

GigaVUE-OS, GigaVUE-FM, and GigaVUE® Cloud Suite Release Notes 6.13.xx

Updated: Friday, September 11, 2026 Document Version: 4.0

Table of Contents

GigaVUE-OS, GigaVUE-FM, and GigaVUE® Cloud Suite Release Notes 6.13.xx	1
Change Notes	2
Introduction	2
View Known and Resolved Issues in the Community Portal	3
Important Document References	4
Release 6.13.02 GigaVUE-OS	5
Release 6.13.02 GigaVUE Cloud Suite	5
New Features in 6.13.02	5
Release 6.13.01 GigaVUE Cloud Suite	6
Release 6.13.01 GigaVUE-OS	6
Release 6.13.00 GigaVUE-OS,GigaVUE-FM and GigaVUE-Cloud-Suite	6
New Features in 6.13.00	6
Announcements and Deprecation Notices	10
Installation and Upgrade	10
GigaVUE-OS Upgrade	10
GigaVUE-FM Installation	12
GigaVUE-FM Upgrade	13
Additional Information	16
Contacting Gigamon Support	16
Copyright	16
Trademark Attributions	16
The VÜE Community	17

Change Notes

Date	Revision	Change
08/31/2026	4.0	This version of the Release Notes includes resolved and known issues. Refer to View Known and Resolved Issues in the Community Portal.
07/10/2026	3.0	This version of the Release Notes includes updates and additions made for the 6.13.02 GA. Refer to New Features in 6.13.02.
06/04/2026	2.0	This version of the Release Notes includes updates and additions made for the 6.13.01 GA. Refer to Security Updates.
02/26/2026	1.0	The original release of this document with version 6.13 GA.

Introduction

These Release Notes describe the new features and enhancements, resolved issues, and known issues for GigaVUE® software version , including:

Product	Summary
GigaVUE-FM	With a web-based interface, GigaVUE-FM provides high-level visibility, reporting, and management of both the physical and virtual traffic visibility nodes that form the deep observability pipeline.
G-TAP A Series 2	Securely manageable active network TAPs that mirror network traffic and utilize the "Always-On" architecture.
GigaVUE HC Series and TA Series Visibility Fabric™ Nodes	With a powerful command-line interface (CLI), the physical GigaVUE-HC Series and GigaVUE TA Series appliances can replicate, filter, optimize and selectively forward network traffic to monitoring, management, and security tools. GigaVUE-OS can be used in conjunction with GigaVUE-FM to provide extended visibility fabric management and reporting capabilities.
GigaVUE Cloud Suite	The GigaVUE Cloud Suite provides consistent visibility into data in motion in cloud-based environments such as AWS, Azure, Google Cloud Platform, Kubernetes, Nutanix, OpenStack and VMware. The GigaVUE Cloud Suite extends GigaVUE traffic distribution principles to containerized and virtualized environments, allowing users to filter, monitor, optimize and forward traffic in private and public clouds environments to monitoring and analysis tools.
GigaSMART®	GigaSMART consists of a number intelligent traffic handling and processing applications and capabilities for the purpose of optimizing and transforming acquired network traffic as needed. GigaSMART provides these extended capabilities on top of the base GigaVUE-OS and GigaVUE Cloud Suite functionality.

To learn more about GigaVUE-OS, GigaVUE Fabric Manager (GigaVUE-FM), TA Series, GigaVUE HC Series, GigaVUE Cloud Suite, and other products, visit www.gigamon.com.

View Known and Resolved Issues in the Community Portal

Use the Known and Resolved Issues page in the Gigamon Community Portal to review the health of a release before you upgrade. This page lists:

- Open issues (known issues)
- Fixed issues
- Security fixes

The data is sourced directly from Gigamon's issue-tracking system and is always up to date. You must sign in to the Community Portal to view this information.

Before you begin

- Make sure you have a valid Community Portal account.
- Access is limited to signed-in customers and partners.

Access the Known and Resolved Issues page

1. Open a web browser and sign in to the Gigamon Community Portal.
2. From the top menu, select: **More > Software & Release Notes > Known & Resolved Issues**

The page displays the full list of issues.

Filter the list

Use the filters at the top of the page to narrow results by Status, Bug ID, Component, and Releases.

