Gigamon®

GigaVUE Firewall Security Guide

GigaVUE

Product Version: 6.6

Document Version: 1.1

Last Updated: Thursday, October 10, 2024

(See Change Notes for document updates.)

Copyright 2024 Gigamon Inc. All rights reserved.

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

Trademark Attributions

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

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

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
6.6	1.1	10/10/2024	This update includes bug fixes and minor cosmetic changes for improved usability and document consistency.
6.6	1.0	3/22/2024	The original release of this document with 6.6.00 GA.

Contents

Audience

This guide is intended for the users who have basic understanding of VMs and Nutanix Environment. This document expects the users to be familiar with the following terminologies that are used in this guide:

- **Cluster:** A group of nodes.
- **Node:** A node is a working machine in Nutanix cluster. Each node runs a standard hypervisor with processors, memories, and local storages.

Get started with GigaVUE Security

This guide provides information about the open ports in GigaVUE-FM, GigaVUE-FM High Availability, open ports in GigaVUE-H series devices, open ports in GigaVUE HC Series and GigaVUE TA Series devices.

You can also get information about the Network Firewall Requirements for GigaVUE V Series Node deployment, OpenStack, Gigamon fabrics for Nutanix deployments, Kubernetes network requirements for GCB.

Topics:

- Open Ports in GigaVUE-FM
- Network Firewall Requirements for VMware
- Network Firewall Requirements for OpenStack
- Network Firewall Requirements for Azure
- Network Requirements for Gigamon Containerized Broker (GCB)
- Network Firewall Requirements for Nutanix

- Security Group for AWS
- Security Group
- Security Group

Rithvik07*

Open Ports in GigaVUE-FM

This appendix provides information about the open ports in GigaVUE-FM and also in the devices. Refer to the following sections:

- Open Default Ports
- Open Ports for GigaVUE-FM Migration
- Open Ports for High Availability
- Open Ports for Communication Between Members of GigaVUE-FM High Availability Cluster
- Open Ports in GigaVUE HC Series Devices
- Open Ports in GigaVUE-FM
- Open Ports for Clustered Node Communication

Open Default Ports

The following table provides information about the default ports open in the firewall for GigaVUE-FM. The table is sorted by Protocol and then Port Number.

Port Number	Protocol	Service	Traffic Direction	Description
80	HTTP	GigaVUE-FM GUI	Bidirectional traffic between Web Browser and GigaVUE-FM	Used for redirecting the traffic internally to port 443. **Note:** You can choose to shut down port 80 for enhanced security.
443	HTTPS	GigaVUE-FM	Bidirectional	Used for normal GigaVUE-FM user

Port Number	Protocol	Service	Traffic Direction	Description
		GUI	traffic between Web Browser and GigaVUE-FM Bidirectional traffic between GigaVUE-FM and GigaVUE-VM.	interaction.
389	LDAP	AAA	Bidirectional traffic between LDAP server and GigaVUE-FM	Used for accessing and maintaining distributed directory information services over the Internet Protocol (IP) network.
636	LDAP	AAA	Bidirectional traffic between LDAP server and GigaVUE-FM	Used for secure LDAP protocol over SSL for accessing and maintaining distributed directory information services over the Internet Protocol (IP) network.
1812/1813 1645/1646	Radius	AAA	Bidirectional traffic between Radius server and GigaVUE-FM	Used for running the client/server protocol in the application layer. They can use either TCP or UDP as the transport protocol.
49	TACACS	AAA	Bidirectional traffic between TACACS server and GigaVUE-FM	Used for communicating with the authentication server in order to determine if you have access to the network.
22	TCP	SSH	Bidirectional traffic between Putty and GigaVUE-FM	• Used for GigaVUE-FM admin user login. Also, used for initial GigaVUE-FM IP configuration. • Used by the web browser to communicate with GigaVUE-VM for troubleshooting purposes.
514	TCP	Logstash	Unidirectional traffic from physical nodes to GigaVUE-FM	Used for sending device log messages via SSL from devices to GigaVUE-FM.
5672	TCP	RabbitMq	Unidirectional traffic from physical nodes to GigaVUE-FM	Used for sending event notifications via SSL from devices to GigaVUE-FM.
5671	TCP/SSL	RabbitMq	Unidirectional traffic from physical nodes to GigaVUE-FM	Used for sending event notifications via SSL from devices to GigaVUE-FM.
53	UDP	DNS	Bidirectional traffic between a DNS server and	Used to resolve Fully Qualified Domain Names (FQDNs).

Port Number	Protocol	Service	Traffic Direction	Description
			GigaVUE-FM	
68	UDP	DHCP	Bidirectional traffic between GigaVUE-FM and DHCP server	Used only if DHCP is enabled on the GigaVUE-FM appliance.
123	UDP	NTP	Bidirectional traffic between a Network Time Protocol (NTP) server and GigaVUE-FM	Used only if GigaVUE-FM is configured to use NTP.
162	UDP	SNMP	Unidirectional traffic from managed appliances to GigaVUE-FM	Used to process incoming traps sent from managed appliances to GigaVUE-FM.
2055	UDP	NetFlow	Unidirectional traffic from managed Appliances to GigaVUE-FM	Used for receiving NetFlow traffic.
2056	UDP	Logstash	Unidirectional traffic from physical and virtual nodes to GigaVUE-FM	Used by Application Intelligence for sending monitoring reports to GigaVUE-FM.
8443	TCP	HTTPS ALT	Bidirectional traffic between GigaVUE-FM and Apache Tomcat web server.	Port 8443 is an alternative HTTPS port and a primary protocol that the Apache Tomcat web server utilizes to open the SSL text service. In addition, this port is primarily used as an HTTPS Client Authentication connection protocol.
9514	TCP	Logstash	Unidirectional traffic from nodes to GigaVUE-FM	Port used by logstash application.

