: String

Attribute Value: Static

Value: local-user-name=operator:role-IT

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

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

Figure 6-14 shows these settings in a CiscoSecure ACS 5.x authorization profile.

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Create

General | Common Tasks | **RADIUS Attributes**

Attribute	Type	Value
Class	String	local-user-name=operator:role-IT

Buttons: Add, Edit, Replace, Delete

Submitted Fields: Submit, Cancel

Figure 6-14: Supplying the Class Field for RADIUS (ACS 5.x)

Configuring Cisco ACS: TACACS+ Authentication

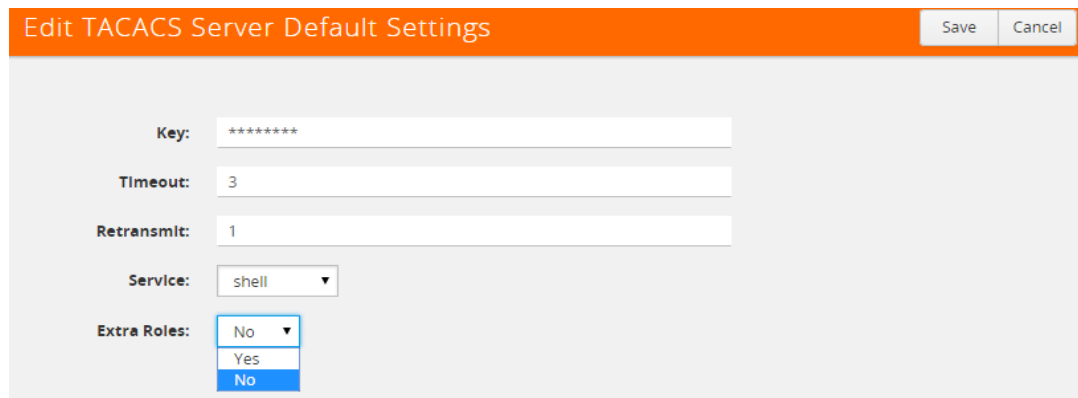
Use the following steps to configure Cisco ACS 5.x (TACACS+) to grant extra roles to externally authenticated users on the GigaVUE H Series node.

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

1. Use the following command to enable the GigaVUE H Series node to accept extra roles in the response from the AAA server.

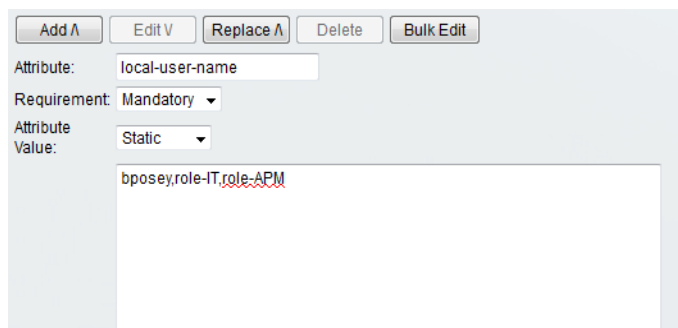
NOTE: The extra role must match a role already configured on the GigaVUE node/cluster.

Settings > Authentication > TACACS > Default Settings



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

2. Navigate to **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles** and click **Create** to add a new shell profile.
3. Give the profile a name and description in the **General** tab.
4. Click on the **Custom Attributes** tab.
5. Set the Attribute field to local-user-name.
6. Leave the **Requirement** and **Attribute Value** fields at their default value (**Mandatory** and **Static**, respectively).
7. Supply the local user mapping and optional roles, as shown in the following figure:



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

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

Figure 6-15 shows the an example of a shell profile for TACACS+ in ACS 5.x with the local-user-name attribute supplied.

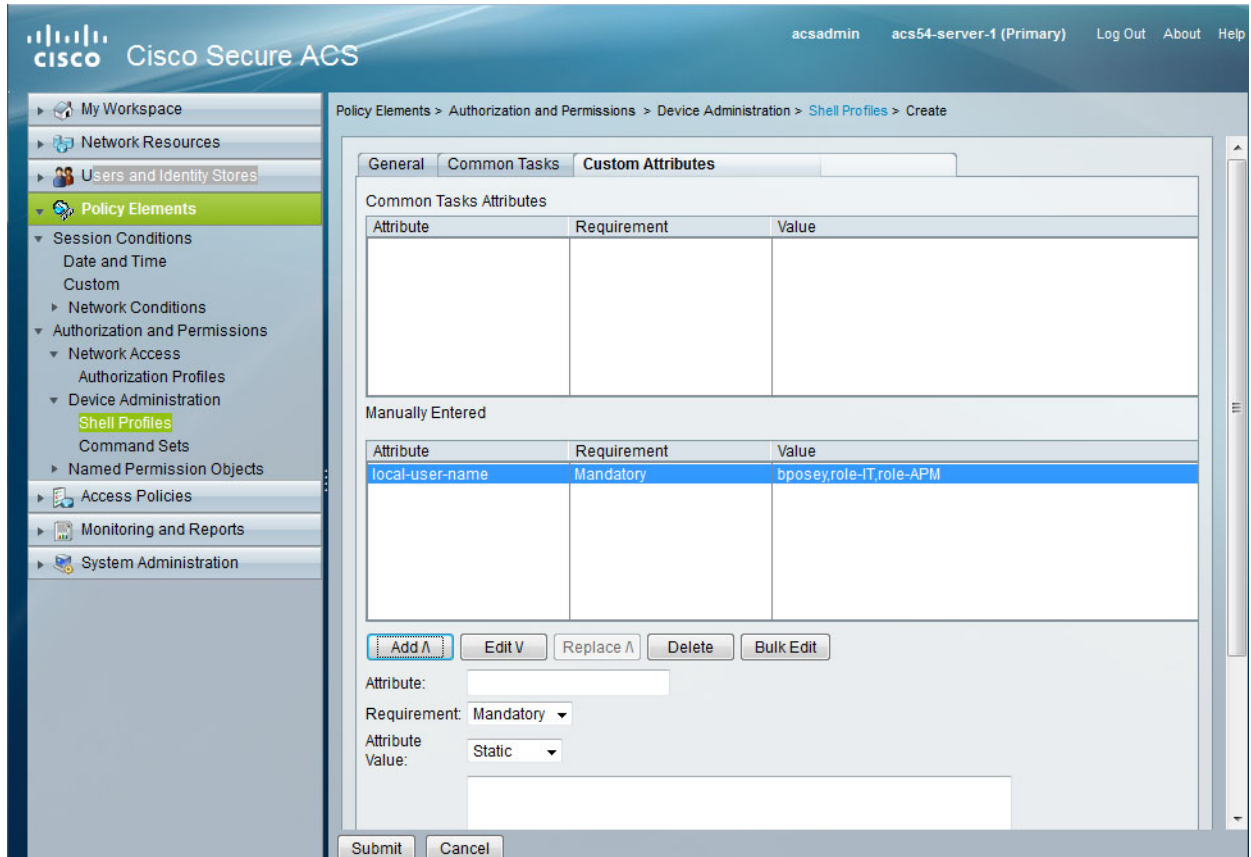


Figure 6-15: Supplying local-user-name and Roles in ACS 5.x for TACACS+

Configuring LDAP Authentication

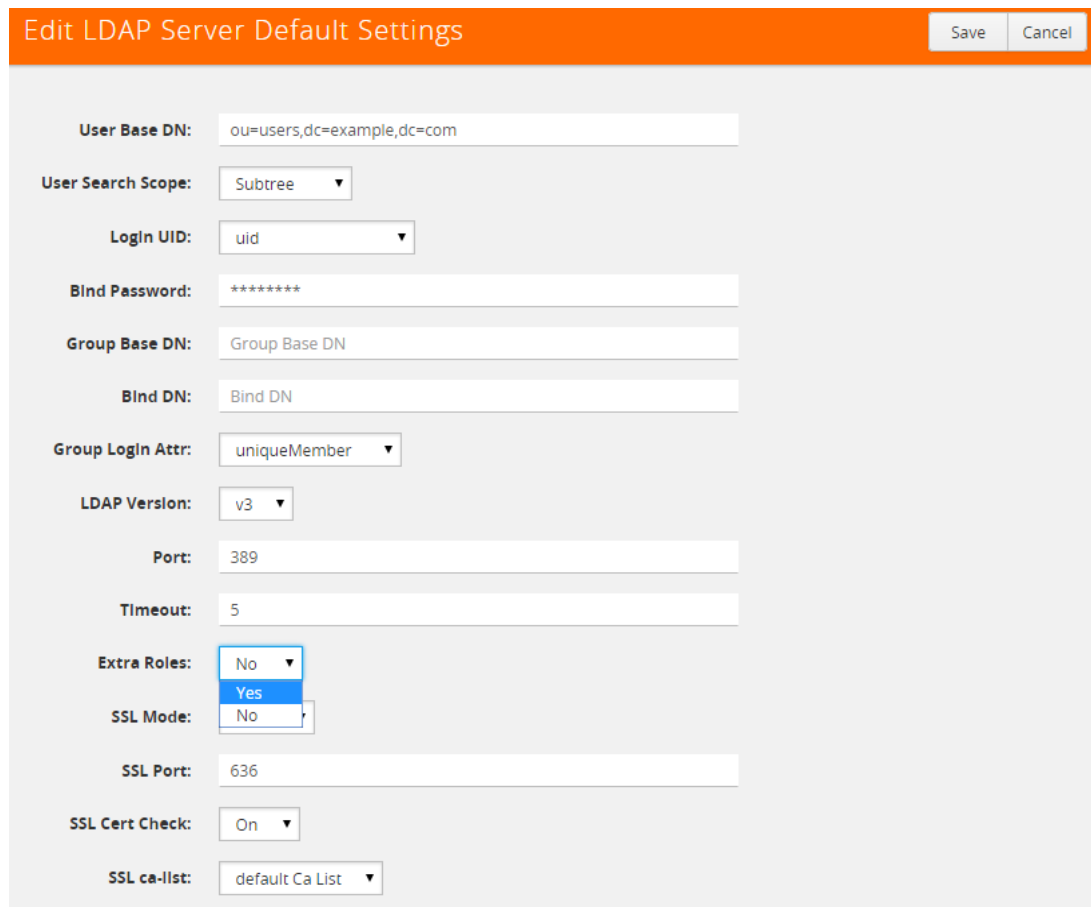
Use the following steps to configure an LDAP server (for example, Apache Directory Server) to grant extra roles to externally authenticated users on the GigaVUE H Series node.

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

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

- a. Select **Settings > Authentication > LDAP**
- b. Click **Default Settings**.
- c. Set the **Extra Roles** field to **Yes** as shown in [Figure 6-16](#).

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



The screenshot shows the 'Edit LDAP Server Default Settings' interface. The 'Extra Roles' dropdown menu is open, with 'Yes' selected. Other visible settings include: User Base DN: ou=users,dc=example,dc=com; User Search Scope: Subtree; Login UID: uid; Bind Password: *****; Group Base DN: Group Base DN; Bind DN: Bind DN; Group Login Attr: uniqueMember; LDAP Version: v3; Port: 389; Timeout: 5; SSL Mode: No; SSL Port: 636; SSL Cert Check: On; SSL ca-list: default Ca List.

Figure 6-16: Setting Extra Roles

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

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

The attribute format is as follows:

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

Figure 6-17 shows an example.

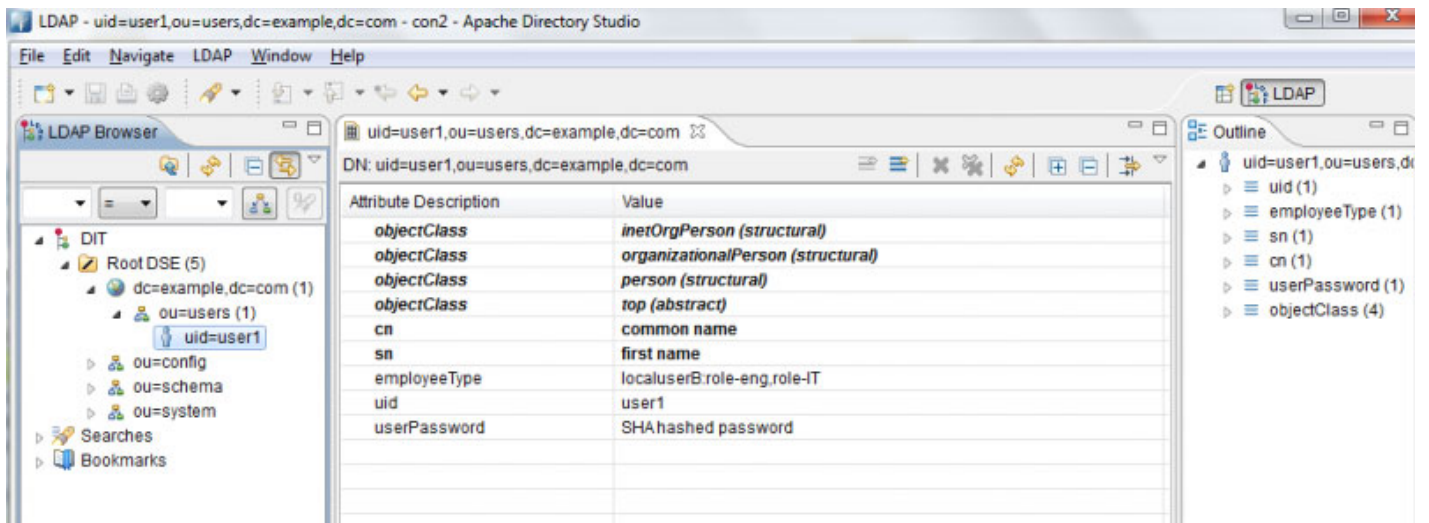


Figure 6-17: Adding the *employeeType* Attribute

Supported Clients

The following versions of serial, SSH, and Telnet clients are supported:

Table 6-2: Tested SSH/Telnet Clients

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

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

Default Ports

The following default ports are normally open on GigaVUE nodes:

Table 6-3: Open Default Ports

Port Number	Protocol	Description	Service/Server
22	TCP	SSH	OpenSSH 6.2
23	TCP	Telnet	Linux telnetd
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 6-4: Default Ports, Normally Closed

Port Number	Description
20	FTP
49	TACACS+
123	NTP
162	SNMP host
389	LDAP
514	syslog
1080	Web proxy
1812	RADIUS
2055	NetFlow Collector

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

Table 6-5: Other Valid Ports

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

FIPS 140-2 Compliance

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

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

FIPS is always enabled. No configuration is required.

For communications with the GigaVUE node, SSL or SSH clients are requested to use high strength ciphers during the session set up negotiation. A high strength cipher is one that uses a key that is equal to or greater than 112 bits.

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

UC APL Compliance

GigaVUE H Series products are compliant with Unified Capabilities Approved Products List (UC APL). The products include the GigaVUE-HB1, GigaVUE-HC2, GigaVUE-HD4, and GigaVUE-HD8, as well as the GigaVUE-TA10 and GigaVUE-TA40.

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

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

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

- httpd 2.4.29
- apr 1.6.3
- apr-util 1.6.1
- pcre 7.8

Configuring 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 [Accepting DoD Web Server Certificates](#) on page 110.
- enable login failure tracking. Refer to [Enabling Login Failure Tracking](#) on page 110.

Accepting 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
```

Enabling 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
```

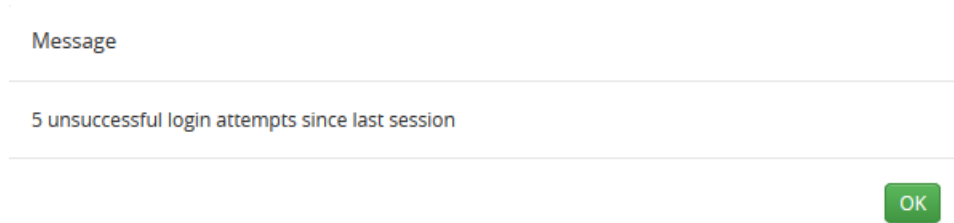
Unsuccessful login attempts are displayed on the CLI. Refer to [Displaying Unsuccessful Login Attempts](#) on page 111.

Displaying 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.

Common Criteria is currently in version 3.1, revision 4.

GigaVUE nodes are classified as a network device by Common Criteria. A network device is defined as an infrastructure device that can be connected to a network. The following GigaVUE nodes that run GigaVUE-OS are certified for Common Criteria:

- GigaVUE-HC1
- GigaVUE-HC2
- GigaVUE-HC3
- GigaVUE-HD4
- GigaVUE-HD8
- GigaVUE-TA1
- GigaVUE-TA10
- GigaVUE-TA40
- GigaVUE-TA100
- GigaVUE-TA200

Configuring Common Criteria

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

- enable secure cryptography mode. Refer to [Configuring Secure Cryptography Mode](#) on page 113.
- enable secure passwords mode and configure a password length of 15. Refer to [Configuring Secure Passwords Mode](#) on page 115.
- configure syslog to send audit data securely. Refer to [Encrypting Syslog Audit Data](#) on page 118.

Configuring Secure Cryptography Mode

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

Initially, the secure cryptography mode is disabled. There are two steps to enabling it: configuring the mode, and then reloading either the node, if it is standalone, or the cluster, if the node is in a cluster environment.

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

Enabling Secure Cryptography Mode

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

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

The system displays the following notification:

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

5. For the secure cryptography mode to take effect the node needs to be reloaded.
 - a. Select **Settings > Reboot and Upgrade**.
 - b. Click **Reboot**.

When a GigaVUE node is in secure cryptography mode, a status is displayed when you log in. For more information, refer to [Status of Secure Cryptography Mode](#) on page 115.

IMPORTANT: TLS version 1.2 is required for secure cryptography mode. Therefore, when enabling secure cryptography mode, you must also verify or change TLS version to 1.2 in the GigaVUE-OS CLI using this command: `web server ssl min-version tls1.2`. Refer to the *GigaVUE-OS CLI Reference Guide* for CLI guidance.

Disabling Secure Cryptography Mode

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

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

The system displays the following notification:

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

5. For the secure cryptography mode to take effect the node needs to be reloaded.
 - a. Select **Settings > Reboot and Upgrade**.
 - b. Click **Reboot**.

Ciphers to Use with Secure Cryptography Mode

Use the following ciphers with secure cryptography mode:

Secure Cryptography Mode
All Platforms
AES128-CBC
AES256-CBC

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

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

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

*AES256-CBC is needed for a GigaVUE-HD8 or GigaVUE-HD4 with two HCCv2 control cards to allow secure cryptography mode to be enabled and disabled.

Cryptographic Algorithms

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

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

Status of Secure Cryptography Mode

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

Configuring Secure Passwords Mode

Passwords that are complex and long in length provide security. To enable the secure passwords mode:

1. Select **Settings > Global Settings > Security**.

The Security page displays. Secure Cryptography and Secure Passwords are disabled by default.

2. Click **Edit**.

3. On the Edit Security Settings page, select **Secure Passwords**.

4. In the **Min Password Length** field, specify the minimum password length from 8 to 30 characters.

For Common Criteria certification, the password length should be at least 15 characters.

5. Click **Save**.

The system displays the following notification:

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

6. To reboot the system:

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

- b. Click **Reboot**.