Common filter scenarios

- View known issues for a release
 - Set Status to Open
 - Select the required version in Releases

- View fixed issues for a release
 - Select the required values in Status and Releases
- View security fixes
 - Set Component to infosec
 - Select the required version in Releases

Interpret the results

Each row represents one issue.

- If Fixed Version shows a version, the issue is fixed in that release.
- If Fixed Version is blank, the issue is still open.

Notes

- Use this page during upgrade planning to assess risk.
- Check both open and fixed issues to understand release stability.

Important Document References

This section lists all information sections that you may require to refer to while updating your device to the 6.13.00 software release.

System and Support Requirements	Refer To
System Requirements	
Firmware/BIOS information for the GigaVUE-FM Hardware Appliance	GigaVUE-FM Hardware Appliance System Requirements
VMware Requirements for GigaVUE-FM Installation	Installing GigaVUE-FM on VMware ESXi
Minimum Virtual Computing Requirements for GigaVUE-FM Installation	Supported Virtual Computing Requirements for GigaVUE-FM
GigaVUE Cloud Suite System Requirements	
Nutanix Requirements	Supported Requirements - Nutanix
OpenStack Requirements	Supported Compute Requirements for OpenStack
OVS-Mirror Requirements	Prerequisites for OVS Mirroring
Supported Hypervisors for GigaVUE V Series Node	Supported Hypervisors for VMware
Supported Operating Systems for UCT-V	Supported Operating Systems for UCT-V
Kernel and CPU Requirements for UCT-C	Kernel and CPU Requirements for Universal Cloud

System and Support Requirements	Refer To
	Tap - Container
Supported Platforms for UCT-C	Supported Platforms for UCT-C
Support and Compatibility	
GigaVUE-FM and GigaVUE-OS Compatibility	Device and Configuration Management for GigaVUE-FM
Supported Browsers for GigaVUE-FM	Supported Browsers for GigaVUE-FM
Line Card or Module Removal Procedure (Hot Removal)	Module Removal and Replacement Procedure (Hot Removal)

Release 6.13.02 GigaVUE-OS

GigaVUE 6.13.02 Software offers resolved and known issues. Refer to [View Known and Resolved Issues in the Community Portal](#).

Release 6.13.02 GigaVUE Cloud Suite

GigaVUE 6.13.02 Software offers resolved and known issues. Refer to [View Known and Resolved Issues in the Community Portal](#).

New Features in 6.13.02

GigaVUE 6.13.02 Software offers usability improvements, resolved issues, and the new capabilities described below.

Product Area	Feature Summary
Cloud Suite	Flexible Npcap Support for UCT-V on Windows UCT-V for Windows now provides more flexible Npcap handling during installation. If the installer detects an existing Npcap driver, users can continue with the existing driver. Compatible Npcap: OEM-licensed Npcap version 1.81 or later. For more details refer to: Windows_UCT-V_Installation NOTE: UCT-V and UCT-V Controller need to be in the v.6.13.02.

Release 6.13.01 GigaVUE Cloud Suite

GigaVUE 6.13.01 Software offers resolved and known issues. Refer to [View Known and Resolved Issues in the Community Portal](#).

Release 6.13.01 GigaVUE-OS

GigaVUE 6.13.01 Software offers resolved and known issues. Refer to [View Known and Resolved Issues in the Community Portal](#).

Release 6.13.00 GigaVUE-OS, GigaVUE-FM and GigaVUE-Cloud-Suite

GigaVUE 6.13.00 Software offers usability improvements, resolved issues, and the new capabilities described below.

New Features in 6.13.00

Product Area	Feature Summary
Cloud Suite	Ericsson vTAP Domain Tagging Support This feature enhances Ericsson vTAP support on the GigaVUE V Series by adding domain aware classification and VLAN based tagging for both SBI and non-SBI flows. It introduces a configurable Ericsson domain-to-VLAN mapping table in the PCAPNG app, FQDN-based SCP detection and destination IP selection in the 5G SBI application, and optional VLAN tagging on VXLAN/L2GRE egress tunnels. These updates let deployments steer traffic from specific Ericsson network functions (such as pc-mm, pc-sm, ccsn-5gc, sc-scp), separate unclassified flows, and meet NetScout probe requirements—improving visibility, simplifying troubleshooting and enabling accurate domain-level monitoring of Ericsson 5G core traffic. Refer to 5G-Service Based Interface Application .
	GCB Sequencing of packets This feature enhances Gigamon GCB's packet reordering capabilities in distributed environments. Previously, GCB could reorder and stitch transactions only when all packets for a transaction arrived at the same instance. With this update, GCB instances can now forward incomplete transactions to each other, enabling transaction stitching across multiple instances. This improvement enhances scalability and reliability, ensures more comprehensive transaction reconstruction, and provides improved support for dynamic scaling and failover in distributed deployments. Refer to Configure GCB Settings .