Note: The following ports are blocked by firewall internally (and no security issues have been observed). You cannot access GigaVUE-FM using these ports:

- 2181
- 8009
- 8080
- 9200

Open Ports for GigaVUE-FM Migration

The following table provides details about ports that must be open during GigaVUE-FM migration.

Port Number	Protocol	Service	Traffic Direction	Description
443	HTTPS	GigaVUE-FM GUI	Bidirectional traffic between Web Browser and GigaVUE-FM	Used for API and GUI access related operations.
22	TCP	SSH	Bidirectional traffic between Putty and GigaVUE-FM	Used for transferring configuration files between two instances of GigaVUE-FM.
902	TCP/UDP	ESXi Host	Bidirectional traffic between VMware vCenter and ESXi hosts	• For migration and provisioning purposes, this port must be open between the VMware vCenter server and the VMware ESXi hosts. Otherwise, GigaVUE-FM bulk deployment fails. • Used for sending data from vCenter Server to the ESXi host. The ESXi host uses this port to send regular heartbeat to the vCenter Server system.

Open Ports for High Availability

The following table provides details about ports that must be open for GigaVUE-FM High Availability.

Port Number	Protocol	Service	Traffic Direction	Description
22	TCP	SSH	Bidirectional traffic between Putty and GigaVUE-FM	• Used for GigaVUE-FM admin user login. Also, used for initial GigaVUE-FM IP configuration. • Used by the web browser to communicate with GigaVUE-VM for troubleshooting purposes. • Used for transferring configuration files between two GigaVUE-FM instances during migration.
80	TCP	HTTP	Bidirectional traffic between Web Browser and GigaVUE-FM	Used for redirecting the traffic internally to port 443. **Note:** You can choose to shut down port 80 for enhanced security.
443	TCP	HTTPS	• Bidirectional traffic between Web Browser and GigaVUE-FM. • Bidirectional traffic between GigaVUE-FM and GigaVUE-VM. • Bidirectional traffic between the GigaVUE-FM instances in a High Availability group.	Used for normal GigaVUE-FM user interaction.
514	TCP/UDP	Shell/Syslog	Unidirectional traffic from physical nodes to GigaVUE-FM	Used for sending device log messages via SSL from devices to GigaVUE-FM.
4369	TCP	EPMD/RMQ	Bidirectional traffic between RMQ members in cluster.	Small additional process that runs alongside every RabbitMQ node and is used by the runtime to discover what port a particular node listens to. The port is then used by peer nodes.
5671	TCP	amqps	Unidirectional traffic from physical nodes to GigaVUE-FM	Used for sending event notifications via SSL from devices to GigaVUE-FM.
25672	TCP	RabbitMQ/ SNMP Traps	Bidirectional traffic between RMQ	

Port Number	Protocol	Service	Traffic Direction	Description
			members in cluster.	
68	UDP	DHCP	Bidirectional traffic between GigaVUE-FM and DHCP server	Used only if DHCP is enabled on the GigaVUE-FM appliance.
162	UDP	SNMP	Unidirectional traffic from managed appliances to GigaVUE-FM	Used to process incoming traps sent from managed appliances to GigaVUE-FM.

NOTE: Ports 9514 and 9162 are used to receive the traffic forwarded by ports 514 and 162, respectively. Therefore, these ports need not be opened explicitly.

Open Ports for Communication Between Members of GigaVUE-FM High Availability Cluster

The following table lists the ports that must be open for communication between the members of GigaVUE-FM High Availability cluster.

NOTE: These ports cannot be accessed by standalone GigaVUE-FM instances.

Port Number	Protocol	Service	Traffic Direction	Description
8300	TCP	Consul	Bidirectional traffic between members in GigaVUE-FM cluster.	Used To handle incoming requests from other agents.
8301	TCP/UDP	Consul	Bidirectional traffic between members in GigaVUE-FM cluster.	Used for inter-cluster communication over LAN.
8302	TCP	Consul	Bidirectional traffic between members in GigaVUE-FM cluster.	Used for inter-cluster communication over WAN.

Port Number	Protocol	Service	Traffic Direction	Description
30865	TCP	CSync2	Bidirectional traffic between members in GigaVUE-FM cluster.	Used for Synchronization of files/directories across cluster. For example, Image files during GigaVUE-FM HA Upgrade.
9300	TCP	Elastic Search	Bidirectional traffic between members in GigaVUE-FM cluster.	Used for inter-cluster communication.
27017	TCP	MongoDB	Bidirectional traffic between members in GigaVUE-FM cluster.	Used for data replication across clusters and data access through GigaVUE-OS CLI.

Open Ports in GigaVUE HC Series Devices

The following table lists the open ports in GigaVUE-H series devices. GigaVUE-FM manages the devices using these open ports.