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

- uppercase letters
- lowercase letters
- numbers
- special characters, for example, !, @, #, \$, %, ^, &, or *

The minimum number of characters allowed is determined by the Secure Passwords setting if it is enabled.

For example, use the following steps to create and set the password for a user named myuserid user:

1. Select **Roles and Users > Users**.

2. On the User Setup page, click **Add**.

The Add New User page displays as shown in [Add New User Page](#) on page 116

The screenshot shows a web form titled "Add New User" with a sub-section "Account Details". The form contains the following fields and controls:

- User Name:** A text input field containing "User Name".
- Name:** A text input field containing "Name".
- Password:** A text input field containing "Password".
- Confirm Password:** A text input field containing "Confirm Password".
- Enabled:** A checkbox that is checked.

In the top right corner, there are "Save" and "Cancel" buttons.

Figure 6-18: Add New User Page

3. Enter the account details for the user. If the password does not adhere to the rules, a message is displayed as shown in Figure 6-19

The screenshot shows the same "Add New User" form as Figure 6-18, but with the following changes:

- User Name:** The text input field now contains "myuserid".
- Name:** The text input field now contains "user1".
- Password:** The text input field contains "*****". Below the field, the text "Password Invalid" is displayed in red.
- Confirm Password:** The text input field contains "Confirm Password".
- Enabled:** The checkbox remains checked.

The "Save" and "Cancel" buttons are still present in the top right corner.

Figure 6-19: Add New User with Invalid Password

4. After completing the account details, click **Save**.

Managing Blank Passwords

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

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

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

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

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

- [Disallowing Login with a Blank Password](#) on page 117
- [Allowing Login with a Blank Password](#) on page 117

Disallowing Login with a Blank Password

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

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

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

1. Go to **Settings > Global Settings > Security**. The Allow Blank Passwords field should be Disabled. Refer to [Figure 6-20 on page 117](#).

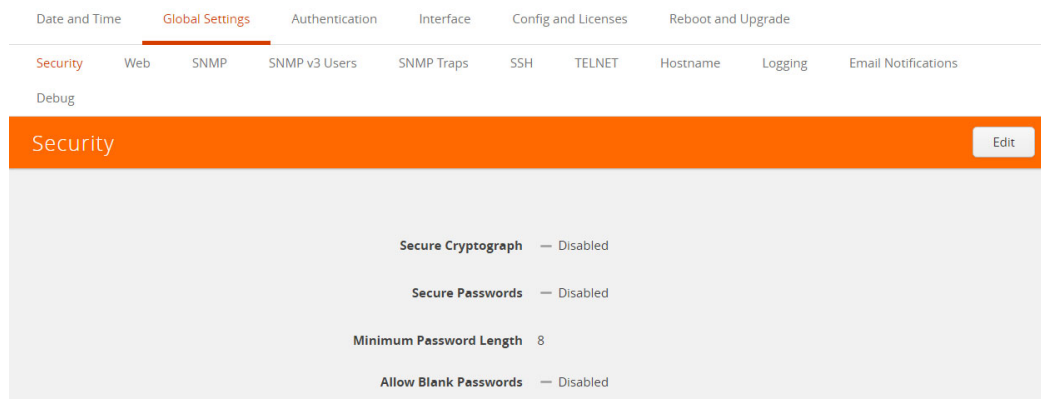


Figure 6-20: Allow Blank Passwords Disabled

2. If it is enabled, click **Edit** and uncheck the Allow Blank Passwords check box shown in [Figure 6-22 on page 118](#).

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

- a warning message if there are any user accounts in the system with a blank password
- an error message if the **admin** user account has a blank password
- an error message if the currently logged in user has a blank password
- an error message if there is an attempt to configure a blank password for a user

Allowing Login with a Blank Password

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

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

To allow logging into a system with a blank password:

1. Go to **Settings > Global Settings > Security**. Click **Edit**. Refer to [Figure 6-21 on page 118](#).

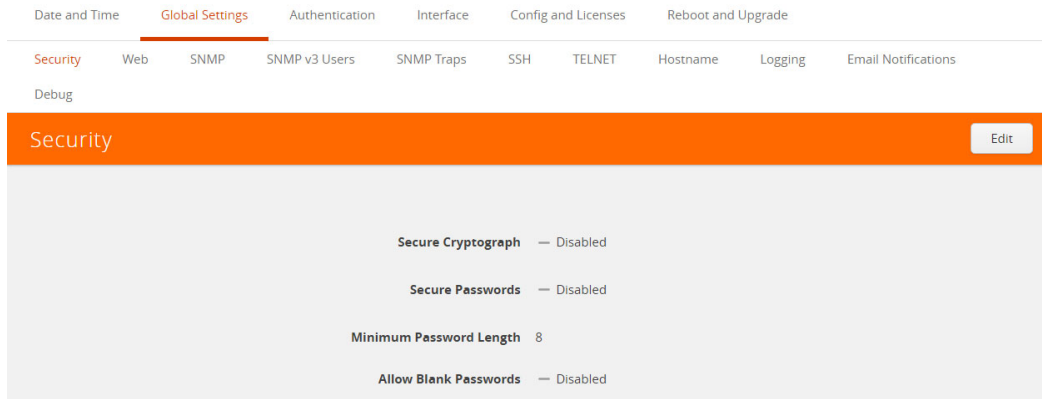


Figure 6-21: Global Settings Security Page

2. Click **Edit**. Select the Allow Blank Passwords check box. Refer to [Figure 6-22 on page 118](#).

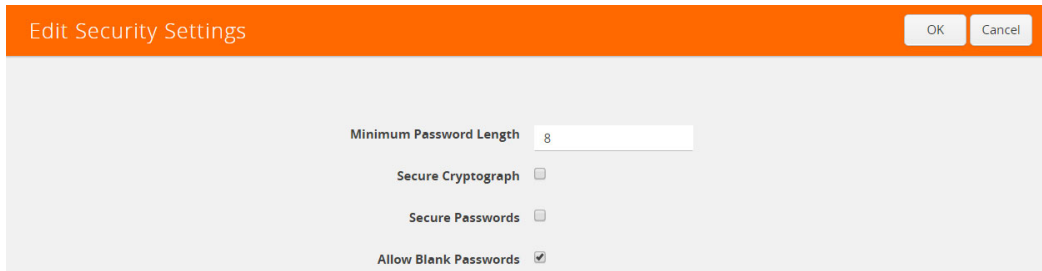


Figure 6-22: Allow Blank Passwords Check box

3. Click OK.

Encrypting 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.

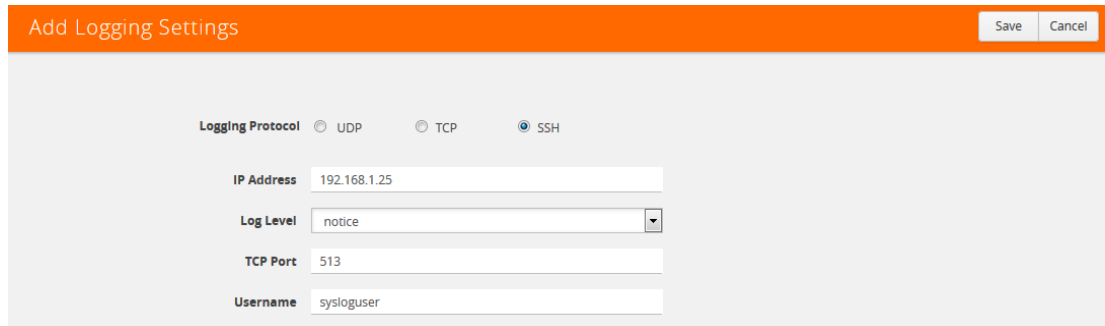
NOTE: The SSH Server needs to be enabled before completing these steps.

- a. Select **Settings > Global Settings > SSH**.
- b. Click **Add**.

The SSH Client Key page displays as shown in [Figure 6-23](#)

Figure 6-23: SSH Client Key Page

- c. In the **Username** field, enter admin and select **rsa1** for **Type**.
 - d. Click Generate **Client Keys** and copy the key contents.
2. Log in to the syslog server to paste the key, and then do the following:
 - a. Change the directory to `.ssh`.
 - b. Edit the `authorized_keys` file, located in the `.ssh` directory, using any editor (such as vi), then paste the key contents.
 If the `authorized_keys` file does not exist, create it
 If the `authorized_keys` file exists but does not have write access, change the access; for example, `chmod 644 authorized_keys`
 - c. Change the access on the `authorized_keys` file back to secure. For example, `chmod 600 authorized_keys`
 3. Configure the secured TCP connection.
 - a. In GigaVUE H-VUE, select **Settings > Global Settings > Logging**.
 - b. Click **Add**.
 - c. On the Add Loggings Settings page, select **SSH**.
 - d. Enter an IP address, Log Level, TCP port, and user name.
[Figure 6-24](#) shows an example with IP address 192.168.1.26, logging level of notice, TCP port 513, and a user name sysloguser.
Note: You can specify an IPv4, IPv6, or hostname.
 - e. Click **Save**.



Add Logging Settings Save Cancel

Logging Protocol UDP TCP SSH

IP Address 192.168.1.25

Log Level notice

TCP Port 513

Username sysloguser

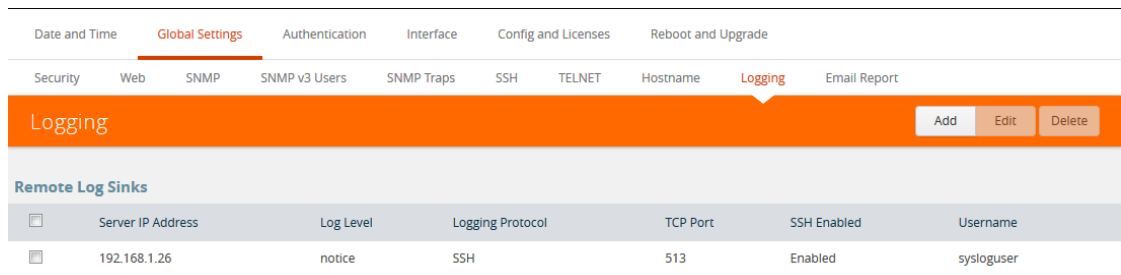
Figure 6-24: Example TCP Secure Connection

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.

Displaying Logging Information

To display logging information, select **Settings > Global Settings Logging**. This displays the Logging page. Figure 6-25 shows an example.



Server IP Address	Log Level	Logging Protocol	TCP Port	SSH Enabled	Username
192.168.1.26	notice	SSH	513	Enabled	sysloguser

Figure 6-25: Logging Page

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

GigaVUE-OS Security Hardening

To harden the GigaVUE operating system, GigaVUE-OS, against security threats, Gigamon fixes known vulnerabilities, keeps up-to-date any OS components that provide remote access (such as Apache, SSH, SSHD, and OpenSSL), and analyzes the system for attack vectors.

GigaVUE nodes run the GigaVUE-OS, which is hardened against the following:

- [SHA1-Based Signature in TLS/SSL Server X.509 Certificate](#) on page 121
- [ICMP Timestamp Response](#) on page 122
- [TCP Timestamp Response](#) on page 122
- [Non-Standard SNMP Community Name](#) on page 123

SHA1-Based Signature in TLS/SSL Server X.509 Certificate

Certificates generated by a third party certification authority are more secure than self-signed certificates. High strength ciphers with key lengths equal to or greater than 112 bits are also more secure than ciphers with less than 112 bits.

GigaVUE-OS supports TLS/SSL server X.509 certificates, including SHA2-256 and SHA2-512-based certificates, as well as SHA1-based certificates.

However, SHA1 has known weaknesses that expose it to collision attacks, which may allow an attacker to generate additional X.509 certificates with the same signature as the original.

Therefore, when a third party certificate is requested, SHA2-256 or SHA2-512 should be requested as the signature algorithm, and not SHA1.

To obtain a third party certificate, on Linux or Linux app (such as Cygwin), generate a private key as follows:

- `openssl req -new -key privkey.pem -out cert.csr`

The file, `cert.pem` will be sent to a third party certificate authority, which will generate a certificate.

The ciphers supported with TLS v1.0, 1.1, and 1.2 are listed in [Table 6-6](#) and [Table 6-7](#).

Table 6-6: Supported Ciphers with TLS v1.0 and v1.1

Modern Ciphers	Classical Ciphers
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	

Table 6-6: Supported Ciphers with TLS v1.0 and v1.1

Modern Ciphers	Classical Ciphers
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	

The ciphers supported with TLS v1.2 are listed in [Table 6-7](#).

Table 6-7: Supported Ciphers with TLS v1.2

Authenticated Encryption with Additional Data (AEAD) Ciphers	SHA-2 Ciphers
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc14)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc13)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc15)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	

ICMP Timestamp Response

The GigaVUE-OS does not respond to Internet Control Message Protocol (ICMP) timestamp requests.

The response to such a request is an ICMP timestamp response. The response can contain the date and time from a GigaVUE node, which could be used to exploit weak time-based random number generators in other services on the node, therefore this is disabled.

In addition, ICMP echo broadcasts, including timestamp requests and responses, are disabled, since ICMP echo requests may be used for Denial of Service (DoS) attacks, such as packet flooding.

TCP Timestamp Response

The GigaVUE-OS does not respond to Transmission Control Protocol (TCP) timestamp requests.

The response to such a request is a TCP timestamp response. The response can be used to approximate the uptime of the GigaVUE node, which can then be used in DoS attacks.

In addition, some operating systems can be fingerprinted based on the behavior of their TCP timestamps, therefore this is disabled.

Non-Standard SNMP Community Name

Gigamon does not recommend using the default SNMP community string, public. It recommends using a non-standard SNMP community name, gigamon.

For steps to protect against SNMP vulnerabilities, refer to [Recommendations for Vulnerabilities](#) on page 182 in the *Using SNMP* chapter.

Best Practices for Security Hardening

The following sections list best practices for security:

- [Using Telnet is Not Recommended](#) on page 123
- [Using SNMPv1 and SNMPv2 are Not Recommended](#) on page 123
- [Using Self-Signed Certificates are Not Recommended](#) on page 124
- [Using FTP and TFTP are Not Recommended](#) on page 124
- [Using Secure Cryptography Mode to Run Scans is Recommended](#) on page 124
- [Changing the Password on admin Account](#) on page 124
- [Best Practices for Passwords](#) on page 125

Using Telnet is Not Recommended

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

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

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

Using SNMPv1 and SNMPv2 are Not Recommended

Using SNMPv1 and SNMPv2 are not recommended because they authenticate using unencrypted, plaintext community strings.

Using SNMPv3 is recommended for access to the SNMP agent, as well as to SNMP traps. SNMPv3 authenticates using encrypted community strings. For more information, refer to [Using SNMP](#) on page 173.

Using Self-Signed Certificates are Not Recommended

Using self-signed TLS/SSL certificates are not recommended.

Certificates generated by a third party certification authority are recommended because they are issued by a Certification Authority (CA). Refer to [SHA1-Based Signature in TLS/SSL Server X.509 Certificate](#) on page 121 for how to obtain a third party certificate.

Using FTP and TFTP are Not Recommended

Using FTP or TFTP for file transfers is not recommended.

Using SFTP, SCP, or HTTPS is recommended for uploading or downloading files to or from GigaVUE nodes.

Using Secure Cryptography Mode to Run Scans is Recommended

Using secure cryptography mode to run scans is recommended.

Refer to [Configuring Secure Cryptography Mode](#) on page 113 for more information.

When a scan includes password brute force testing, it is recommended to disable locking users due to many attempts.

To disable lockout of accounts based on failed authentication attempts, select **Settings > Authentication > AAA**. Under Lockout, unselect **Enable Lockout**. For more information about Lockout, refer to [Lockout](#) on page 83.

Changing the Password on admin Account

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

If you have not changed the default password before the upgrade, you will be prompted to enter a non-default password. When upgrading through the CLI, **configuration jump-start** will automatically launch and prompt the system administrator to change the password on the **admin** account. For details, refer to the *GigaVUE-OS CLI User's Guide*.

Messages Associated with Changing the admin Account Password

There are messages associated with changing the default password on the **admin** account since this password must be changed starting in software version 4.7.

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

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

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

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

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

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

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

For changing passwords and password polices, refer to [Changing Passwords and Setting Up Basic Accounts](#) on page 47 and [GigaVUE-OS Password Policies](#) on page 53.

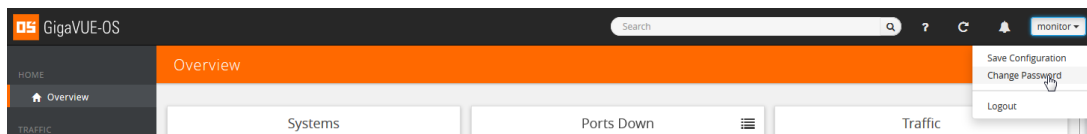
For best practices for other passwords, other than for the admin account, refer to [Best Practices for Passwords](#) on page 125.

Best Practices for Passwords

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

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

1. Log in to GigaVUE H-VUE as the **monitor** user.
2. Click on the **monitor** menu in the UI header and select **Change Password** as shown in the following figure.



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.

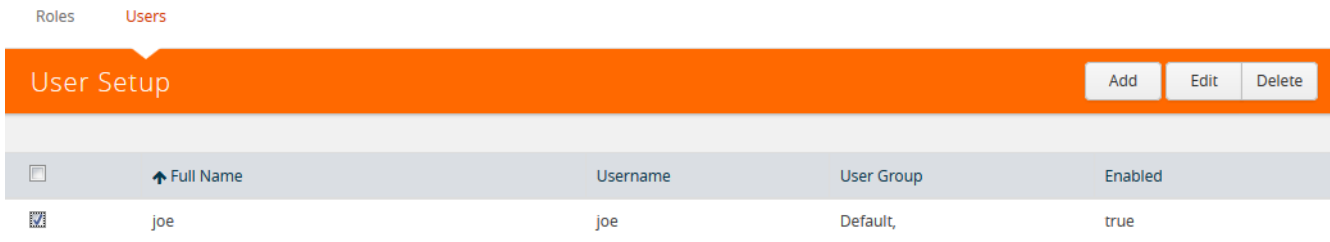
When entering the new password, the system displays “Invalid Password” underneath the New Password field until the password meets the password criteria described in [GigaVUE-OS Password Policies](#) on page 53.

4. Click **Save**.

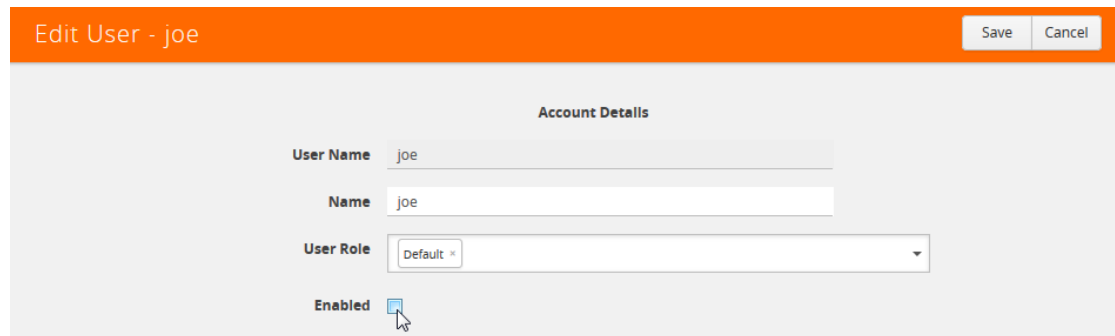
The system logs you out of the system to reset the password. To log in again as the monitor user, use the password created in [Step 3](#).