Product Area	Feature Summary
	Nokia HEP3 Service Map Support The 5G Cloud application on GigaVUE V Series enhances Nokia HEP3 handling by introducing Nokia HEP3 Inbound with a configurable Service Map that normalizes ephemeral SIP request/response ports for IMS vTAP traffic. This update adds deterministic SIP port mapping through a centralized service mapping table enabling consistent SIP translation and accurate packet synthesis for downstream tools while simplifying integrations and reducing operational complexity in Nokia IMS deployments. Refer to 5G Cloud Nokia HEP3 Support (Non-SBI). Azure support for IL6 This feature extends GigaVUE-FM's Azure integration to support IL6 workloads in Azure Government Secret and Top Secret regions. GigaVUE-FM now supports importing custom root CA certificates into its Java trust store to enable secure TLS connectivity to isolated, air gapped service endpoints. These enhancements allow government and defense deployments to run GigaVUE-FM in IL6 environments while maintaining secure, compliant access to non-public Azure services. Refer to Configure Custom Settings for Azure Secret and Top Secret Regions. AWS support for IL6 This feature extends GigaVUE-FM's AWS integration to support IL6 workloads in AWS Government Secret and Top Secret regions. GigaVUE-FM now supports importing custom root CA certificates into its Java trust store to enable secure TLS connectivity to isolated, air gapped service endpoints. These enhancements allow government and defense deployments to run GigaVUE-FM in IL6 environments while maintaining secure, compliant access to non-public AWS services. Refer to Configure Custom Settings for AWS Secret and Top Secret Regions.
GigaVUE-FM Core	GigaVUE-FM Ansible NOTE: GigaVUE-FM Ansible is released as a Early Access (EA) feature, providing you with the opportunity to evaluate its capabilities before its General Availability (GA) release. For access to EA software please contact your Gigamon account team or file a support case. GigaVUE-FM Ansible enables automation of GigaVUE-FM operations using reusable playbooks, helping you streamline configuration, manage deployments consistently, and reduce manual effort. By leveraging Ansible, you can integrate GigaVUE-FM into existing automation workflows and improve operational efficiency across your environment. For instructions on setting up and using Ansible with GigaVUE-FM, refer to the GigaVUE-FM Ansible Users Guide.

Product Area	Feature Summary
	Audit button for CDA in GigaVUE-FM GigaVUE-FM allows you to generate a Customer Deployed Assets (CDA) report. It creates a detailed report of all deployed hardware and software by SKU, including GigaVUE-OS and GigaVUE-FM versions. GigaVUE-FM also automatically generates a CDA report every Sunday. Refer to Generate Report for Customer Deployed Assets. Spine Source Map Mode in Fabric Maps: This feature introduces a global Spine Source Map Mode setting (SEPARATE/COMBINE) that controls whether leaf-and-spine clusters create one spine-source cluster-level map per spine CGS or a single combined map across all spine CGSs, improving scalability and correctness for fabric maps and traffic policies that traverse spine nodes. Refer to Supported Topologies in Fabric Maps Traffic Policy Traffic Policy introduces a unified way to define how traffic is filtered, processed, and delivered across your monitoring and security tools. Instead of managing multiple maps and configurations, you can now express your intent in a single policy. This reduces manual effort and ensures consistent traffic handling. Benefits include: • Centralized, simplified configuration • Reduced operational complexity • Consistent, predictable traffic workflows Refer to Traffic Policy.
GigaSMART	Artificial Intelligence (AI) Traffic Insights Artificial Intelligence (AI) Traffic Intelligence Application Intelligence supports monitoring usage of new AI apps (12) and Vector Database protocols (4) accessed via web browser or desktop/mobile app for Governance, Risk and Compliance (GRC). In addition, it supports monitoring usage of AI apps involving public APIs for 24 apps (check for WebAPI in the Classification Workflows in the Protobook). You can access the Protobook from the GigaVUE-FM in the following ways: • On the left navigation pane, click Setting > Support > App Protobook. OR • Go to Admin > App Protobook. Mutual TLS (mTLS) Support for Inline TLS/SSL Decryption Inline TLS/SSL decryption now supports inbound mutual TLS (mTLS) on Gen 3 platforms. With mTLS enabled, client certificates are validated using a dedicated client trust store, configurable client authentication policies (for example, how to handle expired, self-signed, or unknown-CA certificates) are applied, and new client authentication statistics are exposed as dashboard metrics so you can monitor mTLS adoption and health. This initial base mTLS support is