Port Number	Protocol	Service	Traffic Direction	Description
80	HTTP	Communication	Bidirectional traffic between GigaVUE-FM and devices.	Used for initial communication setup. Assumption is that HTTP redirect will be turned ON in all GigaVUE devices and GigaVUE-FMwill use HTTP(S) henceforth.
443	HTTPS	Communication	Bidirectional traffic between GigaVUE-FM and devices.	GigaVUE-FM to device communication. Refer to the following notes:

Port Number	Protocol	Service	Traffic Direction	Description

				• Starting in software version 5.9.00, XML Gateway services are shutdown in the devices. Therefore, if you change the HTTPS port number of a device using CLI, then:
				  • For devices that are not added and managed by GigaVUE-FM: You must update the HTTPS port number when adding the nodes using the Add Physical Nodes page in GigaVUE-FM GUI. Refer to the *Add Nodes Manually* section for more details.
				  • For devices that have already been added and managed by GigaVUE-FM: You must update the HTTPS port number from the Node Details page (**Admin** > **System** > **Node Details**). In the Node Details page, select the device and click **Edit** to update the port number and click **Save**.
				• Failure to do so will terminate communication between the device and GigaVUE-FM
				NOTE: Until software version 6.6, if the HTTPS port number is changed using CLI, then GigaVUE-FM will learn the port number through the XML Gateway request.
				• Devices with software version greater than or equal to software version 5.9.00 are XSRF enabled, by default.

Open Ports for Clustered Node Communication

The following table lists the open ports in GigaVUE HC Series and GigaVUE TA Series devices.

Port Number	Protocol	Service	Traffic Direction	Description
5353	UDP	Communication	Bidirectional	Used for cluster communication
6379	TCP	Communication	Bidirectional	Used to communicate with clients that need to reach the cluster nodes

Security Group for AWS

A security group defines the virtual firewall rules for your instance to control inbound and outbound traffic. When you launch GigaVUE-FM, GigaVUE V Series Proxies, GigaVUE V Series nodes, and UCT-V Controllers in your project, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

To create a security group, refer to Create a security group topic in the AWS Documentation.

It is recommended to create a separate security group for each component using the rules and port numbers listed in the following table.

The following table lists the Network Firewall / Security Group requirements for GigaVUE Cloud Suite.

NOTE: When using dual stack network, the below mentioned ports must be opened for both IPv4 and IPv6.

Direction	Protocol	Port	CIDR	Purpose
GigaVUE-FM				
Inbound	TCP	443	Administrator Subnet	Allows GigaVUE-FM to create Management connection.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	UCT-V Controller IP	Allows GigaVUE-FM to receive registration requests from UCT-V Controller.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive registration requests from GigaVUE V Series Node, when GigaVUE V Series Proxy is not used.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to receive registration requests from GigaVUE V Series Proxy.
Inbound	TCP	5671	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive traffic health updates from GigaVUE V Series Nodes.
Inbound	TCP	5671	UCT-V or Subnet IP	Allows GigaVUE-FM to receive statistics from Next Generation UCT-V.
Inbound	UDP	2056	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive Application Intelligence and Application Visualization reports from GigaVUE V Series Node.
Outbound	TCP	9900	GigaVUE-FM IP	Allows GigaVUE-FM to communicate control plane and data plane traffic with UCT-V Controller
Outbound (optional)	TCP	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate control plane and data plane traffic to GigaVUE V Series Proxy

Direction	Protocol	Port	CIDR	Purpose
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate control plane and data plane traffic to GigaVUE V Series Node
Outbound	TCP	443	GigaVUE-FM IP Address	Allows GigaVUE-FM to reach the Public Cloud Platform APIs.
Outbound	TCP	8443	UCT-C Controller IP Address	Allows GigaVUE-FM to communicate with UCT-C Controller
UCT-V Controller				
Inbound	TCP	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate with GigaVUE-FM
Inbound (This is the port used for Third Party Orchestration)	TCP	8891	UCT-V or Subnet IP	Allows UCT-V Controller to receive the registration requests from UCT-V.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Outbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE-FM IP	Allows UCT-V Controller to send the registration requests to GigaVUE-FM
Outbound	TCP	9901	UCT-V Controller IP	Allows UCT-V Controller to communicate with UCT-Vs.
Outbound	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM.
UCT-V				
Inbound	TCP	9901	UCT-V Controller IP	Allows UCT-V to receive stateful communication from UCT-V Controller
Outbound (This is the port used for Third Party Orchestration)	TCP	8891	UCT-V or Subnet IP	Allows UCT-V to communicate with UCT-V Controller for registration and Heartbeat
Outbound	• UDP (VXLAN) • IP Protocol	VXLAN (default 4789)	UCT-V or Subnet IP	Allows UCT-V to (VXLAN/L2GRE) tunnel traffic