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** as shown in the following figure.

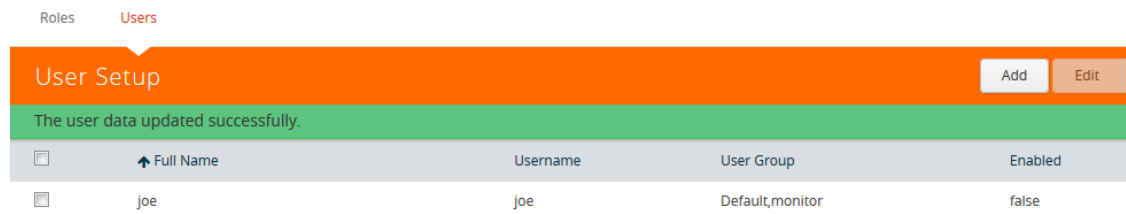


4. On the Edit User page, make sure the **Enable** checkbox is not selected as shown in the following figure.



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 as shown in the following figure.



User accounts that do not have passwords set can also be disabled. Refer to [Disallowing Login with a Blank Password](#) on page 117 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.

7 Licensing GigaVUE TA Series

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

- [Perpetual GigaVUE TA Series Licenses](#) on page 128
- [Applying Licenses for GigaVUE TA Series](#) on page 128

Perpetual GigaVUE TA Series Licenses

Table 7-1 lists perpetual licenses available on GigaVUE TA Series nodes.

Table 7-1: GigaVUE TA Series License Types

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

Applying Licenses for GigaVUE TA Series

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

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

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

On the GigaVUE-TA100, only the first 16 out of 32 100Gb ports are enabled. Two port licenses are available to enable an additional 8 or 16 ports to expand from 16 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 ports are enabled. A port license is available to enable an additional 32 ports.

To view all licenses assigned to a TA Series node, select **Settings > Config and Licenses**, from the navigation pane. Advanced Features Licenses will start with ADV while Ports licenses will have PRT in the license key. For all licenses, the **Expiration Date** column has the word Never to indicate that there is no expiration date as shown in [Figure 7-1](#). Evaluation licenses are currently not available for GigaVUE TA Series.

The screenshot shows the 'Config and Licenses' page for a system. The page is divided into several sections:

- Systems:** A dropdown menu showing '#1: QA-TA1-21 (normal)'.
- Navigation:** Tabs for Date and Time, Global Settings, Authentication, Interface, **Config and Licenses** (selected), and Reboot and Upgrade.
- System Information:** Host Name: QA-TA1-21, Hardware: AG-Chassis, Software: GigaVUE-OS 4.4.00 2015-07-14.
- Configurations:** A sub-tab for Licenses with an 'Install' button.
- Licenses Table:**

Box ID	Slot ID	Features	Parameters	Expiry
1		Advanced Features		never
10		Advanced Features		never
11		Advanced Features		never
12		Advanced Features		never
- Cards:** A table showing card information:

ID	Status	Type
1	●	AG-48X4Q

Figure 7-1: Page to Add and View License Keys

To view serial numbers, select **Chassis** from the Navigation pane, and then click **Table View**. The serial number is displayed in the **Serial Number** column under **Properties**. [Figure 7-2](#) shows the chassis properties for a GigaVUE-TA10.

The screenshot shows the 'Chassis Table View' for Box ID 1 - GigaVUE-TA10. The page has a navigation bar with buttons for Chassis View (selected), Table View, Transceiver View, Type View, Edit View, and Quick Port Editor.

Under the 'Properties' section, there is a table showing chassis information:

Chassis Id	Hardware Type	Hardware Revision	Product Code	Serial Number
D042A	TA10-Chassis	1.0	132-00CB	D042A

Figure 7-2: Chassis Properties in Chassis Table View

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

Moving a License between GigaVUE TA Series

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

System

This section provides information about the following:

- [Chassis](#) on page 133
- [Managing Roles and Users](#) on page 149
- [Reboot and Upgrade Options](#) on page 157
- [Backup and Restore](#) on page 167
- [Using SNMP](#) on page 173
- [Monitoring Utilization](#) on page 185

8 Chassis

The Chassis page provides a detailed snapshot of a selected H Series node, providing views of cards, control cards, and ports on the chassis. It is also possible to view information about individual cards or modules fan trays, and power modules.

This chapter covers the following topics:

- [Chassis View](#) on page 133

This section describes the following:

- [Chassis View + Transceiver View](#) on page 135
- [Chassis View + Port View](#) on page 136

- [Table View](#) on page 138

This sections describes the following:

- [Actions Menu](#) on page 140 for configure/reconfigure, start up/shut down, and changing mode on a selected card
- [Change Mode](#) on page 141 for setting the card mode on a GigaVUE-TA10 or GigaVUE-TA40
- [Change Port Mode](#) on page 143 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 8-1 on page 134](#). Chassis View includes two types of views. Port View and Transceiver View. Transceiver View is the default view.

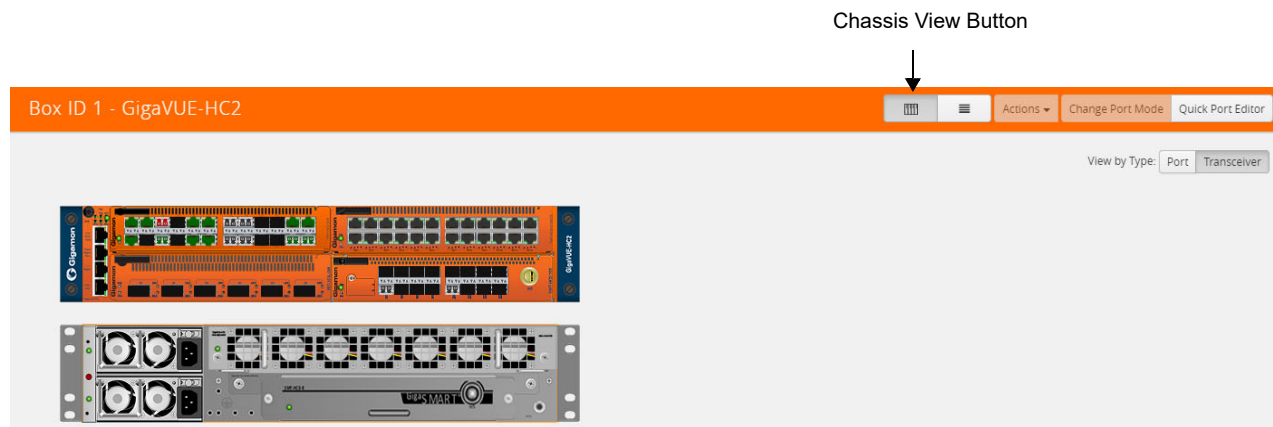


Figure 8-1: Chassis View

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 8-2 on page 134](#) shows an example.

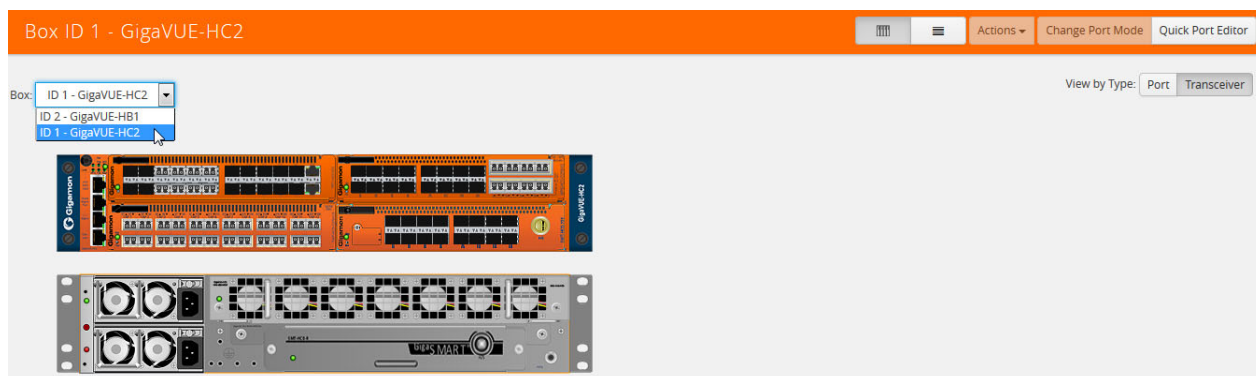


Figure 8-2: Chassis View of Node in a Cluster

From the Chassis page, you can select the following:

- Chassis View + Transceiver View
For details, refer to [Chassis View + Transceiver View](#) on page 135.
- Chassis View + Type View
For details, refer to [Chassis View + Port View](#) on page 136.
- Table View
For details, refer to [Table View](#) on page 138.

NOTE: For GigaVUE-HB1 and GigaVUE-TA1, you will only see one card allocation because these are non-modular nodes.

[Figure 8-3 on page 135](#) and [Figure 8-4 on page 135](#) show some examples of chassis displayed on the Chassis page.



Figure 8-3: Chassis View—HC2

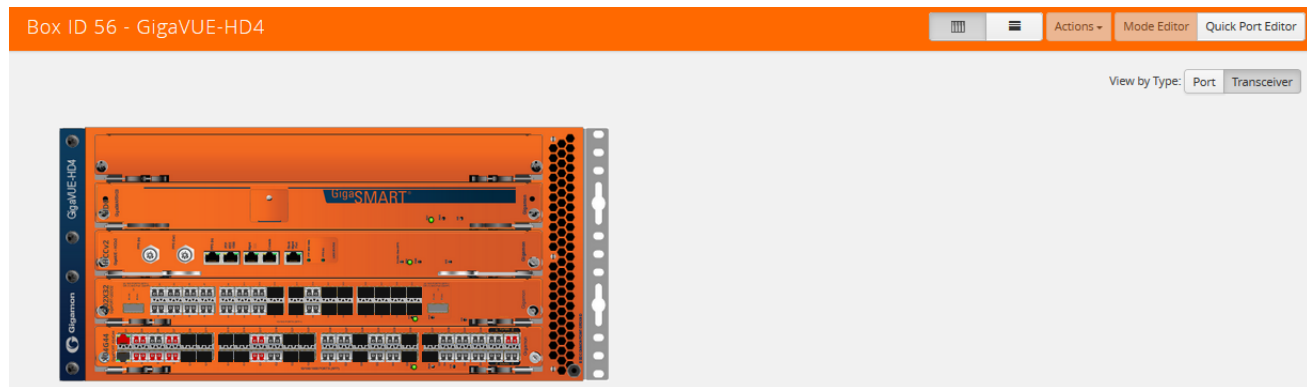


Figure 8-4: Chassis View—HD4

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](#) on page 137.

Chassis View + Transceiver View

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

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

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

Figure 8-5 shows an example of a Chassis + Transceiver View.

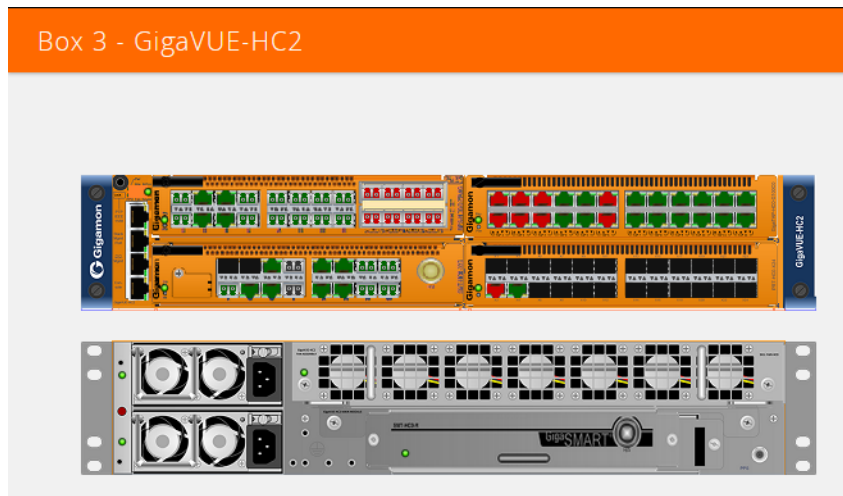


Figure 8-5: Chassis + Transceiver View

In Chassis + Transceiver View, the port type and port ID is displayed by hovering over the ports in the graphic.

Some chassis support fanout of ports, such as the GigaVUE-TA100. When fanout is used, the fanout is displayed on the Chassis page as shown in Figure 8-6 on page 136.

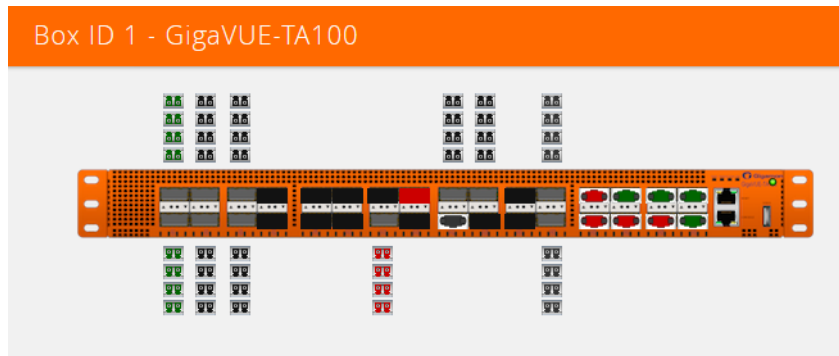


Figure 8-6: Chassis + Transceiver View with Fanout Ports

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 8-5 on page 136. 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.

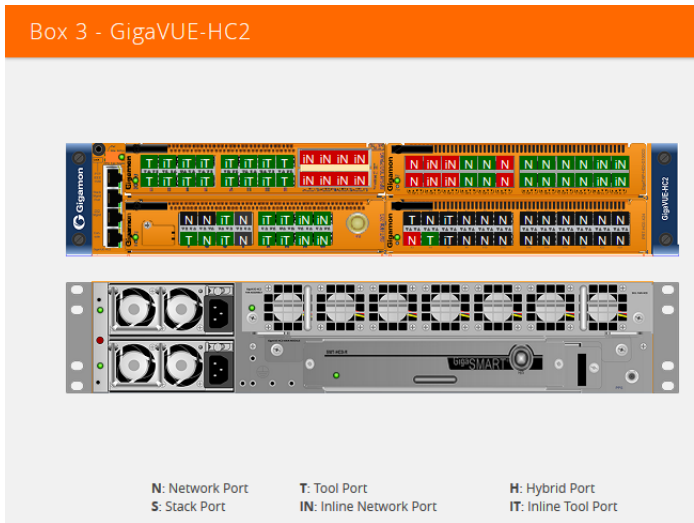


Figure 8-7: Chassis View + Type View

Line Card and Module Numbering

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

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

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

When displaying ports in Chassis View (and H-VUE), the format is box ID/slot ID/port ID. For example, 1/1/x6 refers to box 1, slot 1, port X6.

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

- **GigaVUE-HD8**: Slots are numbered 1-8 from left to right and do not count the two control card slots in the middle of the chassis.
- **GigaVUE-HD4**: Slots are numbered 1-4 from bottom to top and do not count the control card slot in the middle of the chassis

- **GigaVUE-HC1:** Bays are numbered as follows:
 - the base chassis in the center, is numbered 1
 - the left module is numbered 2
 - the right module is numbered 3
- **GigaVUE-HC2:** Bays are numbered 1-4 from left upper, left lower, right upper to right lower.
- **GigaVUE-HC3:** Bays are numbered 1-4 from left upper, left lower, right upper to right lower.

Table View

The Table View selection shows the H Series or TA Series node as a table of the node properties with line card/module information, environment information (temperature and voltage), available power supplies, fan trays, and fan RPM. The health status of these is also indicated in Table View for cards, Power Supplies, and Fan Trays.

[Figure 8-8 on page 139](#) shows an example of the Table View. For GigaVUE-HC2s, the Cards section also displays information about the main board, indicating whether it is in normal or 100G mode if it is equipped with Control Card version 2 (HC2 CCv2) AND 100G modules, PRT-HC0-C02. For GigaVUE-HC1, the Environment section includes a column that shows the GigaSMART CPU Temperature. To select Table View, click the Table View button.

Table View Button

Chassis Id	Hardware Type	Mode	Hardware Revision	Product Code	Serial Number
C0036	HC2-Chassis	normal	A0	132-00AZ	C0036

Slot Id	Hardware Type	Configured	Status	Hardware Revision	Product Code	Serial Number
cc1	HC2-Main-Board	✓	●	3.2-24	132-00AN	1AN0-0056
1	PRT-HC0-X24	✓	●	A1-a2	132-00BD	1BD0-04FF
2	PRT-HC0-Q06	✓	●		132-00BE	
3	TAP-HC0-G100C0	✓	●	B0-a8	132-00B3	1B30-0028
4	SMT-HC0-X16	✓	●	1.5-2	132-00BK	1BK0-0021
5	SMT-HC0-R	✓	●	3.0-5	132-00AT	1AT0-0029

Slot Id	Hardware Type	Board (°C)	Exhaust (°C)	Intake (°C)	2.5v	3.3v	5.0v	12v	vccp1	vccp2
cc1	HC2-Main-Board	-	37	29	2.496	3.25	4.836	11.687	1.24	1.184
1	PRT-HC0-X24	29	-	-	-	3.25	-	11.687	1.17	1.254
3	TAP-HC0-G100C0	34	-	-	2.457	3.233	-	11.75	1.17	0
4	SMT-HC0-X16	39	-	-	2.47	3.268	4.94	11.75	1.269	1.226
5	SMT-HC0-R	31	-	-	2.314	3.268	4.94	11.687	1.297	1.522

Power Module Id	Hardware Type	Top Status	Bottom Status	Hardware Revision	Product Code	Serial Number
-----------------	---------------	------------	---------------	-------------------	--------------	---------------

Figure 8-8: Chassis Table View for a Gigamon HC2 CCv2

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

Chassis Information	Description
Properties	Provides information about the chassis: Chassis ID, Hardware Type, Mode, Hardware Revision, Product Code, and Serial Number. NOTE: Click on the Box ID to view the Fabric Hash setting for the chassis. For a GigaVUE-HC2 CCv2, the Mode field displays either Normal or 100G when 100Gb is enabled on the PRT-HC0-C02 module.
Cards	Describes the cards installed in each slot of the chassis. This section includes the current health status of each card. Selecting a check box next to a card allows you to perform various actions on the card with the Actions menu. For details refer to Actions Menu on page 140.
Environment	Provides temperature information about the main board and cards in the chassis.

