

GigaVUE-OS, GigaVUE-FM, and GigaVUE® Cloud Suite Release Notes 6.14

Document Version: 1.0 ([Change Notes](#))

Table of Contents

GigaVUE-OS, GigaVUE-FM, and GigaVUE® Cloud Suite	
Release Notes 6.14	1
Change Notes	1
Introduction	1
What's New	2
New Features in 6.14.00	2
View Known and Resolved Issues in the Community Portal	9
Announcements and Deprecation Notices	10
Installation and Upgrade	10
GigaVUE-OS Upgrade	11
GigaVUE-FM Installation	14
GigaVUE-FM Upgrade	14
Important Document References	16
Additional Information	18
Contacting Gigamon Support	18
Copyright	18
Trademark Attributions	18
The VUE Community	19

Change Notes

Date	Revision	Change
07/10/2026	1.0	The original release of this document with version 6.14 GA.

Introduction

These Release Notes describe the new features and enhancements, resolved issues, and known issues for GigaVUE® software version 6.14, 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.

What's New

What's New contains a list of features and functionalities introduced in recent releases.

New Features in 6.14.00

GigaVUE 6.14.00 Software offers usability improvements, resolved issues, and the new capabilities described below.

Online Documentation

- For the complete online documentation for this release, visit the [GigaVUE 6.14 Online Documentation](#). No login required.
- View [What's New](#) in the online documentation to access quick links to topics for each of the new features.
- The [API Reference Guide](#) is now available online including APIs and sample output and examples for GigaVUE-FM APIs as well as Ansible examples provided using the same accessible reference style.

Product Area	Feature Summary
Cloud Suite	5G-Ericsson vTAP Packet Processing (5G-EVP) 5G-Ericsson vTAP Packet Processing (5G-EVP) now reorders Ericsson vTAP packets using embedded timestamps before sending them to monitoring probes, preserving original packet sequence and reducing analysis gaps caused by out-of-order delivery. It supports PCC, CCx, and SCP traffic, uses NTP synchronization for accurate timing, and provides configurable ordering parameters. Supported on VMware ESXi, OpenStack, and Third-Party Orchestration. Refer to: 5G-Service Based Interface Application
	Configurable AWS EC2 Instance Type Support for VPC Traffic Mirroring GigaVUE-FM now enables you to control AWS EC2 instance type eligibility for VPC Traffic Mirroring using an GigaVUE-FM owned registry, along with UI and REST API support. This allows you to adopt new AWS instance types more quickly, without waiting for AWS SDK updates while maintaining strong RBAC enforcement and audit visibility within GigaVUE-FM. Refer to: Enable Traffic Mirroring for New AWS EC2 Instance Types
	Enhanced AMX Troubleshooting and Deployment Workflows in GigaVUE-FM GigaVUE-FM improves the AMX experience with faster, UI-driven troubleshooting and simplified deployment workflows. You can download 3PO cloud configuration files, capture AMX ingestor TCP dumps, and retrieve the latest exporter records with clear status indicators—without requiring V-Series console access. It also lets you verify traffic ingestion and confirm that records are sent to the configured tools. GigaVUE-FM also introduces proactive operational events such as resource utilization events, JSON web token expiry warnings, and address resolution failure notifications that help prevent issues. These enhancements reduce deployment errors, streamline exporter options, and improve scalability for high-traffic environments. Refer to: • View Statistics for Application Metadata Exporter • Create Monitoring Domain • Deploy Application Metadata Exporter in VMware ESXi using Third Party Orchestration • Troubleshoot AMX Deployment • View Health Status
	Ericsson 5G DTLS Support Ericsson 5G DTLS Support adds DTLS as an ingress option for 5G-EVP, alongside the existing UDP-GRE tunnel. When enabled, traffic is