Product Area	Feature Summary
	available only for inbound Flexible Inline deployments and is not supported with L3 Tool NAT/PAT, HSM, One-Arm mode, Tool Early Engage/Inspect, or ICAP workflows. Refer to Inline SSL Decryption.
	Adaptive Packet Filtering with Regex masking on Gen 3 GigaSMART Modules APF on Gen 3 GigaSMART modules now supports regex-based masking. Using PCRE compatible APF rules, you can identify and mask Personally Identifiable Information (PIIs) such as Social Security Number (SSN), credit card number, account ID, password and others in packet payloads to meet your organization's security policy and compliance needs. Refer to GigaSMART Adaptive Packet Filtering APF.
	Adaptive Packet Filtering second-level map scale increase on GigaVUE HC Series platforms Increased the per vPort limit for Adaptive Packet Filtering second-level maps from 5 to 25 on supported GigaVUE HC Series platforms, enabling more granular APF-based filtering and more concurrent APF policies per vPort while retaining the existing APF configuration model. The higher map limit applies only when the vPort is configured solely with APF (no other GigaSMART applications or operations are enabled). Refer to GigaSMART Adaptive Packet Filtering APF.
GigaVUE-OS	Support for advanced VLAN manipulation The advanced VLAN manipulation feature extends the existing VLAN manipulation to support Modify and Strip in addition to Add on the outer VLAN tag. It lets you add, replace, or remove the outer VLAN tag on ingress traffic at the map or rule level, with hardware-based processing for line-rate performance. Refer to VLAN Manipulation.
	Introducing enable packet capture on the IP interfaces The PCAP on IP interfaces feature extends the existing packet capture capability to ports associated with IP interfaces. It lets you capture ingress, egress, or bidirectional traffic on IP interfaces using the same CLI syntax, filters, and behavioral rules as standard PCAP, while preserving core IP functions such as ARP and ICMP. In GigaVUE-FM, you configure this capture directly from the IP Interface page using the Troubleshoot > Configure PCAP option. Refer to Packet Capture (PCAP).
Hardware	New DAC Cable, Q28 504, and Q28 511 Transceiver 100Gb Direct Attach Copper Cable (DAC), Q28-504 100G QSFP28 ER4, and Q28-511 100Gb QSFP28 DR1 transceivers are now supported. Refer to Transceivers.

Announcements and Deprecation Notices

- **Support for Entrust/nCipher HSM:** Support for Entrust/nCipher HSM is going under a redesign and as a result being temporarily removed from GigaVUE-OS and GigaVUE-FM. This change affects Gen2 DSSL HSMs (nCipher v1.0) and Gen3 HSMs using nCipher 12.6 (nshield_12_60) support. Thales Luna HSM support on Gen3 devices remains unaffected by this change.

NOTE: Upgrades from 6.13.00 or lower versions to 6.13.01 will be blocked if any Entrust/nCipher HSM configuration is present. Refer to [GigaVUE-FM Upgrade](#).

- GigaVUE-HC3GigaSMART Gen2 Card last supported Software version is 6.12.x. Removed the support for the Gen2 card (SMT-HC3-C05 and SMT-HC3-C05-HW) from release 6.13.

Installation and Upgrade

Complete installation and upgrade instructions can be found in the respective release specific product documentation here:

<https://docs.gigamon.com/pdfs/Content/Documentation-downloads.html>. This section provides additional advice that is important to know before installing or that is specific to this release.