Chassis Information	Description
Power Supplies	<p>Describes the power supply modules installed in the chassis. This section also includes the current health status of each module.</p> <p>For a Gigamon HC-2 node, the health status of both the top and bottom modules.</p> <p>For a GigaVUE-HC3 node, the Power Supplies section includes Power Management. Refer to <i>GigaVUE-HC3 Hardware Installation Guide</i> for details.</p> <p>NOTE: Click on the Power Module ID to view the PSU diagnostic attributes in a Quick View.</p>
Fan Trays	Describes the fan trays installed in the chassis. This section also including the current health status of each tray.
Fan RPM	Provides the current RMP of the each fan.

Actions Menu

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

Action	Description
Configure	Selecting this action sets the port and traffic settings for the system.
Unconfigure	Selecting this action for a card removes all port and traffic settings for the system.
Enable/Disable Gigamon Discovery	Used to enable/disable Gigamon Discovery protocol
Fabric Advance Hash	Used to configure fabric advanced hashing parameters for stack GigaStreams and GigaSMART groups. For details, refer to Fabric Advance Hashing on page 146
Start Up	Selecting this action reboots the card.
Shut Down	Selecting this action shuts down the card.
Change Mode	Used for setting card mode on a GigaVUE-TA1, GigaVUE-TA10, or GigaVUE-TA40 node. For more details, refer to Change Mode on page 141
Enable Fabric Hash	Used for improving packet distribution on PRT-H00-Q02X32 and PRT-HD0-Q08 line cards. For details, refer to Enabling Advanced Fabric Hashing on page 145

Reloading a GigaSMART Line Card or Module

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

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

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

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

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

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

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

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

Change Mode

The Actions menu has a **Change Mode** selection that is used to set the card mode on GigaVUE-TA1, GigaVUE-TA10 and GigaVUE-TA40 nodes. On the GigaVUE-TA1, GigaVUE-TA10, you can configure card modes that let either two (q1..q2) or all four (q1..q4) of the 40Gb ports operate as four logical 10Gb ports (x49..x64). On the GigaVUE-TA40, you can also configure card modes that let either of the 40Gb ports operate as four logical 10Gb ports (x1..x4). Changing the card mode is useful when deploying the GigaVUE-TA10 or the GigaVUE-TA40 in an environment that does not yet include 40Gb interfaces.

Once a 40Gb port has been configured to operate as four 10Gb ports, you will need to cable it to a breakout panel, such as PNL-M341. The breakout panel takes a 40Gb QSFP+ input from a GigaVUE-TA10 or GigaVUE-TA40 and splits it to four independent 10Gb output ports. For details on breakout panel connections, refer to the *GigaVUE TA Series Hardware Installation Guide*.

Changing the card mode resets all port and packet distribution settings, therefore, set the card mode during the initial configuration.

Configuring the Card Mode on a GigaVUE-TA1 or GigaVUE-TA10

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

- **48x** (default) – Four 40Gb ports (q1..q4) and 48 10Gb ports (x1..x48)
- **56x (use with breakout panel or breakout cables)** – Two 40Gb ports (q3..q4) and 56 10Gb ports. Port q1 is used as x49..x52 on the breakout panel. Port q2 is used as x53..56 on the patch panel.

- **64x (use with breakout panel or breakout cables)** – 64 10Gb ports (x1..x64). Port q1..q4 are connected at the breakout panel as follows:
 - **q1** – x49..x52
 - **q2** – x53..x56
 - **q3** – x57..x60
 - **q4** – x61..x64

To specify card modes use the following procedure:

1. Deconfigure the card by doing the following:
 - a. Switch to Table View by clicking the Table View button.
 - b. Under Cards, select the card to deconfigure. This activates the **Actions** menu.
 - c. Select **Actions > Unconfigure**.

NOTE: This removes all port and traffic settings for the system.
2. To set the new card mode for a GigaVUE-TA1 or GigaVUE-TA10:
 - a. Select **Actions > Change Mode**
 - b. For **Mode**, select 48x, 56x, or 64x.
The settings for each available mode are summarized in [Table 8-1](#).
 - c. Click **Save**.
3. Configure the card by selecting **Actions > Configure**.

Table 8-1: 40Gb Port Settings by Card Mode on GigaVUE-TA10

Card Mode	Physical 40Gb Interface on GigaVUE-TA10			
	q1	q2	q3	q4
48x (default)	40Gb (q1)	40Gb (q2)	40Gb (q3)	40Gb (q4)
56x	10Gb (x49..x52)	10Gb (x53..x56)	40Gb (q3)	40Gb (q4)
64x	10Gb (x49..x52)	10Gb (x53..x56)	10Gb (x57..x60)	10Gb (x61..x64)

Notes on GigaVUE-TA10 Card Modes

- The default card mode is 48x.
- When a 40Gb port is used as four 10Gb ports, removing the QSFP+ will affect the connections for all four 10Gb ports. For example, removing the QSFP from q1 results in a loss of signal event for x49..x52.
- The q1..q4 40Gb ports include a single link LED on the GigaVUE-TA10 faceplate. When a physical 40Gb interface is used as four 10Gb ports, the 40Gb port LED indicates the status of the *first* of the four 10Gb ports on the breakout panel (for example x49 in the x49..x52 group, x53 in the x53..x56 group, and so on). The other three ports in the group do not affect the link LED for the 40Gb port on the GigaVUE-TA10 faceplate.

Once the card mode has been configured, make the breakout panel connections. For details, refer to the *GigaVUE TA Series Hardware Installation Guide*.

Change 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 8-9 on page 144](#) displays.

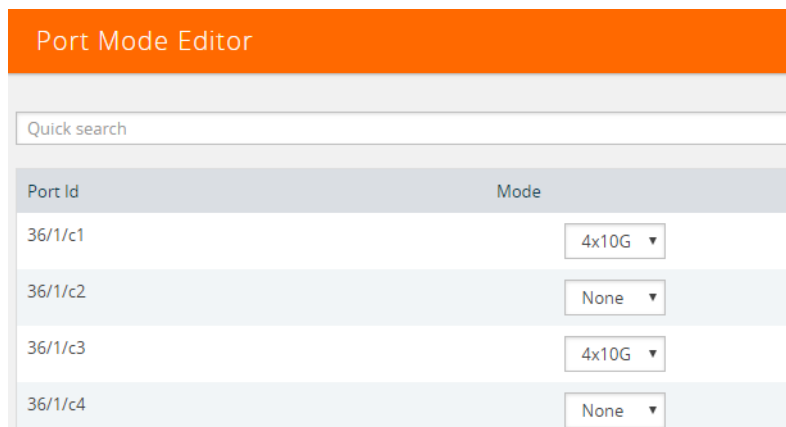


Figure 8-9: Port Mode Editor

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 as shown in the [Figure 8-10 on page 144](#).

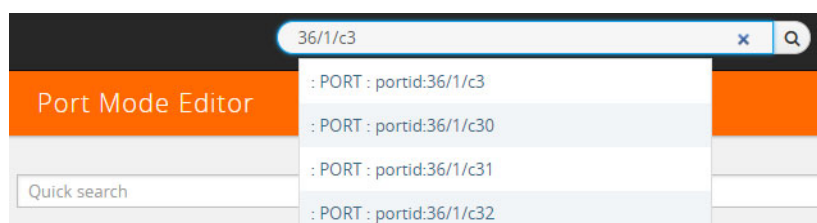


Figure 8-10: Quick Search Results

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 8-11 on page 145. In Figure 8-11, the ports that are set to **4x10G** show four additional ports.

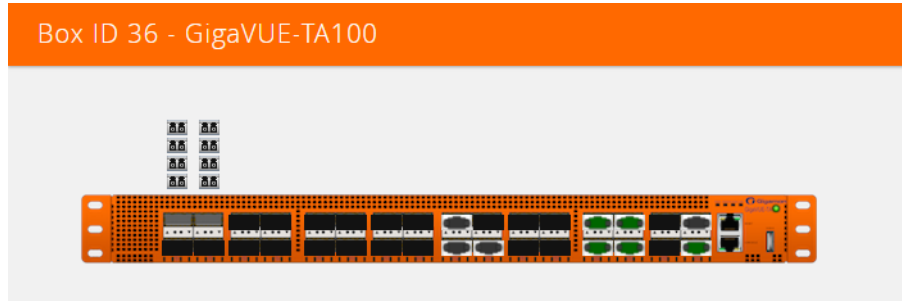


Figure 8-11: Breakouts Displayed on a GigaVUE-TA100 Chassis

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*.

Enabling Advanced Fabric Hashing

The Enable Fabric Hash option is used to enable advanced fabric hashing on a specified card and slot. It only applies to GigaVUE-HD4 and GigaVUE-HD8 nodes with traffic coming into PRT-H00-Q02X32 and PRT-HD0-Q08 line cards. For example, if traffic comes into two PRT-HD0-Q08 line cards and then is sent out to four GigaSMART engines on two GigaSMART cards, configuring advanced fabric hashing on both the PRT-HD0-Q08 line cards improves GigaSMART performance.

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

1. Select **Chassis** in the main navigation pane.
2. Switch the Chassis page to Table View.
3. Under **Cards**, find the line card on which you want to enable fabric hash and select the card. The **Fabric Hash** field for the card indicates the current state of fabric hash. In Figure 8-12 on page 146, fabric hash is disabled on the selected line card.

Box ID 1 - GigaVUE-HD8							Actions	Change Port Mode	Quick Port Editor
▼ Properties									
Chassis Id	Hardware Type	Mode	Hardware Revision	Product Code	Serial Number				
80092	HD8-Chassis	normal	A3	132-0098	80092				
▼ Cards									
<input type="checkbox"/>	Slot Id	Hardware Type	Configured	Fabric Hash	Status	Hardware Revision	Product Code	Serial Number	
<input type="checkbox"/>	1	GigaPORT-X04G44	✓	N/A	●	E1-a2	132-0046	1460-0422	
<input type="checkbox"/>	3	GigaPORT-X12G04	✓	N/A	●	C2-a6	132-0045	1450-0245	
<input checked="" type="checkbox"/>	4	GigaPORT-Q02X32/2q	✓	Disabled	●	B5-a2	132-0087	1870-1914	

Figure 8-12: Fabric Hash Disabled on a PRT-H00-Q02X32 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.

In Figure 8-13, Enable Fabric Hash is selected, where fabric hash is currently disabled on the selected card.

Box ID 1 - GigaVUE-HD8							Actions	Change Port Mode	Quick Port Editor
▼ Properties									
Chassis Id	Hardware Type	Mode	Hardware Revision	Product Code	Serial Number				
80092	HD8-Chassis	normal	A3	132-0098	80092				
▼ Cards									
<input type="checkbox"/>	Slot Id	Hardware Type	Configured	Fabric Hash	Status	Hardware Revision	Product Code	Serial Number	
<input type="checkbox"/>	1	GigaPORT-X04G44	✓	N/A	●	E1-a2	132-0046	1460-0422	
<input type="checkbox"/>	3	GigaPORT-X12G04	✓	N/A	●	C2-a6	132-0045	1450-0245	
<input checked="" type="checkbox"/>	4	GigaPORT-Q02X32/2q	✓	Disabled	●	B5-a2	132-0087	1870-1914	

Figure 8-13: Enable Fabric Hash Selected

Fabric Advance Hashing

Fabric Advance Hashing is used to enable advanced fabric hashing on a chassis in GigaStream stack links and GigaSMART groups. The Fabric Advance Hash option lets

you select the criteria for sending matching flows to the same destination port within stack links.

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

Fabric advanced hashing applies to the following modules:

- GigaVUE-HC1
- GigaVUE-HC2
- GigaVUE-HC2+
- GigaVUE-HC3-v1
- GigaVUE-HC3-v2
- GigaVUE-TA40
- GigaVUE-TA100
- GigaVUE-TA200

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

1. Select **Chassis** in the main navigation pane.
2. Switch the Chassis page to Table View.
3. Select the **Box ID** under Properties and select **Actions**.
4. Select the required **Fabric Advance Hash** type from the drop-down.



Figure 8-14: Fabric Advance Hash

5. The following options are available:
 - **All:** Selects all criteria
 - **Default:** Sets the fabric advanced hash algorithm to its default settings
 - **None:** Clears all fields from advanced hash
 - **Fields:** Allows you to select the required fields for advanced hash.

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

9 Managing Roles and Users

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

- [About Role-Based Access](#) on page 149
- [Configuring Role-Based Access and Setting Permissions in H-VUE](#) on page 151

About Role-Based Access

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

For more detailed information related to role-based access, refer to the following sections:

- [Role-Based Access and Flow Mapping](#) on page 149
- [Locks and Lock Sharing](#) on page 149
- [Role-Based Access: Rules and Notes](#) on page 150

Role-Based Access and Flow Mapping

Flow Mapping allows different users to share network ports. Because Flow Mapping sends a packet matching multiple maps to the destination specified by the map with the highest priority, you must exercised caution when adjusting maps on shared network ports. Administrators can change the priority of maps to ensure that packets are sent to the desired destination.

Permission can also be associated with maps based on roles. For more information about map permissions, refer to [Setting Map-Sharing Permission Levels](#) on page 155

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 [Setting Locks and Lock-Shares](#) on page 154.

Role-Based Access: Rules and Notes

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

- [User Management](#) on page 150
- [Role Management](#) on page 150
- [Port Ownership](#) on page 151

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 [Removing a Lock from a User's Port](#) on page 154.
- To remove a user's lock-share, refer to [Removing a User's Lock-Share](#) on page 154.
- Administrators can also lock a port for a user. Refer to [Locking a Port for a User](#) on page 155.
- The admin role automatically has Level 4 permissions to all ports. The admin role cannot be assigned to any port.

Configuring Role-Based Access and Setting Permissions in H-VUE

Configuring RBAC in H-VUE consists of the following tasks:

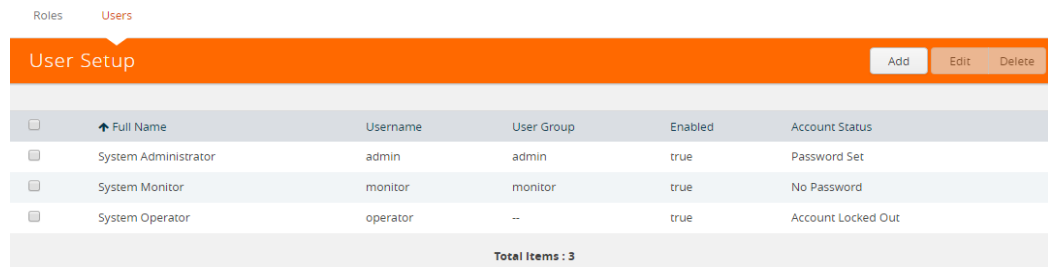
- [Adding Users](#) on page 151
- [Creating Roles](#) on page 152
- [Associating Roles with Port Permissions](#) on page 153
- [Setting Locks and Lock-Shares](#) on page 154
- [Setting Map-Sharing Permission Levels](#) on page 155

Adding Users

This section describes provides the steps for adding users to H-VUE. Users are also assigned to roles that set there access permissions. For the step to create roles, refer to [Creating Roles](#) on page 152.

To add users to H-VUE, do the following:

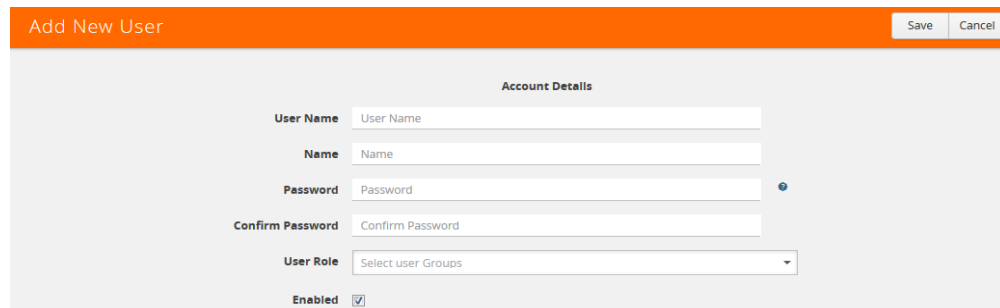
1. Select **Roles and Users > Users**. The **User Setup** page displays.



<input type="checkbox"/>	Full Name	Username	User Group	Enabled	Account Status
<input type="checkbox"/>	System Administrator	admin	admin	true	Password Set
<input type="checkbox"/>	System Monitor	monitor	monitor	true	No Password
<input type="checkbox"/>	System Operator	operator	--	true	Account Locked Out

Total Items : 3

2. Click **Add**. The **Add New User** page displays.



3. On the Add New User page, do the following:
 - Enter a user name for this account in **User Name** field.
 - Enter the user's actual name in the **Name** field.
 - Enter a password for the user in the **Password** field and in the **Confirm Password** field.
 - Assign a role to the user by clicking in **Capability** field and selecting a role from the drop-down list. For the steps to create a role, refer to [Creating Roles](#) on page 152.
4. Select **Enable** to enable the user's account, and then click **Save**.

Creating Roles

This section describes the steps for creating roles and assigning user to those roles. Before creating roles, refer to [About Role-Based Access](#) on page 149. However, H-VUE has three built-in roles for specifying which users have access to a given port. These roles are:

- **Admin**

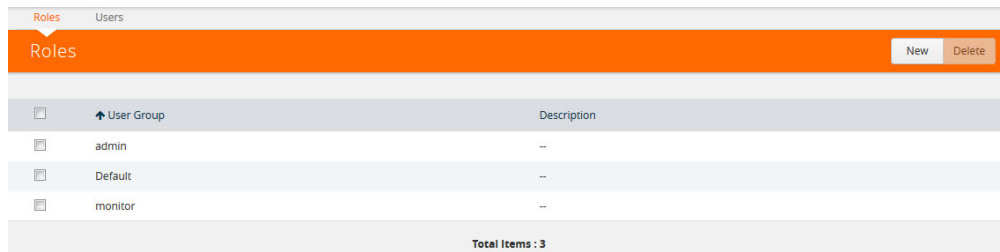
This role provides access to all command modes, including Standard, Enable, and Configure. Admin users also have access to all commands and all ports. They are also members of all groups.
- **Default**

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**

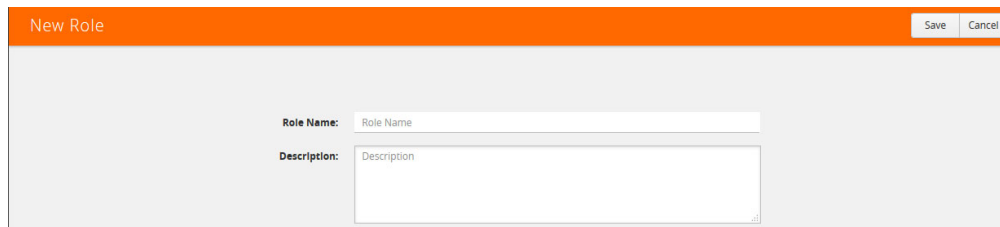
This role provides view-only access to ports and configurations. Administrators create additional custom *roles* and assign them to users together with the Default role. For example, if you create a role named `Security_Team` and assign it to tool port `5/1/x2`, users assigned the `Security_Team` role 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 H-VUE. Users can have multiple assigned roles, allowing administrators to fine-tune access to the Visibility Platform.

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

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



2. Click **New**.
3. On the **New Role** page, do the following:
 - Enter a role in the **Role Name** field. For example, Security_Team.
 - (Optional) Enter a description of the role in the **Descriptions** field.