Direction	Protocol	Port	CIDR	Purpose
	(L2GRE)			to V Series nodes
Outbound	TCP	11443	UCT-V subnet	Allows UCT-V to securely transfer the traffic to GigaVUE V Series Node
Outbound	TCP	9900	UCT-V Controller IP	Allows UCT-V to send traffic health updates to UCT-V Controller.
GigaVUE V Series Proxy (optional)				
Inbound	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Proxy
Inbound (This is the port used for Third Party Orchestration)	TCP	8891	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to receive registration requests and heartbeat messages from GigaVUE V Series Node.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Outbound	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Proxy to communicate the registration requests to GigaVUE-FM
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to communicate with GigaVUE V Series Node
GigaVUE V Series Node				
Inbound	TCP	8889	GigaVUE-FM IP	Allows GigaVUE V Series Node to communicate with GigaVUE-FM
Inbound	TCP	8889	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to communicate with GigaVUE V Series Proxy.
Inbound	• UDP (VXLAN) • IP Protocol (L2GRE)	• VXLAN (default 4789) • L2GRE	UCT-V or Subnet IP	Allows GigaVUE V Series Node to (VXLAN/L2GRE) tunnel traffic to UCT-V.
Inbound	UDPGRE	4754	Ingress Tunnel	Allows GigaVUE V Series Node to communicate and tunnel traffic from UDPGRE Tunnel

Direction	Protocol	Port	CIDR	Purpose
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user initiated management and diagnostics, specifically when using third party orchestration.
Outbound	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM
Outbound	• UDP (VXLAN) • IP Protocol (L2GRE)	VXLAN (default 4789)	Tool IP	Allows GigaVUE V Series Node to communicate and tunnel traffic to the tool
Outbound	UDP	2056	GigaVUE-FM IP	Allows GigaVUE V Series Node to send Application Intelligence, Application Visualization reports to GigaVUE-FM
Outbound	UDP	2055	Tool IP	Allows GigaVUE V Series Node to send NetFlow traffic to external tool.
Outbound	UDP	514	Tool IP	Allows GigaVUE V Series Node to send Application Metadata Intelligence log messages to external tool.
Outbound (optional)	ICMP	• echo request • echo reply	Tool IP	Allows GigaVUE V Series Node to send health check tunnel destination traffic
Outbound (This is the port used for Third Party Orchestration)	TCP	8891	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE V Series Proxy when GigaVUE V Series Proxy is used.
Outbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE-FM IP Address	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE-FM when GigaVUE V Series Proxy is not used.
Bidirectional	TCP	11443	GigaVUE V Series Node subnet	Allows to securely transfer the traffic in between GigaVUE V Series Nodes.
Universal Cloud Tap - Container deployed inside Kubernetes worker node				
Outbound	TCP	42042	Any IP address	Allows UCT-C to send statistics to UCT-C Controller.
UCT-C Controller deployed inside Kubernetes worker node				
Inbound	TCP	8443	Any IP address	Allows UCT-C Controller to

Direction	Protocol	Port	CIDR	Purpose
		(configurable)		communicate with GigaVUE-FM
Outbound	TCP	5671	Any IP address	Allows UCT-C controller to send statistics to GigaVUE-FM.
Outbound	TCP	VXLAN (default 4789)	Any IP address	Allows UCT-C Controller to communicate and tunnel traffic to the tool
Outbound	TCP	443	Any IP address	Allows UCT-C Controller to communicate with GigaVUE-FM

Network Firewall Requirements for Azure

The following table lists the Network Firewall / Security Group requirements for GigaVUE Cloud Suite.

NOTE: When using dual stack network, the below mentioned ports must be opened for both IPv4 and IPv6.

Direction	Protocol	Port	CIDR	Purpose
GigaVUE-FM				
Inbound	TCP	443	Administrator Subnet	Allows GigaVUE-FM to create Management connection.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	UCT-V Controller IP	Allows GigaVUE-FM to receive registration requests from UCT-V Controller.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive registration requests from GigaVUE V Series Node, when GigaVUE V Series Proxy is not used.
Inbound	TCP	443	GigaVUE V	Allows GigaVUE-FM to

Direction	Protocol	Port	CIDR	Purpose
(This is the port used for Third Party Orchestration)			Series Proxy IP	receive registration requests from GigaVUE V Series Proxy.
Inbound	TCP	5671	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive traffic health updates from GigaVUE V Series Nodes.
Inbound	TCP	5671	UCT-V or Subnet IP	Allows GigaVUE-FM to receive statistics from Next Generation UCT-V.
Inbound	UDP	2056	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive Application Intelligence and Application Visualization reports from GigaVUE V Series Node.
Outbound	TCP	9900	GigaVUE-FM IP	Allows GigaVUE-FM to communicate control plane and data plane traffic with UCT-V Controller
Outbound (optional)	TCP	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate control plane and data plane traffic to GigaVUE V Series Proxy
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate control plane and data plane traffic to GigaVUE V Series Node
Outbound	TCP	443	GigaVUE-FM IP Address	Allows GigaVUE-FM to reach the Public Cloud Platform APIs.
Outbound	TCP	8443	UCT-C Controller IP Address	Allows GigaVUE-FM to communicate with UCT-C Controller
UCT-V Controller				
Inbound	TCP	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate with GigaVUE-FM
Inbound (This is the port used for Third Party Orchestration)	TCP	8891	UCT-V or Subnet IP	Allows UCT-V Controller to receive the registration requests from UCT-V.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically

Direction	Protocol	Port	CIDR	Purpose
				when using third party orchestration.
Outbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE-FM IP	Allows UCT-V Controller to send the registration requests to GigaVUE-FM
Outbound	TCP	9901	UCT-V Controller IP	Allows UCT-V Controller to communicate with UCT-Vs.
Outbound	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM.
UCT-V				
Inbound	TCP	9901	UCT-V Controller IP	Allows UCT-V to receive stateful communication from UCT-V Controller
Outbound (This is the port used for Third Party Orchestration)	TCP	8891	UCT-V or Subnet IP	Allows UCT-V to communicate with UCT-V Controller for registration and Heartbeat
Outbound	• UDP (VXLAN) • IP Protocol (L2GRE)	VXLAN (default 4789)	UCT-V or Subnet IP	Allows UCT-V to (VXLAN/L2GRE) tunnel traffic to V Series nodes
Outbound	TCP	11443	UCT-V subnet	Allows UCT-V to securely transfer the traffic to GigaVUE V Series Node
Outbound	TCP	9900	UCT-V Controller IP	Allows UCT-V to send traffic health updates to UCT-V Controller.
GigaVUE V Series Proxy (optional)				
Inbound	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Proxy
Inbound (This is the port used for Third Party Orchestration)	TCP	8891	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to receive registration requests and heartbeat messages from GigaVUE V Series Node.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.

Direction	Protocol	Port	CIDR	Purpose
Outbound	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Proxy to communicate the registration requests to GigaVUE-FM
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to communicate with GigaVUE V Series Node
GigaVUE V Series Node				
Inbound	TCP	8889	GigaVUE-FM IP	Allows GigaVUE V Series Node to communicate with GigaVUE-FM
Inbound	TCP	8889	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to communicate with GigaVUE V Series Proxy.
Inbound	• UDP (VXLAN) • IP Protocol (L2GRE)	• VXLAN (default 4789) • L2GRE	UCT-V or Subnet IP	Allows GigaVUE V Series Node to (VXLAN/L2GRE) tunnel traffic to UCT-V.
Inbound	UDPGRE	4754	Ingress Tunnel	Allows GigaVUE V Series Node to communicate and tunnel traffic from UDPGRE Tunnel
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user initiated management and diagnostics, specifically when using third party orchestration.
Outbound	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM
Outbound	• UDP (VXLAN) • IP Protocol (L2GRE)	VXLAN (default 4789)	Tool IP	Allows GigaVUE V Series Node to communicate and tunnel traffic to the tool
Outbound	UDP	2056	GigaVUE-FM IP	Allows GigaVUE V Series Node to send Application Intelligence, Application Visualization reports to GigaVUE-FM
Outbound	UDP	2055	Tool IP	Allows GigaVUE V Series Node to send NetFlow traffic to external tool.
Outbound	UDP	514	Tool IP	Allows GigaVUE V Series Node to send Application Metadata Intelligence log messages to external tool.

Direction	Protocol	Port	CIDR	Purpose
Outbound (optional)	ICMP	• echo request • echo reply	Tool IP	Allows GigaVUE V Series Node to send health check tunnel destination traffic
Outbound (This is the port used for Third Party Orchestration)	TCP	8891	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE V Series Proxy when GigaVUE V Series Proxy is used.
Outbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE-FM IP Address	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE-FM when GigaVUE V Series Proxy is not used.
Bidirectional	TCP	11443	GigaVUE V Series Node subnet	Allows to securely transfer the traffic in between GigaVUE V Series Nodes.
Universal Cloud Tap - Container deployed inside Kubernetes worker node				
Outbound	TCP	42042	Any IP address	Allows UCT-C to send statistics to UCT-C Controller.
UCT-C Controller deployed inside Kubernetes worker node				
Inbound	TCP	8443 (configurable)	Any IP address	Allows UCT-C Controller to communicate with GigaVUE-FM
Outbound	TCP	5671	Any IP address	Allows UCT-C controller to send statistics to GigaVUE-FM.
Outbound	TCP	VXLAN (default 4789)	Any IP address	Allows UCT-C Controller to communicate and tunnel traffic to the tool
Outbound	TCP	443	Any IP address	Allows UCT-C Controller to communicate with GigaVUE-FM

Network Firewall Requirements for OpenStack

Following are the Network Firewall Requirements for OpenStack.

NOTE: When using dual stack network, the below mentioned ports must be opened for both IPv4 and IPv6.

Direction	Ether Type	Protocol	Port	CIDR	Purpose
GigaVUE-FM					
Inbound	HTTPS	TCP	443	Any IP address	Allows users to connect to the GigaVUE-FM GUI.
Inbound	IPv4	UDP	53	Any IP address	Allows GigaVUE-FM to communicate with standard DNS server
Inbound	Custom TCP Rule	TCP	5671	GigaVUE V Series Node IP	Allows GigaVUE V Series Nodes to send traffic health updates to GigaVUE-FM Allows Next Generation UCT-V to send statistics to GigaVUE-FM.
Outbound (optional)	Custom TCP Rule	TCP	8890	V Series Proxy IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate with V Series node
UCT-V Controller					
Inbound	Custom TCP Rule	TCP	9900	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with UCT-V Controllers
Inbound (This is the port used for Third Party Orchestration)	Custom TCP Rule	TCP(6)	8891	UCT-V or Subnet IP	Allows UCT-V Controller to communicate the registration requests from UCT-V and forward the same to GigaVUE-FM.
Outbound (This is the port used for Third Party Orchestration)	Custom TCP Rule	TCP(6)	443	GigaVUE-FM IP	Allows UCT-V Controller to communicate the registration requests to GigaVUE-FM
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM

Direction	Ether Type	Protocol	Port	CIDR	Purpose
UCT-V					
Inbound	Custom TCP Rule	TCP	9901	Custom UCT-V Controller IP	Allows UCT-V Controllers to communicate with UCT-Vs
Outbound (This is the port used for Third Party Orchestration)	Custom TCP Rule	TCP(6)	8891	UCT-V or Subnet IP	Allows UCT-V to communicate with UCT-V Controller for registration and Heartbeat
Outbound	Custom TCP Rule	TCP	11443	UCT-V subnet	Allows UCT-V to securely transfer the traffic to GigaVUE V Series Node
UCT-V OVS Controller					
Inbound	Custom TCP Rule	TCP	9900	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with UCT-V OVS Controllers
UCT-V OVS Agent					
Inbound	Custom TCP Rule	TCP	9901	Custom UCT-V OVS Controller IP	Allows UCT-V OVS Controllers to communicate with UCT-V OVS Agents
GigaVUE V Series Proxy					
Inbound	IPv4	TCP	8890	GigaVUE-FM IP address	Allows GigaVUE-FM to communicate with GigaVUE V Series Proxys.
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows V Series Proxy to communicate with GigaVUE V Series Nodes
GigaVUE V Series Node					
Inbound	Custom TCP Rule	TCP(6)	8889	GigaVUE V Series Proxy IP address	Allows GigaVUE V Series Proxys to communicate with GigaVUE V Series nodes
Outbound	IPv4	TCP	8890	GigaVUE-FM IP address	Allows GigaVUE V Series Node to communicate with GigaVUE V Series Proxy

Direction	Ether Type	Protocol	Port	CIDR	Purpose
Outbound	Custom UDP Rule	UDP	• VXLAN (default 4789) • L2GRE (IP 47)	Tool IP	Allows V Series node to communicate and tunnel traffic to the Tool
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM
Bi-directional	Custom TCP Rule	TCP	11443	GigaVUE V Series Node subnet	Allows to securely transfer the traffic in between GigaVUE V Series Nodes.

Network	Purpose
Management	Identify the subnets that GigaVUE-FM uses to communicate with the GigaVUE V Series nodes and controllers.
Data	Identify the subnets that receives the mirrored tunnel traffic from the monitored instances. In data network, if a tool subnet is selected then the V Series node egress traffic on to the destinations or tools.

NOTE: If you are using IPv6 in the tenant network, then it is recommended to use SLAAC or stateless DHCPv6 for dynamic address assignment.

Network Firewall Requirements for VMware

This section consist of following topics:

- Network Firewall Requirements for ESXi
- Network Firewall Requirements for NSX-T

Network Firewall Requirements for ESXi

Following are the Network Firewall Requirements for GigaVUE V Series Node deployment.

Source	Destination	Source Port	Destination Port	Protocol	Service	Purpose
GigaVUE-FM	ESXi hosts	Any (1024-65535)	443	TCP	https	Allows GigaVUE-FM to communicate with vCenter and all ESXi hosts to import the V Series OVA files
	vCenter					
GigaVUE-FM	GigaVUE V Series Nodes	Any (1024-65535)	8889	TCP	Custom API	Allows GigaVUE-FM to communicate with GigaVUE V Series Node
GigaVUE-FM	GigaVUE V Series Nodes	Any (1024-65535)	5671	TCP	Custom TCP	Allows GigaVUE-FM to receive the traffic health updates with GigaVUE V Series Node
Administrator	GigaVUE-FM	Any (1024-65535)	443	TCP	https	Management connection to GigaVUE-FM
			22		ssh	
Remote Source	GigaVUE V Series Nodes	Custom Port (VXLAN and UDPGRE),N/A for GRE	4789	UDP	VXLAN	Allows to UDPGRE Tunnel to communicate and tunnel traffic to GigaVUE V Series Nodes (Applicable for Tunnel Ingress option only)
			N/A	IP 47	GRE	
			4754	UDP	UDPGRE	
GigaVUE V Series Nodes	Tool/ HC Series instance	Custom Port (VXLAN),N/A for GRE	4789	UDP	VXLAN	Allows GigaVUE V Series Node to communicate and tunnel traffic to the Tool
			N/A	IP 47	GRE	
GigaVUE V	Tool/ HC Series	N/A	N/A	ICMP	Echo	Allows

Series Nodes	instance				Request Echo Response	GigaVUE V Series Node to health check tunnel destination traffic (Optional)
GigaVUE V Series Nodes	GigaVUE-FM	Any (1024-65535)	Any (1024-65535)	TCP	Custom TCP	Allows GigaVUE V Series Nodes to communicate the traffic health updates with GigaVUE-FM

Network Firewall Requirements for NSX-T

Following are the Network Firewall Requirements for GigaVUE V Series Node deployment.