Installation and Upgrade Documentation

Product	Reference	Includes
GigaVUE-OS	<i>GigaVUE-OS Upgrade Guide</i>	Instructions for installing the bootloader and upgrading all GigaVUE HC Series and GigaVUE TA Series visibility nodes and certified traffic aggregation commercial off-the-shelf (COTS) boxes, as standalone nodes or clusters.
GigaVUE-FM	<i>GigaVUE-FM Installation and Upgrade Guide</i>	Instructions to install GigaVUE-FM on VMware ESXi, MS Hyper-V, AWS, Azure, OpenStack, Kubernetes, Nutanix and KVM.
GigaVUE Fabric Components	GigaVUE-FM Installation and Upgrade Guide	Instructions to install and upgrade the GigaVUE fabric components.

GigaVUE-OS Upgrade

To upgrade GigaVUE-OS, the recommended procedure is to back-up your settings on each node and perform the pre-upgrade checks (default admin password, the maximum number of images, U-Boot version, and Coreboot version) before installing the image. The upgrade path from previous versions of the GigaVUE-OS varies depending on the current OS version and node type. It is recommended that you plan your upgrade before performing any upgrade steps.

Support for SHA1

SHA1 support has been removed from 5.13.xx to improve security.

Rules and Notes

The following rules and notes must be considered while upgrading:

- The upgrade to 6.13.01 will be blocked if you have any Entrust/nCipher HSM integrations. Remove the Entrust/nCipher integration before you attempt to upgrade to 6.13.01.
- Upgrade of an HC3 chassis with an SMT-C05 card is blocked for version 6.13.01. Replace the SMT-C05 card with an SMT-C08 card before upgrading to 6.13.01.
- Before you upgrade to version 6.11 on a FIPS-enabled device, complete the following steps to ensure a successful upgrade:
 - Delete all Inline SSL (iSSL) configurations and the keystore before the upgrade. After the upgrade, reconfigure the Gen 3 GigaSMART module.
 - Remove all HSM and HSM Groups, including nCipher and Luna, from the device.
 - Delete all Inline SSL (iSSL) configurations for Gen 2 GigaSMART modules, since they do not support FIPS 140-3. If you require Inline SSL on GigaVUE-HC1 or GigaVUE-HC3 devices, add a Gen 3 GigaSMART card.
 - Remove SNMPv3 configurations that use the MD5 authentication protocol because FIPS 140-3 does not support MD5 algorithms.
 - If you don't complete all required steps before upgrading, the upgrade will fail. The system will automatically revert to the previous version.
- **6.2.00.04:** Software version 6.2.xx is replaced with 6.2.00.04.
- **6.1.01.04:** Software version 6.1.01 is replaced with 6.1.01.04.
- GigaVUE-HCT is supported from 6.5.00.
- If you are installing the SMT-HC1-S module in a GigaVUE-HC1 Chassis, use the recommended upgrade path specific to this module. Refer to *SMT-HC1-S (Gen 3 GigaSMART Card)* in GigaVUE-HC1 Hardware Installation Guide, for details.
- **If upgrading from GigaVUE-OS versions lower than 6.0:** Refer to the "Supported Upgrade Path—Standalone Nodes" section in the GigaVUE-OS Upgrade Guide that is specific to the release.
- **If upgrading from GigaVUE-OS versions lower than 5.5.xx:** While upgrading from any GigaVUE-OS version lower than v5.5.xx, an association of more than one vport to the same GigaSMART group needs to be removed for any existing GTP GigaSMART operation.
- **If upgrading from GigaVUE-FM versions lower than 5.10.01:** The size of the GigaVUE-OS image for GigaVUE-HC1 increased in 5.10.01. Upgrading directly from a pre-5.9 release to 5.10.01 or above is not supported. The following upgrade path is recommended: 5.9.00.04 or 5.9.01 → 5.10.01.
- You cannot upgrade GigaVUE-HC2 nodes beyond v6.5.xx.