4. Click **Save**.
5. Add users to the role. Refer to [Adding Users](#) on page 151.

Associating Roles with Port Permissions

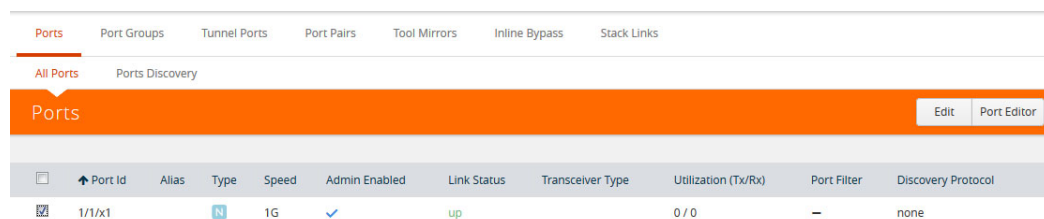
Users are assigned roles based on their user group. Each user group is given permission to specific ports on the node. There are four port-based permission levels, which are as follows:

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.



<input type="checkbox"/>	Port Id	Alias	Type	Speed	Admin Enabled	Link Status	Transceiver Type	Utilization (Tx/Rx)	Port Filter	Discovery Protocol
<input checked="" type="checkbox"/>	1/1/x1		N	1G	✓	up		0 / 0	-	none

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

Setting Locks and Lock-Shares

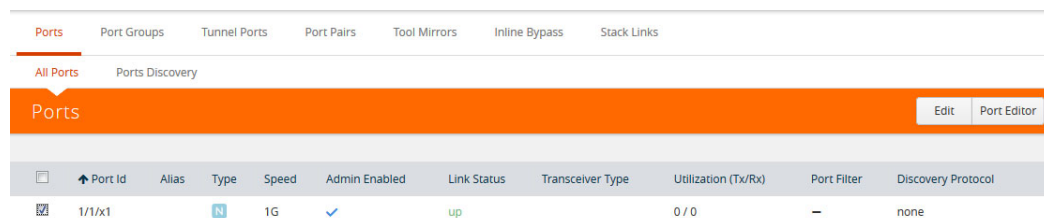
This section provides the procedures for setting port locks and lock-sharing. Before doing these procedures, refer to [Locks and Lock Sharing](#) on page 149. The procedures for setting lock and lock-sharing in H-VUE are:

- [Removing a Lock from a User's Port](#) on page 154
- [Removing a User's Lock-Share](#) on page 154
- [Locking a Port for a User](#) on page 155

Removing a Lock from a User's Port

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

1. Select **Ports** in the Navigation pane, then go to **Ports > All Ports**.
2. Select the port on which you want to remove a lock.



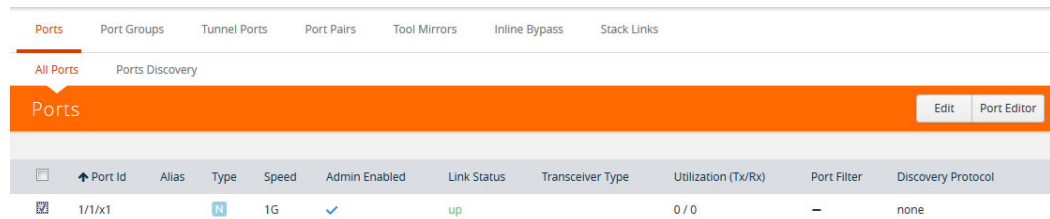
<input type="checkbox"/>	Port Id	Alias	Type	Speed	Admin Enabled	Link Status	Transceiver Type	Utilization (Tx/Rx)	Port Filter	Discovery Protocol
<input checked="" type="checkbox"/>	1/1/x1		N	1G	✓	up		0 / 0	-	none

3. Click **Edit**.
4. Clear the **Lock Port** check box.

Removing a User's Lock-Share

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

1. Select **Ports** in the Navigation pane, then go to **Ports > All Ports**.
2. Select the port or ports on which you want to remove a lock-share.

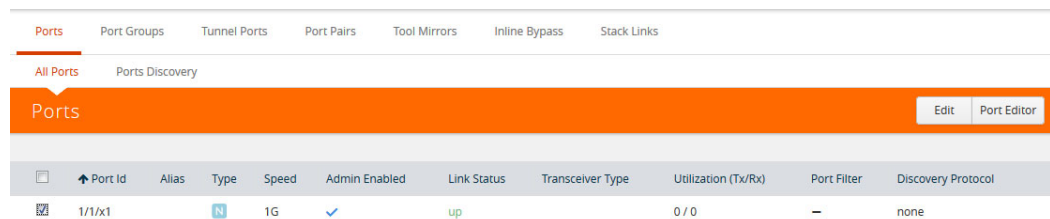


3. Click **Edit**.
4. Click on the **Lock shared with Users** field and remove the user.
5. Click **Save**.

Locking a Port for a User

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

1. Select **Ports > Ports > All Ports**.
2. Select the port or ports on which you want to remove a lock.



3. Click **Edit**.
4. Select **Lock Port** if it is not already selected.
5. Click on the **Lock shared with Users** field and add the user.

Setting 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.

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

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**.

<input type="checkbox"/>	↑ Alias	Comments	Type	Sub Type	Source	No of Rules	GSOP	Priority	Access Level	Destination
<input checked="" type="checkbox"/>	collector		regular	collector	1/1/x11	0			admin	1/1/x7

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.

10 Reboot and Upgrade Options

This section describes how to upload and upgrade images on GigaVUE nodes. For more detailed instructions on the upgrade paths available, refer to the *GigaVUE H Series Upgrade Guide* and *GigaVUE TA Series Upgrade Guide*. The major sections include:

- [Rebooting Nodes](#) on page 157
- [Upgrading Software](#) on page 158
- [Working with Configuration Files in the Configurations Page](#) on page 163

Rebooting Nodes

Use the Reboot page to reboot the node. The reboot steps are as follows:

1. Using administrator user credentials, log in to H-VUE for the node to reboot.
2. Select **Settings > Reboot and Upgrade > Reboot**. The Reboot page displays as shown in [Figure 10-1](#).

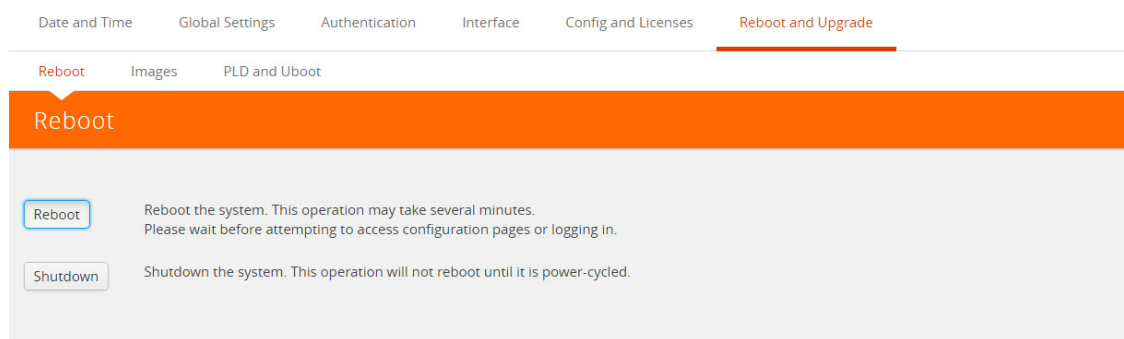


Figure 10-1: Reboot Page

3. Click **Reboot**. A dialog will appear asking if you want to proceed.
4. To reboot the node, do either of the following:
 - **Reboot**
If no changes have been made to the current configuration, the dialog shown in [Figure 10-2](#) appears. Click **OK** to reboot the node.

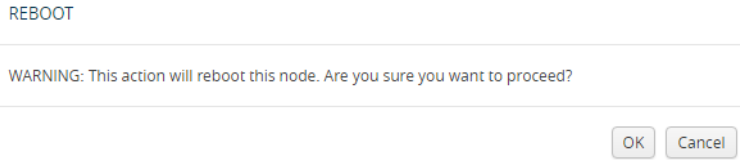


Figure 10-2: Reboot Dialog

- Save the configuration and reboot

If there are any changes to the current configuration, the reboot dialog displays a warning that current configuration has been modified as shown in [Figure 10-3](#). Click **Save and Reboot** to save the configuration before reboot.

Note: If you click Reboot, the configuration will not be saved and any changes to the configuration will be lost after reboot.

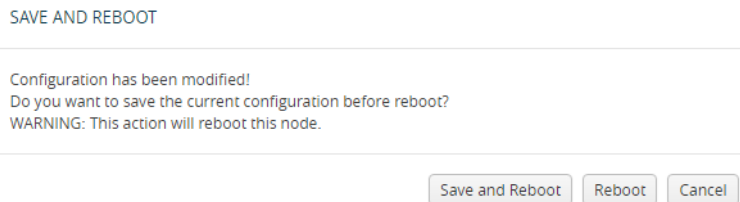


Figure 10-3: Save and Reboot

A dialog displays indicating that the running configuration was saved and system reboot initiated successfully. Click **OK**. When the login page appears, you can log back in.

Upgrading Software

This section provides the steps for upgrading the software version on a standalone GigaVUE node.

In a cluster configuration, if you try to update the software through H-VUE, the following message is displayed across the Images tab:

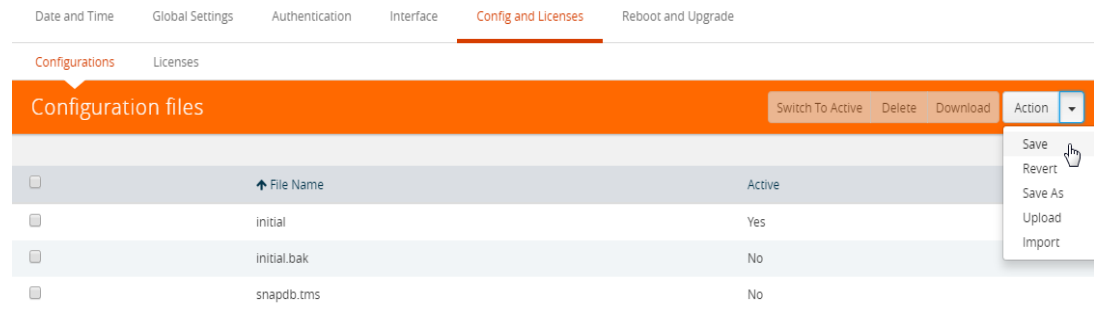
```
This is just a WARNING. It is recommended that you use the CLI to upgrade software on the GigaVUE H Series nodes when in a cluster.
```

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

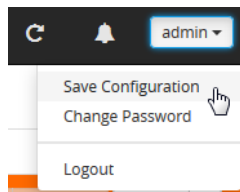
Saving the Configuration

Before upgrading the software, save your currently running configuration by doing the following:

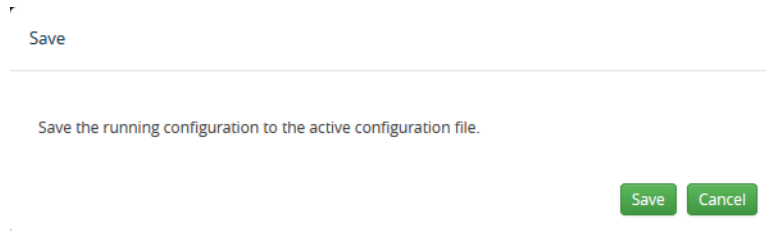
1. Select **Setting > Config and Licenses > Configurations > Actions**.
2. Select **Action > Save** menu as shown in the following figure.



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:



Upgrading the Software

Use the following steps to upgrade the software:

1. Access the GigaVUE node using a Web browser and log in with administrator user credentials.
2. Select **Settings > Reboot and Upgrade > Images**.

The Images page shows the currently installed images and indicates the which image will boot next. [Figure 10-4](#) shows an example where three images are currently installed. To change the image that will boot next select, **Action > Switch Boot Partition**.

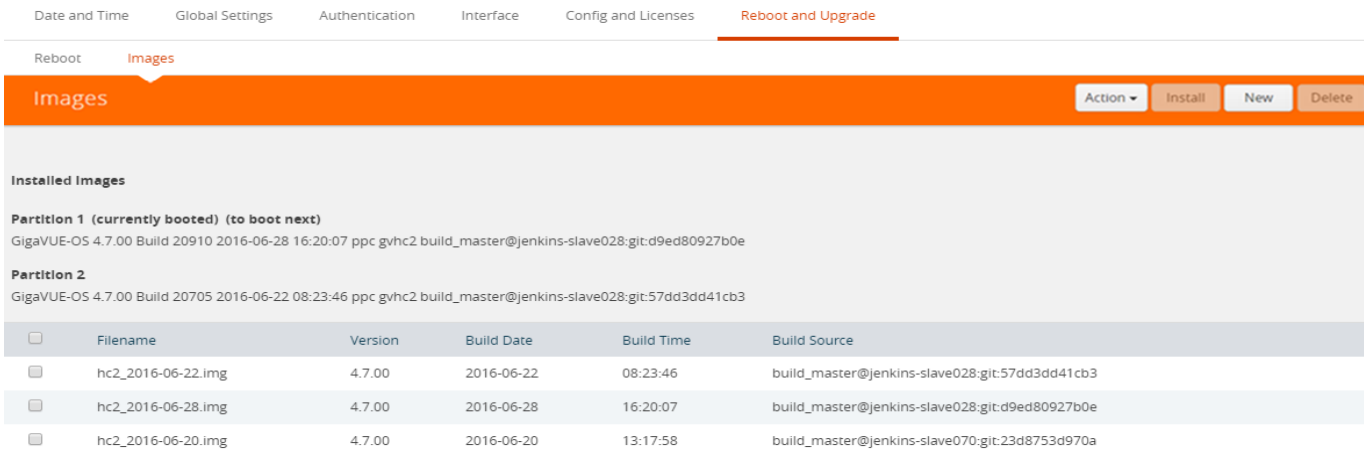


Figure 10-4: Active Images Page Showing Both Partitions

3. Remove all the currently uploaded images.
 - a. As shown in Figure 10-5 on page 160, select the check boxes.
 - b. Click **Delete**.

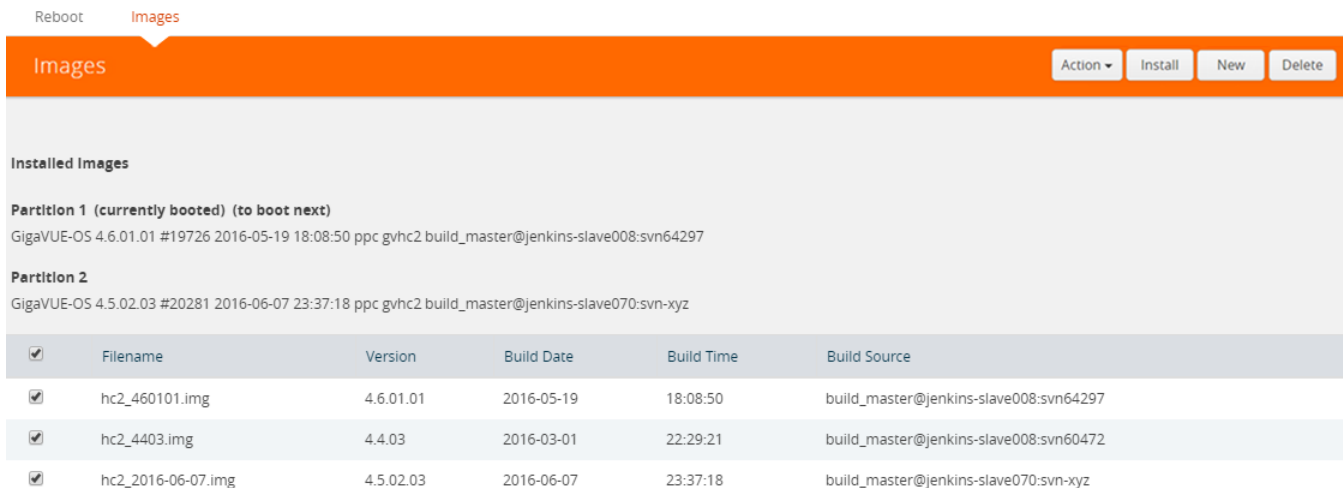


Figure 10-5: All Image Files Selected

4. On the Images page, click **New** to access a new application image. The Install New Image page displays as shown in Figure 10-6.

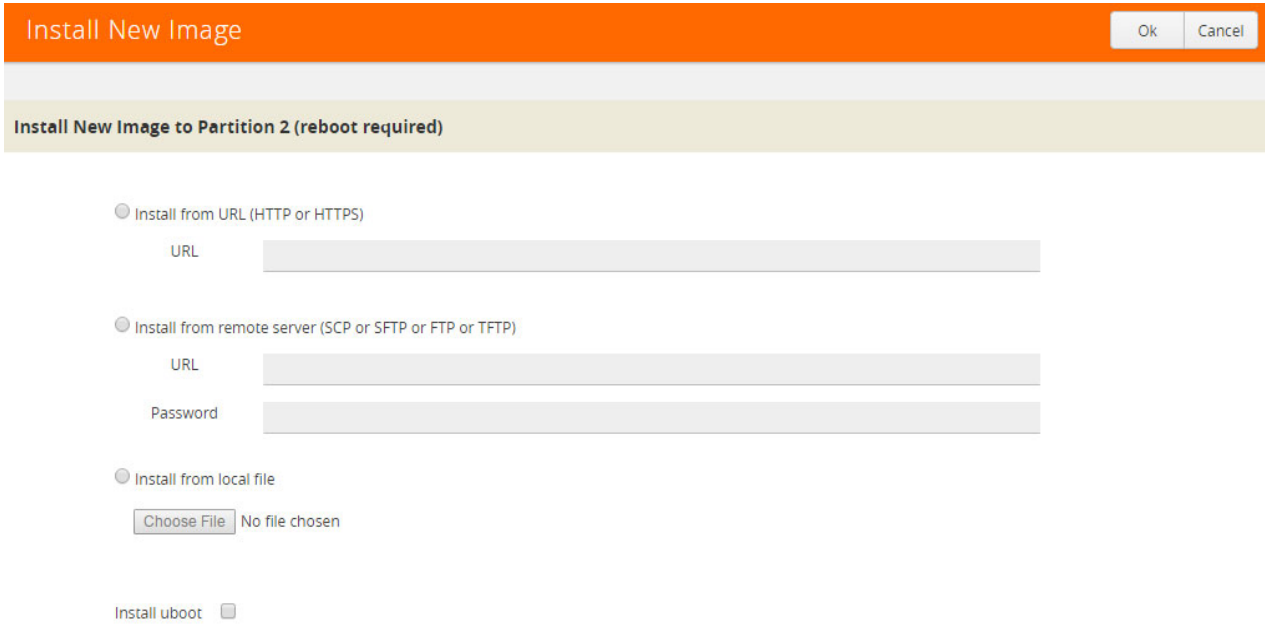


Figure 10-6: Install a New Image Page

5. Select the method for installing the new image, which is one of the following:

- **Install from URL** — Enter the URL from which to fetch the image.
- **Install from scp or sftp** — Enter the URL and password of the SCP or SFTP server from which to fetch the image.
- **Install from local file** — Use this option to upload the image file from your local environment. Click **Choose File** to select the file.