Source	Destination	Source Port	Destination Port	Protocol	Service	Purpose
GigaVUE-FM	ESXi hosts NSX-T Manager vCenter	Any (1024-65535)	443	TCP	https	Allows GigaVUE-FM to communicate with vCenter, NSX-T and all ESXi hosts.
GigaVUE-FM	GigaVUE V Series Node	Any (1024-65535)	8889	TCP	Custom API	Allows GigaVUE-FM to communicate with GigaVUE V Series Node
Administrator	GigaVUE-FM	Any (1024-65535)	443 22	TCP	https ssh	Management connection to GigaVUE-FM
GigaVUE-FM	GigaVUE V Series Node	Any (1024-65535)	5671	TCP	Custom TCP	Allows GigaVUE-FM to receive the traffic health updates with GigaVUE V Series Node

Remote Source	GigaVUE V Series Node	Custom Port (VXLAN and UDPGRE),N/A for GRE	4789	UDP	VXLAN	Allows to UDPGRE Tunnel to communicate and tunnel traffic to GigaVUE V Series Nodes (Applicable for Tunnel Ingress option only)
			N/A	IP 47	GRE	
			4754	UDP	UDPGRE	
GigaVUE V Series Node	Tool/ HC Series instance	Custom Port (VXLAN),N/A for GRE	4789	UDP	VXLAN	Allows GigaVUE V Series Node to communicate and tunnel traffic to the Tool
			N/A	IP 47	GRE	
GigaVUE V Series Node	Tool/ HC Series instance	N/A	N/A	ICMP	echo Request	Allows V Series node to health check tunnel destination traffic (Optional)
					echo Response	
GigaVUE V Series Node	GigaVUE-FM	Any (1024-65535)	5671	TCP	Custom TCP	Allows GigaVUE V Series Nodes to communicate the traffic health updates with GigaVUE-FM
GigaVUE-FM	External Image Server URL	Any (1024-65535)	Custom port on web Server	TCP	http	Access to image server to image lookup and checks, and downloading the image
NSX-T Manager						
vCenter						
ESXi host						
NSX-T Manager	GigaVUE-FM	Any (1024-65535)	443	TCP	http	When using GigaVUE-FM as the image server for uploading the GigaVUE V Series Image.
vCenter						
ESXi host						

Network Requirements for Gigamon Containerized Broker (GCB)

The following table describes the Kubernetes network requirements for GCB to work efficiently.

Direction	Type	Protocol	Port	CIDR	Purpose
Gigamon Containerized Broker deployed inside Kubernetes worker node					
Outbound	HTTPS	TCP	443	Any IP address	Allows GCB Controller to communicate with GigaVUE-FM
Inbound	HTTPS	TCP	8443 (configurable)	Any IP address	Allows GigaVUE-FM to communicate with GCB Controller.
Outbound	HTTPS	TCP	42042	Any IP address	Allows GCB to communicate with GigaVUE-FM to send statistics data.

Network Firewall Requirements for Nutanix

This section consists of the following topics:

- Network Firewall Requirements for Nutanix (GigaVUE-VM)
- Network Firewall Requirements for Nutanix (GigaVUE V Series Node)

Network Firewall Requirements for Nutanix (GigaVUE-VM)

Following are the Network Firewall Requirements for Gigamon fabrics for Nutanix deployments.

Direction	Type	Protocol	Port	CIDR	Purpose
GigaVUE-FM Inside Nutanix					
Inbound	HTTPS	TCP	443	Anywhere Any IP	Allow GVMs, GigaVUE Cloud Suite fabric

Direction	Type	Protocol	Port	CIDR	Purpose
					controllers, and GigaVUE-FM administrators to communicate with GigaVUE-FM
Inbound	SSH	TCP	22	Anywhere Any IP	Allow GVMs, GigaVUE Cloud Suite fabric controllers, and GigaVUE-FM administrators to communicate with GigaVUE-FM
Outbound	Custom TCP Rule	TCP	9902	GigaVUE Cloud Suite Fabric Controller IP	Allows GigaVUE-FM to communicate with GigaVUE Cloud Suite Fabric Controllers IP.
GigaVUE Cloud Suite Fabric Controller					
Inbound	Custom TCP Rule	TCP	9902	GigaVUE-FM IP	Allows GVM to communicate with GigaVUE Cloud Suite Fabric Controllers.
Outbound	Custom TCP Rule	TCP	9903	GVM IP Subnet	Allows GigaVUE Cloud Suite Fabric Controller to communicate with GVMs.
GVM					
Inbound	Custom TCP Rule	TCP	9903	GigaVUE Cloud Suite Fabric Controller IP	Allows GigaVUE Cloud Suite Fabric Controller IP to communicate with GVMs.
Outbound	Custom UDP Rule	UDP	• VXLAN (default 4789) • L2GRE (IP 47)	Tool IP	Allows GVM to communicate and tunnel traffic to the tool
Outbound	Custom ICMP Rule	ICMP	-	Tool IP	Allows GVM to health check the tool traffic.

Network Firewall Requirements for Nutanix (GigaVUE V Series Node)

Following are the Network Firewall Requirements for Gigamon fabrics for Nutanix deployments.