Table 1: GigaVUE-OS Upgrade Summary table

To upgrade to 6.13.xx from...	Use the recommended upgrade path for the device...
	GigaVUE HC Series, GigaVUE TA Series, and G-TAP A Series 2
v6.12.xx	6.12.xx ► 6.13.xx
v6.11.xx	6.11.xx ► 6.12.xx ► 6.13.xx
v6.10.xx	6.10.xx ► 6.12.xx ► 6.13.xx
v6.9.xx	6.9.xx ► 6.12.xx ► 6.13.xx
v6.8.xx	6.8.xx ► 6.9.xx ► 6.12.xx ► 6.13.xx
v6.7.xx	6.7.xx ► 6.9.xx ► 6.12.xx ► 6.13.xx
v6.6.xx	6.6.xx ► 6.9.xx ► 6.12.xx ► 6.13.xx
v6.5.xx	6.5.xx ► 6.9.xx ► 6.12.xx ► 6.13.xx
v6.4.xx	6.4.xx ► 6.5.xx ► 6.9.xx ► 6.12.xx ► 6.13.xx
v6.3.xx	6.3.xx ► 6.5.xx ► 6.9.xx ► 6.12.xx ► 6.13.xx
v6.2.00.04	6.2.00.04 ► 6.5.xx ► 6.9.xx ► 6.12.xx ► 6.13.xx
v6.1.xx	6.1.xx ► 6.5.xx ► 6.9.xx ► 6.12.xx ► 6.13.xx

GigaVUE-FM Installation

For documentation:

- Refer to the GigaVUE-FM Installation and Upgrade Guide for the procedures or search for “GigaVUE-FM Installation and Upgrade” from the [Gigamon Community](#) or the [Online Documentation Library](#).
- If you are deploying a GigaVUE-FM Hardware Appliance 2.0, for the initial configuration of iDRAC9, refer to [Dell PowerEdge - How to configure the iDRAC9 and the LifeCycle Controller Network IP](#).

Credentials for Admin Account for New Deployments

During new installations of GigaVUE-FM, you will be forced to create a new password that meets the password criteria. The default password, ‘admin123A!!’, can no longer be used after the first login.

GigaVUE-FM Upgrade

To upgrade GigaVUE-FM, the recommended procedure is to back up your current configuration and perform the pre-upgrade checks (memory requirements, the maximum number of images) before installing the image. You can upgrade via the GigaVUE-FM UI or GigaVUE-OS CLI. It is recommended that you plan your upgrade before performing any upgrade steps.

Rules and Notes

- **IMPORTANT:** Intent-Based Orchestration (IBO) Policies are removed when upgrading from any pre-5.11 version of GigaVUE-FM to version 5.11.00 or above. IBO Policies will need to be recreated after upgrading to 5.11.00 or above. (Ref: FM-33169)
- **BEST PRACTICES:**
 - Before performing an upgrade, in addition to taking a backup of GigaVUE-FM, also take a Sysdump, which provides valuable configuration information that is not captured in the backup. You can use the Sysdump after the upgrade to troubleshoot any upgrade-related issues with your configurations.
 - Always upgrade your GigaVUE-FM instance before upgrading the GigaVUE-OS nodes. You can upgrade the attached nodes from the device or from GigaVUE-FM. The latter is recommended. Refer to “Upgrade Software on a GigaVUE Node or a Cluster from GigaVUE-FM” in the GigaVUE-FM User’s Guide.
- **If upgrading from GigaVUE-FM versions lower than 5.8.xx to 5.10.xx :** If you are upgrading from a version lower than 5.8.xx to 5.10.xx refer to the GigaVUE-FM Migration instructions in version 5.10 of the Online Documentation Library for details.
- **If upgrading from GigaVUE-FM versions lower than 5.5.00:** While upgrading from any version lower than 5.5.00, an association of more than one vport to the same GigaSMART group needs to be removed for any existing GTP GigaSMART operation.
- **If upgrading from GigaVUE-FM versions lower than 5.4.00:** Be aware of the minimum memory requirement changes between releases. Earlier releases specified 4GB of memory for the OVA template, whereas versions after 5.4.00 require 8GB and versions after 5.7.00 require 16GB. If the existing virtual or physical hardware running GigaVUE-FM is configured with less memory than required, then increase the amount of memory available to the GigaVUE-FM machine. Refer to GigaVUE-FM Memory and CPU Requirements in this document for details.
- For upgrades to versions 5.11.xx and 5.12.xx, a password change is mandated.
- For all other versions, the password change is mandated only if the current password is a default password.