NOTE: The image must match the type of control card system (for example, HCCv2, GigaVUE-HB1, GigaVUE-TA1, or GigaVUE-HC2).

In [Figure 10-7](#), a local file is selected for the install.

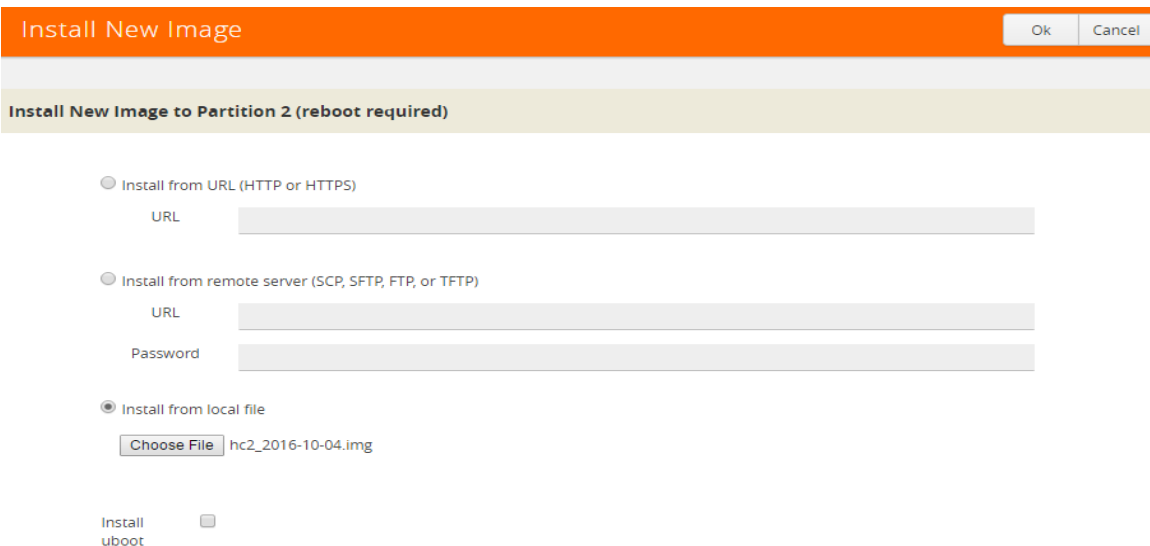


Figure 10-7: Local File Selected for Install

6. Click **OK** after the software path is selected. A progress bar appears below the title bar.
The new software is uploaded and installed. It is then active upon the next reboot.
7. To make the image effective, reboot the system.
Refer to [Rebooting Nodes](#) on page 157 for the steps to reboot the system.

Upgrading Uboot and PLD

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

1. Access the GigaVUE node using a Web browser and log in with administrator user credentials.
2. Select **Settings > Reboot and Upgrade > PLD and Uboot**.

[Figure 10-8](#) shows two check boxes.

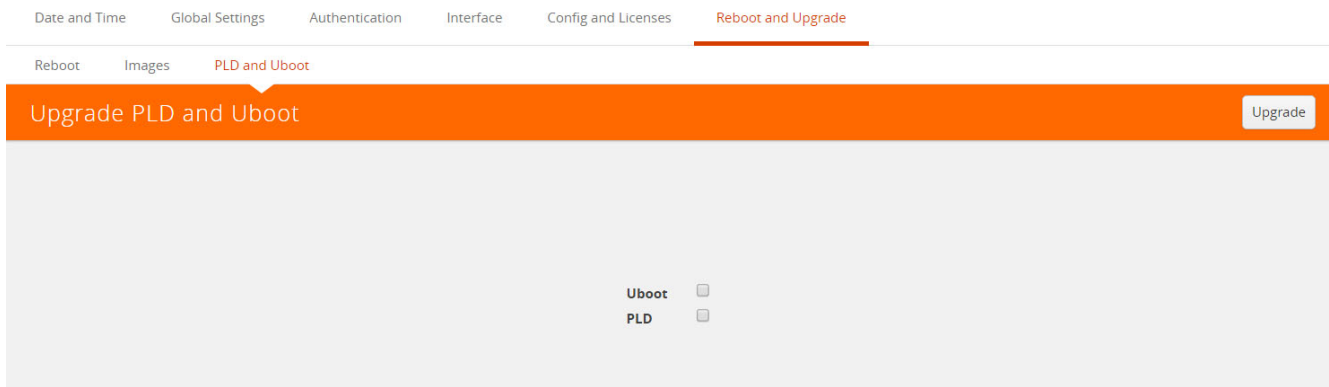


Figure 10-8: Upgrade PLD and Uboot

3. For Uboot upgrade, check **Uboot** to upgrade to a new Uboot version, then click **Upgrade**.
4. For PLD upgrade, check **PLD** to upgrade Programmable Logic Devices (PLDs) such as Field Programmable Gate Arrays (FPGAs) on GigaVUE-HC3 nodes.

[Figure 10-9](#) shows the slots and the control card that can be upgraded.

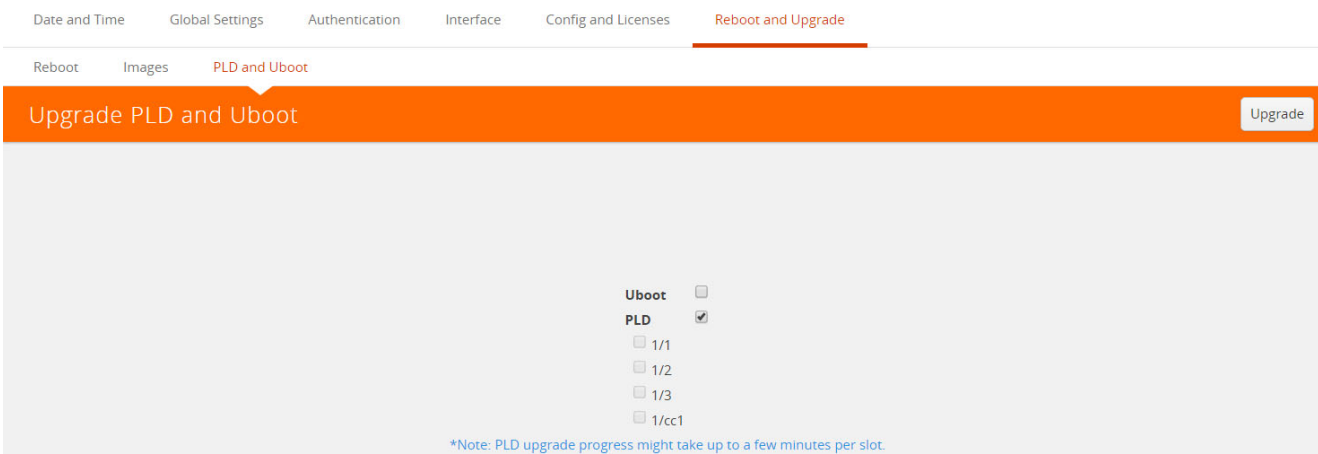


Figure 10-9: Slots and Control Card for PLD Upgrade

5. Select the slot, then click **Upgrade**.

Working 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 10-10.

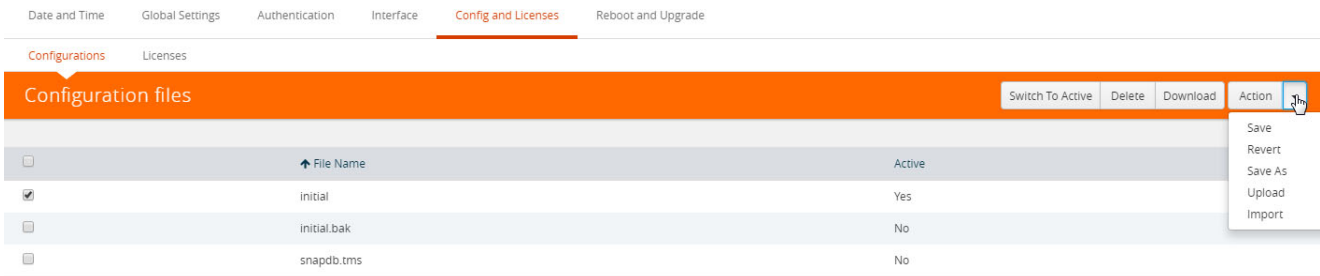


Figure 10-10: Configuration Files Page

The following sections describe how to set the options:

- [Configuration File Options](#) on page 163
- [Configuration Actions](#) on page 163
- [Uploading a Configuration](#) on page 164
- [Importing a Configuration](#) on page 164

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](#) on page 163.

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 [Uploading a Configuration](#) on page 164.
- Click **Action > Import** to import a configuration file. For details, refer [Importing a Configuration](#) on page 164.

Uploading a Configuration

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

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

Upload

Upload local binary file:

No file chosen

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

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

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

Importing a Configuration

To retrieve a saved configuration file from a remote host, using HTTP, HTTPS, SCP, SFTP, FTP, or TFTP, do the following:

1. Select the **Action > Import**. The Import Configuration Files page displays.

Import Configuration files

Protocol

Hostname or IP address

Remote Username

Remote Password

File Path

2. Select the **Protocol** to use, which is one of the following: HTTP, HTTPS, SCP, SFTP, FTP, or TFTP.
3. Supply the IP address or hostname of the remote host in the **Hostname or IP Address** field.
4. Provide the credentials used to log in to the system by entering the user name in the **Remote Username** field and the user's password in the **Remote Password** field.
5. In the File Path field, provide the filename and filename path on the remote system.
6. Click **Import**.

11 Backup and Restore

GigaVUE H Series nodes provide the ability to backup and restore **configuration files** including all of the settings in place on the node at any one time. This section describes how to use configuration files, including the following major topics:

- [What Is Saved In a Configuration File](#) on page 167
- [Saving a Configuration File](#) on page 168

What Is Saved In a Configuration File

Configuration files store all of the settings in place on the GigaVUE H Series node when the file was saved—everything necessary to restore the node to its exact state when the file was saved. This includes:

- Map settings
- Port aliases
- Port parameters, including duplex, medium, speed, cable length, and so on
- Port-groups
- Port-pair settings
- Tool-mirror settings
- Port-type settings
- GigaStream settings
- All settings shown by the **show system** command
- User accounts, groups, and roles
- SNMP server/trap settings
- TACACS+, RADIUS, and LDAP servers
- NTP servers
- Syslog servers
- Host names
- Mgmt port IP settings
- Logging settings, including email notifications

Saving a Configuration File

To save a configuration file, do the following:

1. Select **Settings > Config and Licenses > Configurations**.

The Configuration files page shown in [Figure 11-1](#) displays.



Figure 11-1: Configuration File Page

2. Select **Actions > Save** the currently running configuration.

NOTE: If the you want to switch between multiple saved configuration files, you can use the **Switch to Active** button after selecting an existing configuration file.

3. When confirmation dialog shown in [Figure 11-2](#) displays, click **Save** to save the GigaVUE H Series node's current systems to the active configuration file.

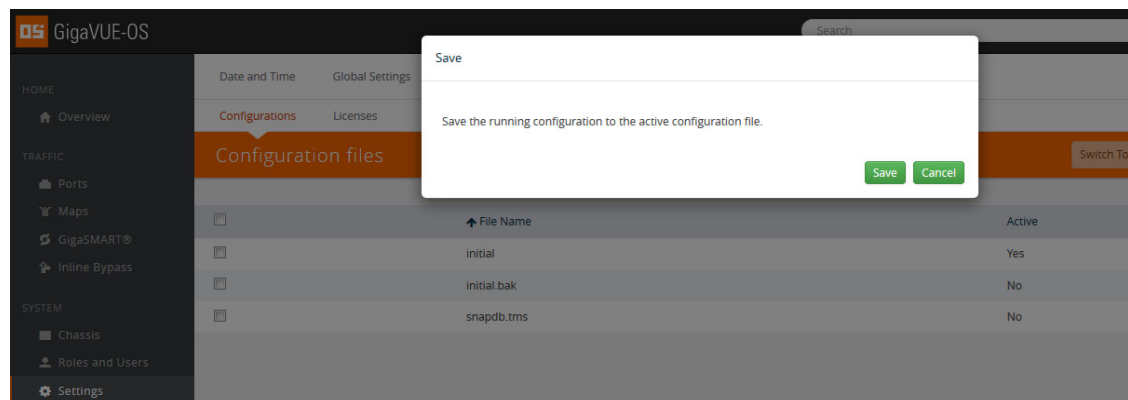


Figure 11-2: Saving a Running Configuration

You can also save the GigaVUE H Series node's current systems to a new filename by selecting **Actions > Save As**, entering a filename in the **New Filename** field of the confirmation dialog shown in [Figure 11-3](#), and then clicking **Save**.

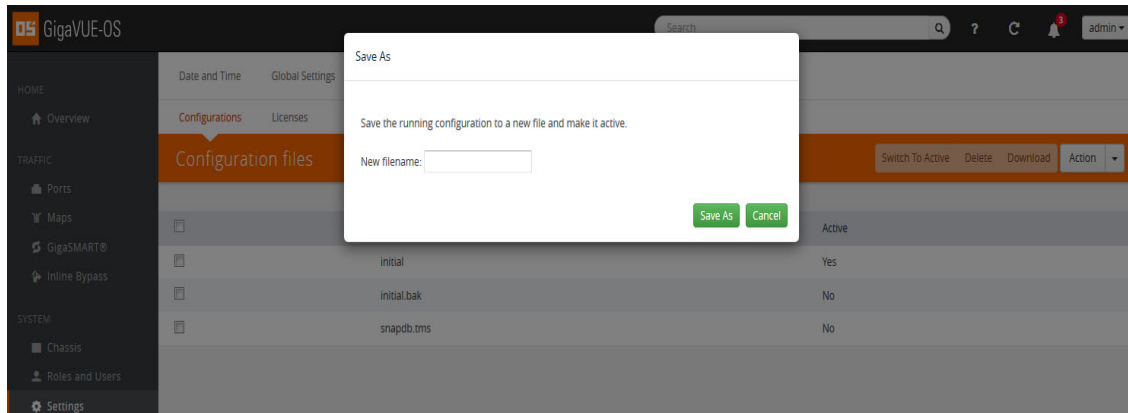


Figure 11-3: Saving a Running Configuration With Another Filename

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.

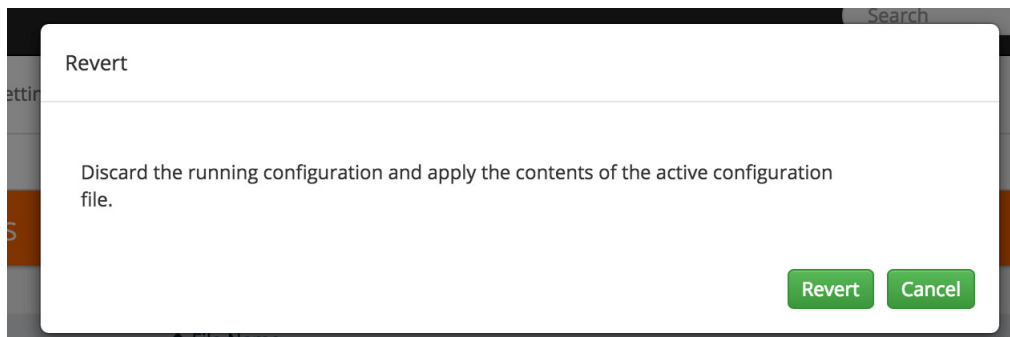


Figure 11-4: Revert

- **Reset**—resetting changes the running and active configuration to the factory default. The active licenses, host keys, and configuration for network connectivity is preserved.

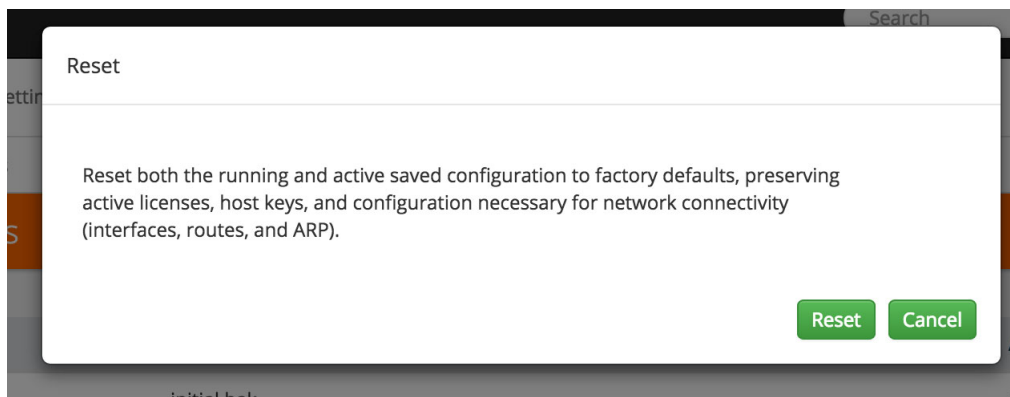


Figure 11-5: Reset

- **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.

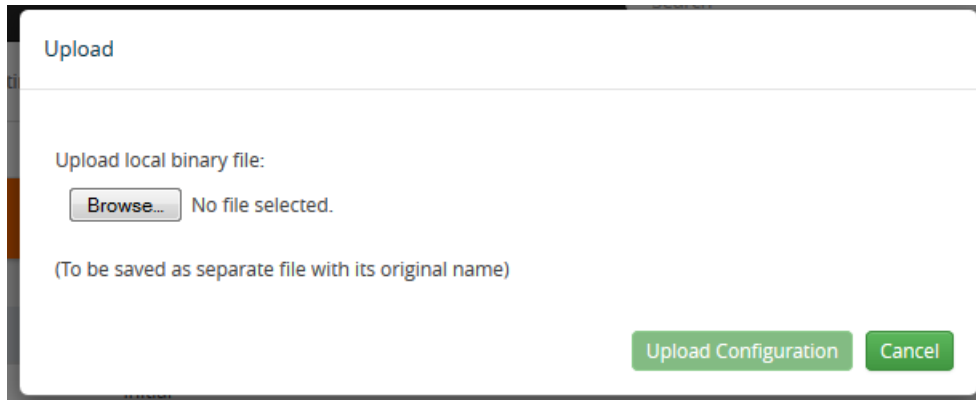


Figure 11-6: Upload Configuration

- **Import**—importing opens the **Import Configuration files** page. This page allows you to use external hosts that use protocols such as SFTP, FTP, TFTP or SCP. You can upload from a URL or IP address.

Figure 11-7: Importing Configuration Files from External Sources

Sharing Configuration Files with Other GigaVUE H Series Nodes

You can apply a configuration file created on one node to a second node. Keep in mind the following notes:

- All configuration settings that are not related to packet distribution (maps, tool-mirrors, port-pairs, and GigaStream) are reusable on the new node.
- Configuration settings related to packet distribution are tied to the chassis ID from the node on which they were saved. You can move these to the new node using either of the following methods:
 - Delete the old node (no chassis) and provision a new one, using a new box ID, if required.
 - If the box ID and module configuration of the new node is the same as the old node, you can perform a node migration using the procedure in the *Hardware Installation Guide*.