Direction	Type	Protocol	Port	CIDR	Purpose
GigaVUE-FM					
Inbound	HTTPS	TCP	443	Anywhere Any IP	Allows GigaVUE® V Series Nodes, GigaVUE V Series Proxy, and GigaVUE-FM administrators to communicate with GigaVUE-FM
Inbound	SSH	TCP	22	Anywhere Any IP	Allows GigaVUE® V Series Nodes, GigaVUE V Series Proxy, and GigaVUE-FM administrators to communicate with GigaVUE-FM
Outbound (optional)	Custom TCP Rule	TCP	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Node
Outbound	Custom TCP Rule	TCP	9440	Prism Central IP, Prism Element IP	Allows GigaVUE-FM to communicate with Prism Central and Prism Element.
GigaVUE V Series Node					
Inbound	Custom TCP Rule	TCP	9903	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Proxy to communicate with GigaVUE® V Series Nodes
Inbound	UDP	UDPGRE	4754	Ingress Tunnel	Allows to UDPGRE tunnel to communicate and tunnel traffic toGigaVUE V Series Nodes
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows GigaVUE® V Series Node to communicate and tunnel traffic to the Tool
Outbound	Custom UDP Rule	• UDP (VXLAN) • IP Protocol (L2GRE)	• VXLAN (default 4789) • L2GRE (IP 47)	Tool IP	Allows GigaVUE® V Series Node to communicate and tunnel traffic to the Tool
Outbound (optional)	Custom ICMP Rule	ICMP	• echo request • echo reply	Tool IP	Allows GigaVUE® V Series Node to health check the tunnel destination traffic.

Direction	Type	Protocol	Port	CIDR	Purpose
GigaVUE V Series Proxy (optional)					
Inbound	Custom TCP Rule	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Node

Network Firewall Requirements for Universal Container Tap

Following are the Network Firewall Requirements for Universal Container Tap (UCT).

Direction	Type	Protocol	Port	CIDR	Purpose
Universal Cloud Tap - Container deployed inside Kubernetes worker node					
Outbound	HTTPS	TCP	443	Any IP address	Allows UCT-C Controller to communicate with GigaVUE-FM
Inbound	HTTPS	TCP	8443 (configurable)	Any IP address	Allows GigaVUE-FM to communicate with UCT-C Controller.
Outbound	HTTPS	TCP	5671	Any IP address	Allows UCT-C controller to send statistics to GigaVUE-FM through Rabbit-MQ port.
Outbound	HTTPS	TCP	42042	Any IP address	Allows UCT-C to send statistics information to UCT-Ccontroller.
Outbound	HTTPS	TCP	4789	Any IP address	VXLAN Default Port

Network Firewall Requirements for Gigamon Containerized Box

Following are the Network Firewall Requirements for Gigamon Containerized Box (GCB).

Direction	Type	Protocol	Port	CIDR	Purpose
Gigamon Containerized Broker deployed inside Kubernetes worker node					
Outbound	HTTPS	TCP	443	Any IP address	Allows GCB Controller to communicate with GigaVUE-FM
Inbound	HTTPS	TCP	8443 (configurable)	Any IP address	Allows GigaVUE-FM to communicate with GCB Controller.
Outbound	HTTPS	TCP	42042	Any IP address	Allows GCB to communicate with GigaVUE-FM to send statistics data.

Additional Sources of Information

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

- Documentation
- Documentation Feedback
- Contact Technical Support
- Contact Sales
- The VÜE Community

Documentation

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

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

Table 1: Documentation Set for Gigamon Products

GigaVUE 6.6 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE devices; reference information and specifications for the respective GigaVUE devices
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-HCT Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide
GigaVUE-TA100 Hardware Installation Guide
GigaVUE-TA200 Hardware Installation Guide

GigaVUE 6.6 Hardware and Software Guides
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliances Guide
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Applications Guide
GigaVUE V Series Quick Start Guide
GigaVUE Cloud Suite Deployment Guide - AWS
GigaVUE Cloud Suite Deployment Guide - Azure
GigaVUE Cloud Suite Deployment Guide - OpenStack
GigaVUE Cloud Suite Deployment Guide - Nutanix
GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
Universal Cloud Tap - Container Deployment Guide
Gigamon Containerized Broker Deployment Guide

GigaVUE 6.6 Hardware and Software Guides
GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions
GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions
Reference Guides
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices
GigaVUE-OS Security Hardening Guide
GigaVUE Firewall and Security Guide
GigaVUE Licensing Guide
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **NOTE:** Release Notes are not included in the online documentation. **NOTE:** Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software and Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

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

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

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

1. Log in to My Gigamon.
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "6.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 6.6.xx.

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

Documentation Feedback

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

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

Documentation Feedback Form		
About You	**Your Name**	
	Your Role	
	Your Company	
For Online Topics	**Online doc link**	*(URL for where the issue is)*
	Topic Heading	*(if it's a long topic, please provide the heading of the section where the issue is)*

For PDF Topics	**Document Title**	*(shown on the cover page or in page header)*
	Product Version	*(shown on the cover page)*
	Document Version	*(shown on the cover page)*
	Chapter Heading	*(shown in footer)*
	PDF page #	*(shown in footer)*
How can we improve?	**Describe the issue**	*Describe the error or issue in the documentation.* *(If it helps, attach an image to show the issue.)*
	How can we improve the content? **Be as specific as possible.**	
	Any other comments?	

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The VÜE Community

The VÜE Community is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the VÜE Community site to:

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

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

Register today at community.gigamon.com

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

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

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

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

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

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)