Supported upgrade paths for GigaVUE-FM 6.1.xx and later:

You can upgrade your GigaVUE-FM instance to any of the subsequent two versions. To upgrade your GigaVUE-FM from 6.1.xx to later versions, the supported upgrade paths are:

**IMPORTANT:**

- When you are upgrading to 6.13, you must upgrade all fabric components within **30** days of upgrading GigaVUE-FM to ensure version compatibility before the next UCT-V certificate renewal. Complete the following upgrades immediately after the GigaVUE-FM upgrade to ensure that UCT-V certificates renew only after all components are running compatible versions, reducing the risk of registration or communication failures:
 - UCT-V Controller
 - UCT-V's
 - GigaVUE V Series Node
 - GigaVUE V Series Proxy
- When GigaVUE-FM manages GigaVUE Cloud Suite components (UCT-V Controller, UCT-V, GigaVUE V Series Node, and GigaVUE V Series Proxy), you must keep these components within two releases (N+2) of the GigaVUE-FM release. Upgrade the components at each GigaVUE-FM hop before starting the next GigaVUE-FM upgrade. For example, when upgrading GigaVUE-FM from 6.1.xx to 6.3.xx, upgrade all Cloud components to 6.3.xx before upgrading GigaVUE-FM to 6.5.xx.

Table 2: GigaVUE-FM Upgrade Summary Table

To upgrade to 6.13.xx from...	Use the recommended upgrade path for GigaVUE-FM
v6.12.xx	6.12.00 or 6.12.01 or 6.12.02 ► 6.13.xx
v6.11.xx	6.11.xx ► 6.12.00 or 6.12.01 or 6.12.02 ► 6.13.xx
v6.10.xx	6.10.00 or 6.10.01 ► 6.10.02* ► 6.12.00 or 6.12.01 or 6.12.02 ► 6.13.xx
v6.9.xx	6.9.xx ► 6.10.02* ► 6.12.00 or 6.12.02 ► 6.13.xx
v6.8.xx	6.8.xx ► 6.10.02* ► 6.12.00 or 6.12.01 or 6.12.02 ► 6.13.xx
v6.7.xx	6.7.xx ► 6.8.xx ► 6.10.02* ► 6.12.00 or 6.12.01 or 6.12.02 ► 6.13.xx
v6.6.xx	6.6.xx ► 6.8.xx ► 6.10.02* ► 6.12.00 or 6.12.01 or 6.12.02 ► 6.13.xx
v6.5.xx	6.5.xx ► 6.7.xx ► 6.8.xx ► 6.10.02* ► 6.12.00 or 6.12.01 or 6.12.02 ► 6.13.xx
v6.4.xx	6.4.xx ► 6.6.xx ► 6.8.xx ► 6.10.02* ► 6.12.00 or 6.12.01 or 6.12.02 ► 6.13.xx
v6.3.xx	6.3.xx ► 6.5.xx ► 6.7.xx ► 6.8.xx ► 6.10.02* ► 6.12.00 or 6.12.01 or 6.12.02 ► 6.13.xx

To upgrade to 6.13.xx from...	Use the recommended upgrade path for GigaVUE-FM
v6.2.xx	6.2.00 ► 6.4.xx ► 6.6.xx ► 6.8.xx ► 6.10.02* ► 6.12.00 or 6.12.01 or 6.12.02 ► 6.13.xx
v6.1.xx	6.1.xx ► 6.3.xx ► 6.5.xx ► 6.7.xx ► 6.8.xx ► 6.10.02* ► 6.12.00 or 6.12.01 or 6.12.02 ► 6.13.xx
	NOTE: *MongoDB changes were introduced in 6.10.02. You must upgrade to 6.10.02 before moving to 6.11.xx or later.

**IMPORTANT:**

- To prevent upgrades outside the supported paths, which may cause GigaVUE-FM to corrupt, a prevention mechanism has been introduced in GigaVUE-FM version 6.12. Starting from GigaVUE-FM version 6.12, any unsupported upgrade attempt is blocked and marked as failed. Review the **FMCTL log** (*/var/log.fm-ctl.log*) for details on the failure.
- For versions prior to 6.12, unsupported upgrade paths are not automatically blocked. You must follow the correct upgrade sequence mentioned above. If you fail to follow, it may cause GigaVUE-FM to corrupt or lockup.

Additional Information

Contacting Gigamon 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. Refer also to the Gigamon Community at <https://gigamoncp.force.com/gigamoncp/>.

Copyright

Copyright © 2026 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 written permission of Gigamon.

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.

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 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.
- 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.