12 Using SNMP

This chapter describes how to use the SNMP features on the GigaVUE H Series and TA Series nodes. Refer to the following sections for details:

- [SNMP and Clusters](#) on page 173
- [Configuring SNMP Notifications](#) on page 173
 - [Configuring the SNMP Server and Notification Destinations](#) on page 174
 - [Configuring SNMP v3 Users](#) on page 175
 - [Enabling Notifications](#) on page 175
 - [Deleting a Destination for SNMP Notifications](#) on page 176
 - [Enabling or Disabling Events for SNMP Notifications](#) on page 177
 - [Receiving Traps](#) on page 178
 - [Viewing Associated Log Messages](#) on page 178
- [Enabling the SNMP Server](#) on page 180

SNMP and Clusters

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

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

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

Configuring SNMP Notifications

GigaVUE H Series nodes can send SNMP v1/v2c/v3 traps to specified destinations based on a variety of events on the node. Configuring SNMP traps consists of the following major steps:

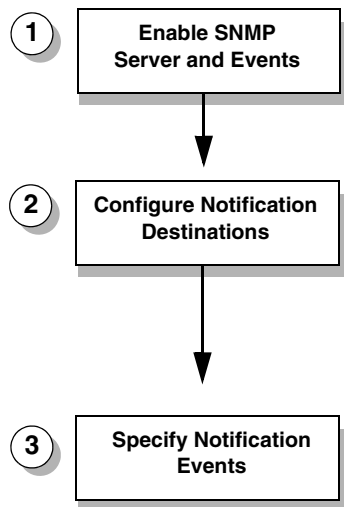


Figure 12-1: Configuring SNMP Notifications

Configuring the SNMP Server and Notification Destinations

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

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

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

1. Select **Settings > Global Settings > SNMP Traps**.
2. Click **Add**. The Add SNMP Traps page shown in [Figure 12-7](#) displays.

Figure 12-2: Add SNMP Traps Page

3. Configure the notification destination by doing the following:
 - a. Enter the IP address for the trap destination in the **IP Address** field.
 - b. Enter the community string in the **Community** field. For example, public.
 - c. Enter the server port number in the **Port** field.
 - d. Click in the **Trap Type** field and select **v2c**, **v1** or **v3** for the drop-down list.

If you select v3, you will also need to configure the SNMP v3 Users. Refer to [Configuring SNMP v3 Users](#) on page 175.

- e. Click in the Notify Type field and select **trap** or **inform**.
 - f. (Optional) If you selected v3 for Trap Type, enter the v3 username in the **v3 user** field.
 - g. Select **Enable** for **Trap Host** to enable the host.
4. Click **Save**.

Configuring SNMP v3 Users

If v3 is selected for the Trap Type when adding an SNMP trap, the SNMPv3 users also need to be configured. To configure an SNMP v3 user, do the following:

1. Select **Settings > Global Settings > SNMP v3 Users**.
2. Click **New**.
3. Enter the information for the SNMP v3 user.
 - **Username**—the name of the v3 user
 - **User**—Enables the user specified in the **Username** field when selected.
 - **Authentication Type**—the authentication type is either **md5** or **sha1**, which specified the mechanism to use for password hashing.
 - **Privacy Type**—the privacy type specifies the level of encryption for the password, which is either **des** or **aes-128**.
 - **Authentication Password**—the password used to authenticate the user specified by **Username**.
 - **Privacy Password**—a privacy password associated with the user specified by **Username** if a privacy type is specified. If no privacy type is specified, and a privacy password is entered, the default privacy type is aes-128.
4. Click **Save**.

Enabling Notifications

Once the GigaVUE H Series or TA Series SNMP server is enabled, you can enable the sending of SNMP notifications from the SNMP through the SNMP page shown in [Figure 12-3](#).

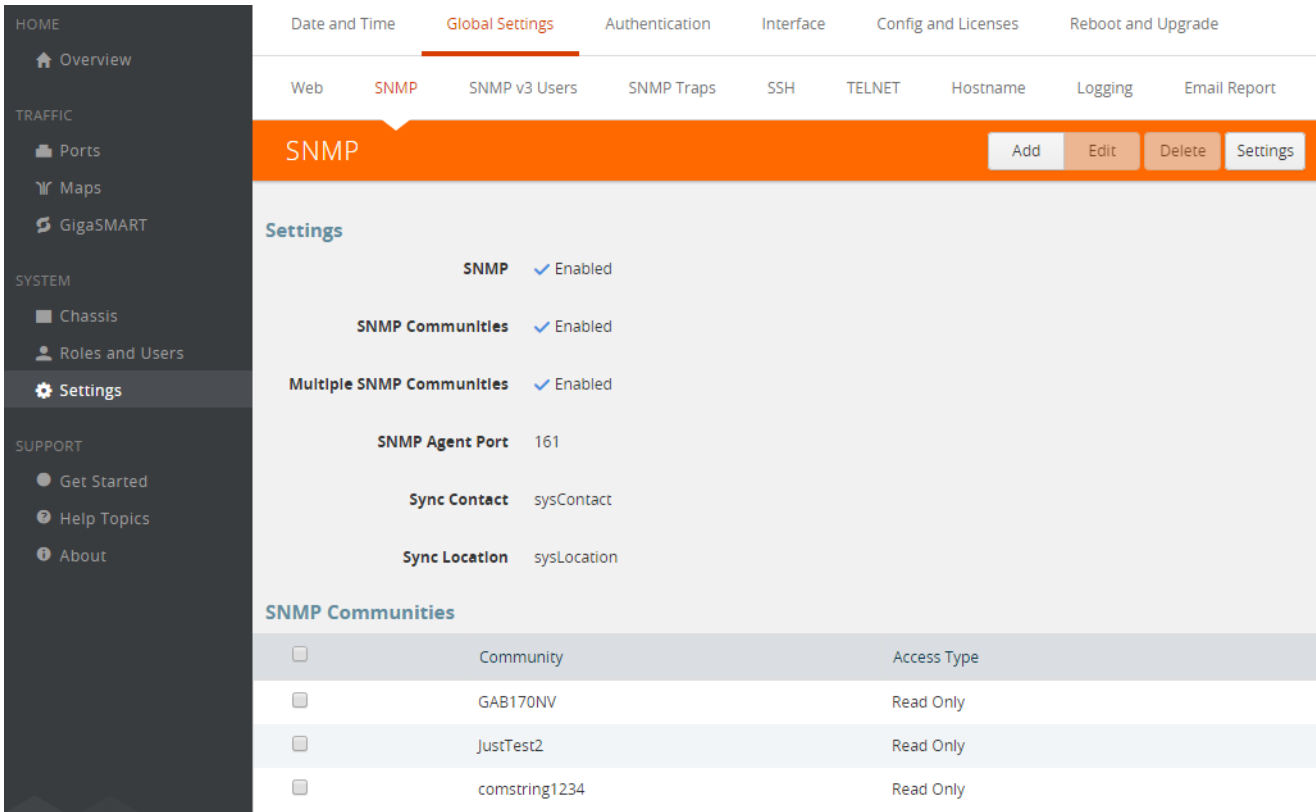


Figure 12-3: SNMP Settings Page

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

Deleting 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 12-4, 10.115.152.40 is selected.

Remote Log Sinks						
<input type="checkbox"/>	Server IP	Community	Port	Version	Enabled	
<input type="checkbox"/>	10.115.152.47	public	162	trap-v2c	true	
<input type="checkbox"/>	10.115.152.46	public	162	trap-v2c	true	
<input type="checkbox"/>	10.115.152.45	public	162	trap-v2c	true	
<input type="checkbox"/>	10.115.152.48	public	162	trap-v2c	true	
<input checked="" type="checkbox"/>	10.115.152.40	public	162	trap-v2c	true	

Figure 12-4: 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.

Enabling or Disabling Events for SNMP Notifications

To enable and disabling events for SNMP Notifications, do the following:

1. Selecting **Settings > Global Settings > SNMP Traps** to open the SNMP Traps page shown in [Figure 12-5](#).

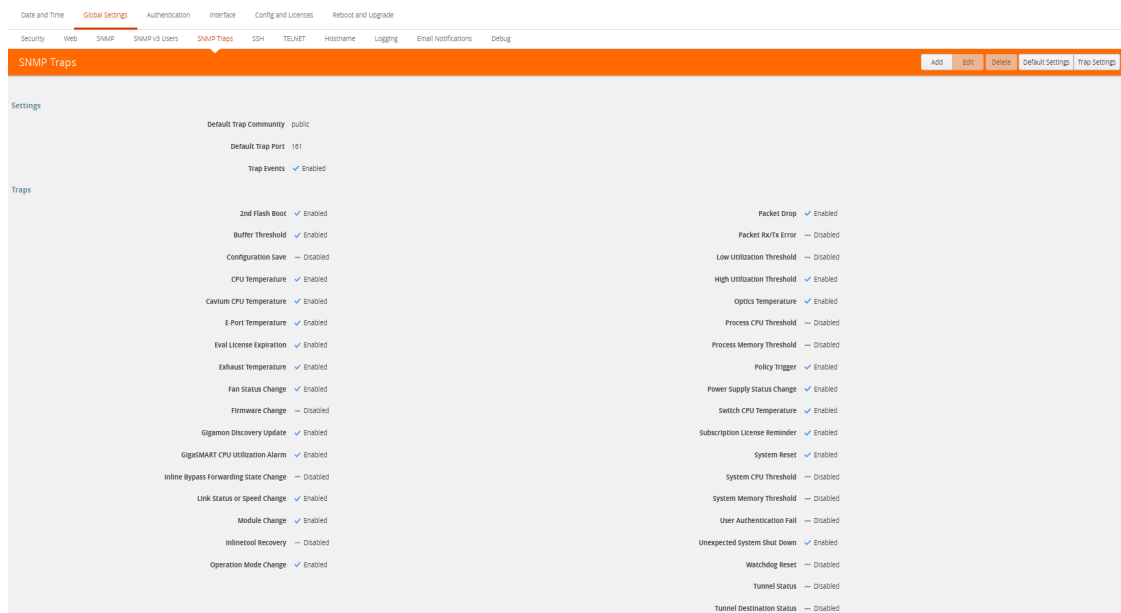


Figure 12-5: SNMP Notification Events Configured

2. Click **Trap Settings**. The Edit SNMP Trap Settings page opens as shown in [Figure 12-6](#).

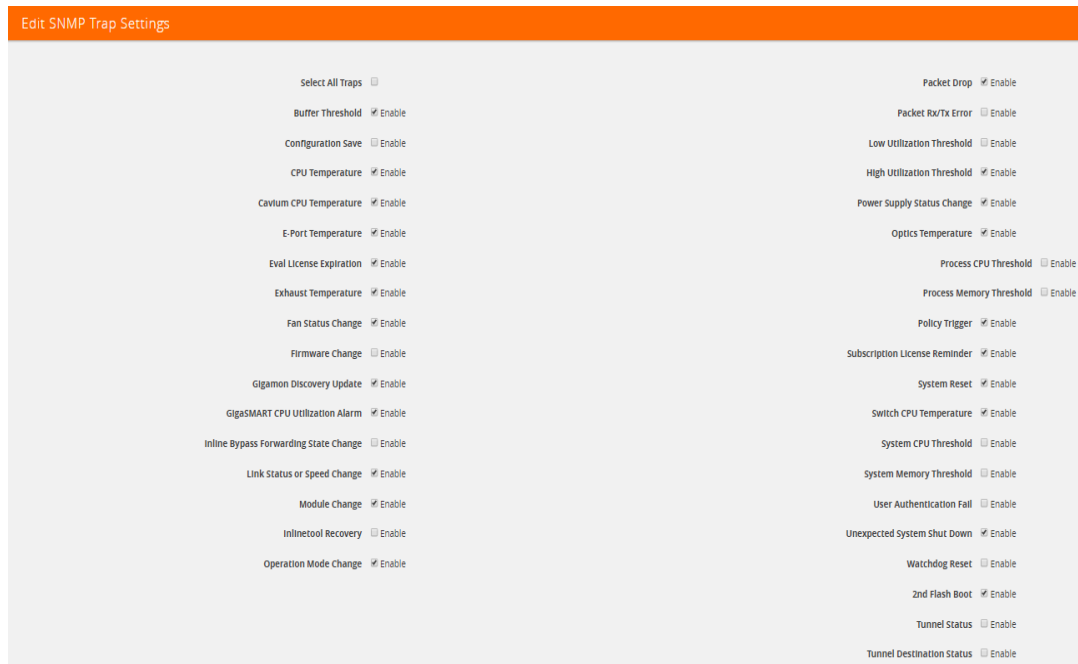


Figure 12-6: SNMP Trap Settings

3. On the Edit SNMP Traps Settings page, do the following:
 - Select the check box to enable a trap.
 - Clear the check box to disable a trap.
4. When you are done enabling or disabling taps, click **Save**.

Receiving Traps

The GigaVUE H Series node's MIB is available for download from the [Gigamon Customer Portal](#). The name of the MIB is GIGAMON-SNMP-MIB. Contact Technical Support for details.

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

Viewing Associated Log Messages

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

Table 12-1: 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

Table 12-1: Log messages Associated with SNMP Event

SNMP Event	Description	Log Message
gigasmarcputemp	GigaSMART engine temperature (for GigaVUE-HC1)	/gv/snmp/events/GigaSMARTCPUTemp
configsave	Configuration saved notification	/gv/snmp/events/ConfigSave
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
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 (not supported on GigaVUE-HB1)	/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

Table 12-1: Log messages Associated with SNMP Event

SNMP Event	Description	Log Message
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
systememthreshold	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
tunneldeststatus	Tunnel destination status notification	/gv/gs/snmp/events/TunnelDestStatusChange
unexpectedshutdown	Unexpected system shut down notification	/gv/snmp/events/UnexpectedShutdown
userauthfail	User authentication failure notification	/gv/snmp/events/UserAuthFail
vportstatuschange	vport status change notification	/gv/snmp/events/VportStateChange
watchdogreset	Watchdog monitor reset notification	/gv/snmp/events/WatchdogReset

The following is a sample log message:

```
sysdump-hc2-144-20150506-150207/messages.1:May 6 14:26:33 hc2-144
mgmtd[1829]: [mgmtd.INFO]: EVENT: /gv/snmp/events/
LinkSpeedStatusChange
```

Enabling the SNMP Server

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

The GigaVUE H Series and GigaVUE TA Series SNMP server is enabled so that management stations can poll the node remotely using standard SNMP commands (**Get**, **GetNext**, and **Walk**). The GigaVUE H Series and GigaVUE TA Series nodes support MIB polling using the standard MIB-II OIDs. You can retrieve statistics for any of the data ports. For a sample of ifIndex numbers, as well as a list of the supported statistics from the ifTable and ifXTable, refer to [Available SNMP Statistics for Data Ports](#) on page 182.

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

To enable the SNMP server:

1. Select **Settings > Global Settings > SNMP**.
2. On the SNMP page, click **Settings**.

The Edit SNMP Settings page displays as shown in [Figure 12-7](#)

SNMP	<input checked="" type="checkbox"/> Enable
SNMP Communities	<input checked="" type="checkbox"/> Enable
Multiple SNMP Communities	<input checked="" type="checkbox"/> Enable
SNMP Agent Port	161
Sync Contact	sysContact
Sync Location	sysLocation
Default Trap Community	Public
Default Trap Port	162

Figure 12-7: Edit SNMP Settings Page

3. Select **Enable** for SNMP.
4. Click **Save**.

Configuring 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 [Configuring the SNMP Server and Notification Destinations](#) on page 174.

4. Click **Save**.

Recommendations for Vulnerabilities

For SNMP recommended best practices for vulnerabilities such as, Multiple Vendor SNMP public Community String Information Disclosure, refer to:

<http://www.kb.cert.org/vuls/id/107186>

Gigamon makes the following recommendations to protect against SNMP vulnerabilities:

- Use the Gigamon ready-only community string (gigamon) to send traps and informs.
- Disable the default public community string.
- Use SNMPv3 to send traps and informs.
- Use a different port number from the default (162).

Available SNMP Statistics for Data Ports

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

You can use the **ifDescr** OID to correlate an ifIndex with a data port number on the GigaVUE H Series node. For example, the following table shows how ifIndex numbers are assigned to PRT-H00-X12G04 cards in slot 1 and slot 2 in the GigaVUE H Series node:

ifDescr OID	Value for a PRT-H00-X12G04 in Slots 1/2
ifDescr.1; Value (OctetString)	1/1/x1
ifDescr.2; Value (OctetString)	1/1/x2
ifDescr.3; Value (OctetString)	1/1/x3
ifDescr.4; Value (OctetString)	1/1/x4
ifDescr.5; Value (OctetString)	1/1/x5
ifDescr.6; Value (OctetString)	1/1/x6
ifDescr.7; Value (OctetString)	1/1/x7
ifDescr.8; Value (OctetString)	1/1/x8
ifDescr.9; Value (OctetString)	1/1/x9
ifDescr.10; Value (OctetString)	1/1/x10
ifDescr.11; Value (OctetString)	1/1/x11
ifDescr.12; Value (OctetString)	1/1/x12
ifDescr.13; Value (OctetString)	1/1/g1

ifDescr OID	Value for a PRT-H00-X12G04 in Slots 1/2
ifDescr.14; Value (OctetString)	1/1/g2
ifDescr.15; Value (OctetString)	1/1/g3
ifDescr.16; Value (OctetString)	1/1/g4
ifDescr.17; Value (OctetString)	1/2/x1
ifDescr.18; Value (OctetString)	1/2/x2
ifDescr.19; Value (OctetString)	1/2/x3
ifDescr.20; Value (OctetString)	1/2/x4
ifDescr.21; Value (OctetString)	1/2/x5
ifDescr.22; Value (OctetString)	1/2/x6
ifDescr.23; Value (OctetString)	1/2/x7
ifDescr.24; Value (OctetString)	1/2/x8
ifDescr.25; Value (OctetString)	1/2/x9
ifDescr.26; Value (OctetString)	1/2/x10
ifDescr.27; Value (OctetString)	1/2/x11
ifDescr.28; Value (OctetString)	1/2/x12
ifDescr.29; Value (OctetString)	1/2/g1
ifDescr.30; Value (OctetString)	1/2/g2
ifDescr.31; Value (OctetString)	1/2/g3
ifDescr.32; Value (OctetString)	1/2/g4

SNMP Statistics

The supported SNMP statistics from the ifTable are as follows:

- ifInOctets
- ifInUcastPkts
- ifInNUcastPkts
- ifInDiscards
- ifInErrors
- ifInUnknownProtos
- ifOutOctets
- ifOutUcastPkts
- ifOutNUcastPkts
- ifOutDiscards
- ifOutErrors

The supported SNMP statistics from the ifXTable are as follows:

- ifInMulticastPkts
- ifInBroadcastPkts
- ifOutMulticastPkts
- ifOutBroadcastPkts
- ifHCInOctets
- ifHCInUcastPkts
- ifHCInMulticastPkts
- ifHCInBroadcastPkts
- ifHCOctets
- ifHCOUcastPkts
- ifHCOMulticastPkts
- ifHCOBroadcastPkts

13 Monitoring Utilization

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

- [Viewing System Health Information](#) on page 185
- [Configuring Packet Capture](#) on page 193
- [Working with Port Utilization Measurements](#) on page 196
- [Configuring Alarm Buffer Thresholds](#) on page 200

Viewing 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:

- [Displaying the System Health Statistics](#) on page 186
- [Enabling the System Health Threshold Notification](#) on page 189
- [Configuring the System Health Threshold](#) on page 190

Displaying the System Health Statistics

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

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

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

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

Table 13-1 describes the statistics for CPU utilization:

Table 13-1: 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.

The following table describes the statistics for memory utilization:

Table 13-2: 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
syspth         1983  0.39%   0.31%   0.30%   145
profiler       1977  0.19%   0.09%   0.07%   31
redis-server   2103  0.00%   0.08%   0.07%   37
snmpd          1956  0.19%   0.03%   0.02%   69
pm             1851  0.00%   0.00%   0.00%   64
clusterd      2174  0.00%   0.00%   0.00%   5
crond          1962  0.00%   0.00%   0.00%   0
sshd           1957  0.00%   0.00%   0.00%   19
httpd         1969  0.00%   0.00%   0.00%   24
licd           1970  0.00%   0.00%   0.00%   2
ndiscd        1972  0.00%   0.00%   0.00%   7
restapid      1963  0.00%   0.00%   0.00%   0
syncd         1980  0.00%   0.00%   0.00%   0
sched         1964  0.00%   0.00%   0.00%   161
xinetd        1966  0.00%   0.00%   0.00%   0
```

```

Memory Usage :
=====
Physical: Total 3614M    Used 586M    Free 3028M
Swap:      Total 0M     Used 0M     Free 0M

process          pid    %mem    RAM    total
-----          -
netdevd          1958   1.83    66M    402M
mgmtd            1852   1.19    43M    91M
sched            1964   0.86    31M    81M
profiler         1977   0.44    16M    85M
peripd           1959   0.39    14M    35M
ugwd             1965   0.19    7M     55M
pm               1851   0.19    6M     10M
snmpd            1956   0.16    6M     14M
httpd            1969   0.12    4M     12M
wsmd             1960   0.09    3M     8M
avd              1985   0.07    2M     74M
gsd              1967   0.06    2M     23M
sshd             1957   0.06    2M     7M
clusterd         2174   0.05    2M     6M
syshth           1983   0.05    1M     21M
licd             1970   0.05    1M     5M
redis-server     2103   0.05    1M     20M
ndiscd           1972   0.04    1M     28M
syncd            1980   0.04    1M     4M
xinetd           1966   0.02    1M     4M
restapid         1963   0.02    1M     3M
crond            1962   0.01    0M     2M

```

Enabling the System Health Threshold Notification

The system health thresholds are pre-defined. When the CPU and memory utilization crosses the pre-defined threshold values, SNMP events are generated.

For example, assuming the memory utilization threshold value for the process 'netdevd' is 1GB and the system health threshold is enabled, when the memory utilization for netdevd crosses 1GB, an SNMP trap can be generated.

These SNMP events help in troubleshooting. Collect this information and report it to Gigamon Technical Support. A Gigamon Technical Support personnel can use this information to resolve the CPU and memory utilization issues. Refer to [Contacting Technical Support](#) on page 206.

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
```

Configuring 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_mgcmd	process cpu (mgcmd)	>= 98% (600 sec)	syslog, snmp trap
rule_proc_mem_mgcmd	process mem (mgcmd)	>= 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_lidcd	process cpu (lidcd)	>= 98% (600 sec)	syslog, snmp trap
rule_proc_mem_lidcd	process mem (lidcd)	>= 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

Viewing 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>
```

Enabling 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*.

Viewing the System Health Diagnostics

Use the following command to view a detailed diagnostics of system health for troubleshooting:

```
(config) # show diag detail
```

The detail command displays diagnostic information about fabric statistics, system-health, and inline SSL statistics detail, in addition to the diagnostic information displayed in **show diag**.

An upload option on the **show diag detail** command lets you upload the output to a specified URL using HTTP, HTTPS, FTP, TFTP, SCP, SFTP, or USB.

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

Configuring Packet Capture

This feature is at Beta. In software version 5.4, it is intended to be used by Gigamon Technical Support.

Use packet capture to assist with debugging traffic. Packets can be captured at an ingress port, an egress port, or both. Packets are captured at the specified port and are stored in a PCAP file.

Packet capture is supported on GigaVUE-HC1, GigaVUE-HC2, and GigaVUE-HC3 nodes. It is supported for standalone nodes, but not for nodes in a cluster.

The port type used for packet capture can be tool, network, hybrid, inline tool, or inline network. They must be physical ports.

To configure packet capture, define filters to capture specific traffic based on rules. The following criteria can be specified in the rules:

- source IPv4 address
- destination IPv4 address
- Layer 4 destination port number
- Layer 4 source port number
- Internet protocol
- TCP flags

Refer to the following notes for packet capture:

- The criteria listed above can be defined in any combination.
- The source and destination can only be IPv4 addresses.
- The source and destination can be specified as an IP address or a wildcard with an IP mask.
- The Layer 4 source and destination ports can be specified as a port number only. A range of ports is not supported.
- The TCP flags are control bits, such as SYN, FIN, ACK, URG, specified as 1 byte hex values.
- The number of ports on which packets can be simultaneously captured is 4.
- The number of ports on which **tx** packets can be captured is 4.
- The number of filters that can be configured on a node is 64.
- The same filter can be specified on multiple ports.
- The same port can have multiple filters configured on it.
- When multiple filters are configured, the traffic matching each filter is stored in a separate PCAP file.
- The PCAP file is stored in the following directory:
`/var/log/tmp`

Use the **show files pcap** command to display the PCAP file.

- The PCAP file can be exported from the GigaVUE node to an external location using the **file pcap upload** command.

NOTE: If Q-in-Q and packet capture are both configured on a GigaVUE node, there may be a conflict with the 6 tuples.

For details on the parameters for packet capture, refer to the “*pcap*” section in the *GigaVUE-OS CLI Reference Guide*.

To configure a packet capture filter, refer to the following example:

Step	Description	Command
1.	Configure the name of the packet capture filter.	(config) # pcap alias p1
2.	Configure the capture port and specify the direction.	(config pcap alias p1) # port 6/1/x7 tx
3.	Specify the channel port.	(config pcap alias p1) # channel-port 6/1/x1
4.	(Optional) Specify the number of packets to capture. If you do not specify a packet limit, delete the packet capture filter to stop capturing.	(config pcap alias p1) # packet-limit 1000
5.	Specify the rule on which to filter traffic and exit from the prefix mode.	(config pcap alias p1) # rule ipsrc 100.10.1.0 /24 portsrc 2048 protocol tcp (config pcap alias p1) # exit (config) #

To display the packet capture configuration, use the following CLI command:

```
(config) # show pcap
```

```
Packet Capture Rules
Total Pcap Count: 1
```

```
01) Pcap alias           : p1
   Enable                : true
   Port                  : 6/1/x7
   Direction             : tx
   Channel-port          : 6/1/x1
   Packet-limit          : 0
   Packet hit-count      : 0
   Rule                  :
-----
   Source IPv4/Mask      : 100.10.1.0/255.255.255.0
   Source Port           : 2048
   Protocol              : tcp
-----
```

To stop the packet capture, delete the packet capture filter using the following CLI command:

```
(config) # no pcap alias p1
```

To display the PCAP file, use the following CLI command:

```
(config) # show files pcap
pcap_p1_2018_05_08_17_17.pcap
```

To upload the PCAP file, use the following CLI command:

```
(config) # file pcap upload pcap_p1_2018_05_08_17_28.pcap scp://myNode@10.115.0.100/tftpboot/myName/.
Password (if required): *****
```

NOTE: Delete the packet capture filter before uploading the PCAP file.

Packet Capture Limitations

Refer to the following limitations of packet capture:

- IPv6 addresses are not supported.
- Configuration in a cluster is not supported.
- The port type of stack is not supported on the capture port or the channel port.
- GigaSMART engine ports are not supported.
- Inline network groups are not supported. Specify up to 4 individual ports for packet capturing.
- Packet capture filters cannot be saved or restored.
- Reload is not supported. Delete the packet capture filter before reloading.

Working with Port Utilization Measurements

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

Feature	CLI Command
View Port Utilization Percentage You can view the percentage utilization measurement over the last second for one or more ports. Refer to Viewing Port Utilization on page 196.	<code>show port utilization</code> <code>all</code> <code>box-id <box ID></code> <code>port-list <port list></code> <code>slot <slot ID></code>
Configure Percentage Utilization You can configure the utilization percentage at which the GigaVUE H Series node will generate high or low utilization alarms for a port. Utilization alarms are forwarded as SNMP notifications to all SNMP notification destinations configured in the CLI. Refer to Configuring Port Utilization Thresholds and Notifications on page 198.	<code>port <port list> alarm low-utilization-threshold <percentage></code> <code>port <port list> alarm high-utilization-threshold <percentage></code>

Port Utilization Availability by Port Type

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

Viewing 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
<code>show port utilization port-list 1/1/x1..x4</code>	This command displays port utilization for ports 1/1/x1, 1/1/x2, 1/1/1/x3, and 1/1/x4.
<code>show port utilization port-list streamdisk</code>	This command displays port utilization for the port with the alias streamdisk .
<code>show port utilization</code>	This command displays port utilization for all ports in the node or cluster.

Port Utilization Thresholds

Use CLI commands to set the thresholds for high and low utilization alarms on a port. When a threshold is exceeded, the GigaVUE H Series node will write a utilization alarm to syslog and forward it to all configured SNMP notification destinations.

Argument	Description
<code>port <port list></code>	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)
<code>alarm high-utilization-threshold <0~100></code> <code>alarm low-utilization-threshold <0~100></code>	Specifies the high and low utilization thresholds on a port, as a percentage. The thresholds specify the value at which the GigaVUE H Series node will log an alarm for the specified ports. The threshold must be exceeded for at least a 5-second interval. By default, the thresholds are 0 , which means disabled.

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

Utilization Alarm/SNMP Notification Generation

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

Requirement	Description
SNMP Enabled	Use the snmp-server enable options to turn on the node's SNMP functionality and enable notifications.

Requirement	Description
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: <pre>(config) # snmp-server notify event portutilization</pre> Use the lowportutilization argument for the snmp-server notify event command to enable low utilization notifications. For example: <pre>(config) # snmp-server notify event lowportutilization</pre> Refer to Configuring Port Utilization Thresholds and Notifications on page 198.
GigaVUE MIB Compiled at Management Station	You can obtain Gigamon's latest private MIB file by contacting support@gigamon.com .

Refer to [Using SNMP](#) on page 173 for information on configuring the GigaVUE H Series node's SNMP features.

Configuring 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.

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.

Configuring Alarm Buffer Thresholds

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

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

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

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

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

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

The buffer usage feature is supported on all ports and module types on the GigaVUE-HC3 and GigaVUE-HC2 (equipped with Control Card version 1 only).

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

- [Setting Alarm Buffer Thresholds](#) on page 201
- [Configuration Example](#) on page 202
- [Buffer Usage Alarm](#) on page 203

Setting Alarm Buffer Thresholds

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

The card level threshold indicates usage levels of the node.

The following table describes the arguments:

Argument	Description
card slot <slot ID>	Specifies the slot.
alarm buffer-threshold <0-100%>	Sets the alarm buffer threshold for a slot, as a percentage. By default, the threshold is set to 0 , which disables the threshold. NOTE: On the GigaVUE-HC2 and GigaVUE-HC3, this command configures the same alarm buffer threshold on all the slots in the chassis.

The following are examples of configuring alarm buffer thresholds on slots:

Command	Comments
(config) # card slot 4/1 alarm buffer-threshold 30	Configures the alarm buffer threshold on box id 4 and slot 1.
(config) # no card slot 4/1 alarm buffer-threshold	Removes the alarm buffer threshold on box id 4 and slot 1.

Use the **port <port list> alarm buffer-threshold** command to set rx (ingress) and tx (egress) alarm buffer thresholds on a port.

The port level thresholds indicate usage levels of each port.

The following table describes the arguments:

Argument	Description
port <port list>	Specifies the ports to which the alarm buffer threshold is to be applied. Use one of the following formats for the port-list: port-id <bid/sid/pid> port-alias <port-alias> port-list <bid/sid/pid_x..pid_y> (range) or <bid/sid/pid_x,bid/sid/pid_y,bid/sid/pid_z> (list)
alarm buffer-threshold <0-100%> rx <0-100%> tx <0-100%>	Specifies the alarm buffer threshold on a port. You can specify the alarm buffer threshold in the rx and tx directions on network and stack type ports and in the tx direction on tool type ports. By default, the threshold is set to 0 , which disables the threshold.

For details on the CLI command, refer to the “*card*” and “*port*” sections in the *GigaVUE-OS CLI Reference Guide* .

Configuration Example

The following example configures two network ports, one tool port, and a passall map and configures alarm buffer thresholds on the ports.

Step	Description	Command
1.	Configure two network ports and a tool port.	<code>(config) # port 12/1/x5..x6 type network</code> <code>(config) # port 12/1/x2 type tool</code>
2.	Configure buffer thresholds on each port.	<code>(config) # port 12/1/x5 alarm buffer-threshold 30</code> <code>(config) # port 12/1/x6 alarm buffer-threshold 32</code> <code>(config) # port 12/1/x2 alarm buffer-threshold 35</code>
3.	Create a passall map.	<code>(config) # map-passall alias bufExample</code> <code>(config map-passall alias bufExample) # from 12/1/x5..x6</code> <code>(config map-passall alias bufExample) # to 12/1/x2</code> <code>(config map-passall alias bufExample) # exit</code> <code>(config) #</code>
4.	Display buffer statistics.	<code>(config) # show buffer port 12/1/x5,12/1/x6,12/1/x2</code> <code>(config) # show profile current buffer</code> <code>(config) # show profile history buffer</code>

Use the following command to display the buffer statistics on the ports.

`(config) # show buffer port 12/1/x5,12/1/x6,12/1/x2`

Port	Buffer Usage (%)		Last Time Exceeds Threshold		Buffer Alarm Threshold (%)	
	RX	TX	RX	TX	RX	TX
12/1/x5	41	N/A	2014/07/01 17:30:07.371	N/A	30	N/A
12/1/x6	39	N/A	2014/07/01 17:30:07.378	N/A	32	N/A
12/1/x2	N/A	37	N/A	2014/07/01 17:30:07.384	N/A	35

Use the following command to display the current buffers:

`(config) # show profile current buffer all`

```

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

```

```

12/1/x5 counters      value
-----
                RX: 41
                TX: 0
            RX Config: 30
            TX Config: 0
Last Time Exceeding: 0

```

```

12/1/x6 counters      value
-----
                RX: 39
                TX: 0
            RX Config: 32
            TX Config: 0
Last Time Exceeding: 0

```

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

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

```
=====  
Port: 12/1/x5 minute history report  
=====
```

Counter Name	0 sec ago	5 secs ago	10 secs ago	15 secs ago
RX:	44	44	44	44
TX:	0	0	0	0
RX Config:	30	30	30	30
TX Config:	0	0	0	0

Counter Name	20 secs ago	25 secs ago	30 secs ago	35 secs ago
RX:	44	44	44	44
TX:	0	0	0	0
RX Config:	30	30	30	30
TX Config:	0	0	0	0

Counter Name	40 secs ago	45 secs ago	50 secs ago	55 secs ago
RX:	44	44	44	44
TX:	0	0	0	0
RX Config:	30	30	30	30
TX Config:	0	0	0	0

Buffer Usage Alarm

When a buffer usage threshold has exceeded its configured percentage, a message is logged, and optionally, an SNMP notification is sent to all configured destinations.

Use the following command to configure the notification that is sent when the buffer usage has exceeded the configured threshold:

```
(config) # snmp-server notify event bufferoverusage
```

The SNMP notification will be sent when a threshold is exceeded in any 5-second interval. Once the notification is sent, there is a 30 second holdoff time before the notification is sent again.

Additional Sources of Information

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

- [Documentation](#) on page 205
- [Documentation Feedback](#) on page 206
- [Contacting Technical Support](#) on page 206
- [Contacting Sales](#) on page 206
- [The Gigamon Community](#) on page 206

Documentation

Gigamon provides additional documentation for GigaVUE H Series and TA Series nodes on the Gigamon Customer Portal at www.gigamon.com/customer-portal-login.

Document	Summary
GigaVUE-HC1 Hardware Installation Guide	Describes how to unpack, assemble, rack-mount, connect, and perform the initial configuration of GigaVUE-HC1 nodes. Also provides reference information for the GigaVUE-HC1 node, including specifications.
GigaVUE-HC2 Hardware Installation Guide	Describes how to unpack, assemble, rack-mount, connect, and perform the initial configuration of GigaVUE-HC2 nodes. Also provides reference information for the GigaVUE-HC2 node, including specifications.
GigaVUE-HC3 Hardware Installation Guide	Describes how to unpack, assemble, rack-mount, connect, and perform the initial configuration of GigaVUE-HC3 nodes. Also provides reference information for the GigaVUE-HC3 node, including specifications.
GigaVUE TA Series Hardware Installation Guide	Describes how to unpack, assemble, rack-mount, connect, and perform the initial configuration of GigaVUE-TA10, GigaVUE-TA40, GigaVUE-TA100, GigaVUE-TA100-CXP, and GigaVUE-TA200 nodes. Also provides reference information for these nodes, including specifications.
GigaVUE-OS Installation Guide on a White Box	Describes how to install the GigaVUE-OS on a white box.
GigaVUE-OS CLI Reference Guide	Describes how to use the CLI (Command Line Interface) to configure and operate the GigaVUE H Series and TA Series software.
GigaVUE-OS H-VUE Online Help	Describes the web-based GUI for the GigaVUE-OS

Document	Summary
GigaVUE-OS Upgrade Guide	Describes how to upgrade GigaVUE H Series and GigaVUE TA Series nodes to the latest GigaVUE-OS.
GigaVUE TA Series Upgrade Guide	Describes how to upgrade a GigaVUE TA Series node to the latest GigaVUE-OS.
GigaVUE-OS Release Notes	Describes new features and known issues in the release.
GigaVUE-FM User's Guide	Describes how to install, deploy, and operate the GigaVUE® Fabric Manager (GigaVUE-FM)
GigaVUE VM User's Guide	Describes how to install, deploy, and operate the GigaVUE® Virtual Machine (GigaVUE-VM)

Documentation Feedback

To send feedback and report issues in our documentation, complete the short survey at the following link:

<https://www.surveymonkey.com/r/gigamondocumentationfeedback>

Contacting Technical Support

Refer to <http://www.gigamon.com/support-and-services/contact-support> for Technical Support hours and contact information. You can also email Technical Support at support@gigamon.com.

Contacting Sales

Table i: Sales Contact Information

Telephone	+1 408.831.4025
Sales	inside.sales@gigamon.com

The Gigamon Community

The [Gigamon Community](#) is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the Gigamon Community site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.

- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Submit and vote on feature enhancements and share product feedback. (Customers only)
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

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

Register today at community.gigamon.com

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