Product Area	Feature Summary
	decrypted using the configured certificate and private key before EVP processing. DTLS can be enabled in GigaVUE-FM, and the required SSL key pair can be uploaded under Inventory > Security > SSL Key. Supported on VMware ESXi, OpenStack, and Third-Party Orchestration. Refer to: 5G-Service Based Interface Application
	Fully Qualified Domain Name (FQDN) GigaVUE Cloud Suite supports the use of a fully qualified domain name (FQDN) in addition to an IPv4 or IPv6 address for the remote destination of supported egress tunnels. This support is available for VXLAN and L2GRE egress tunnels. By using an FQDN, you can keep the same tunnel configuration even when the destination IP address changes, because the system resolves the FQDN to the current IP address during operation. Refer to: • Fully Qualified Domain Name (FQDN) • Configure Monitoring Session
	Nokia HEP3 Support for SBI Traffic from Nokia CMM GigaVUE Cloud Suite now supports processing of SBI and non-SBI traffic from Nokia Cloud Mobility Manager (CMM) vTAPs using the HEP3 (Homer Encapsulation Protocol Version 3) format. The 5G Cloud application decodes and synthesizes HEP3-encapsulated traffic and delivers it to connected tools via VXLAN or L2GRE tunnels. mTLS is supported for secure ingress connections. This feature is supported on VMware ESXi, OpenStack, and Third-Party Orchestration platforms. Refer to: 5G Cloud Nokia HEP3 CMM Solution
	Oracle Cloud Infrastructure (OCI) Support GigaVUE Cloud Suite now supports deployment in Oracle Cloud Infrastructure (OCI), enabling organizations to deploy and manage cloud visibility solutions in OCI environments. This enhancement extends platform support and provides consistent traffic visibility across multi-cloud deployments. Refer to: GigaVUE Cloud Suite Deployment Guide - Oracle
	Traffic Acquisition Enhancements for Nutanix pc.7.5 with FNS-NG 7.5.0 Environments Gigamon Cloud Suite now supports Nutanix Prism Central pc.7.5 environments that use Flow Network Security – Next Generation (FNS-NG) 7.5.0 and the newer single-stack architecture. This update restores underlay east-west visibility by letting you steer traffic to Gigamon V Series nodes using Prism Central security policies

Product Area	Feature Summary
	(customer-orchestrated service insertion) or use Generic 3PO with UCT-V mirroring. It also prevents unsupported GigaVUE-FM orchestrated underlay deployments on FNS single-stack clusters and guides you to supported options. Refer to Acquire Traffic using Customer Orchestrated Source.
GigaVUE-FM Core	Customer Telemetry GigaVUE-FM provides a unified Telemetry Insight dashboard and built-in EOS/EOL notifications, which enable you to quickly view health, usage, licensing risk (due to End of Sale, End of Life), and recommended actions across your physical and cloud deployments without switching between multiple pages. It also provides enhanced feature-adoption metrics that help you validate how key capabilities are used in your environment. Refer to Telemetry Insights Dashboard.
	Enhanced Port and Map Alias Search GigaVUE-FM now provides comprehensive search capabilities for port and map aliases. You can search using a port alias (including partial matches) and instantly see the port along with directly related resources such as maps, GigaStreams, inline components, port groups, and interfaces in a single result set. This streamlines troubleshooting and impact analysis by eliminating the need for a separate search using the port ID. Refer to : How to Search in GigaVUE-FM.
	Flexible Element Positioning in the Map's Diagram view GigaVUE-FM now lets you reposition elements such as devices, ports, and maps in the Topology View (Free Layout), so you can organize these elements in a layout that matches how you troubleshoot traffic flows. This reduces clutter from fixed-lane layouts and makes complex topologies easier to read. Refer to Map Views.
	Manage Rulesets across Traffic Policies You can now copy and paste Source rules or Application rules between traffic policies to quickly reuse proven rule sets, reduce manual work, and avoid rebuilding large policies from scratch. This workflow also detects exact duplicate rules, so you can paste only the non-duplicates and keep your policies clean. Refer to Manage Rulesets across Traffic Policies.
Gigamon Insights	Simplified Deployment and AI Experience with a Unified Prompt Library Gigamon Insights 6.14 modernizes deployment and configuration and improves the AI experience. You can now configure your LLM provider, MCP data tool, and outbound proxy in guided Fabric Manager workflows

Product Area	Feature Summary
	with built-in validation and dynamic updates, and you get a unified Prompt Library with search, favorites, and history to make it easy to find and reuse prompts. The release also improves accuracy for AMI/AMX-based questions by automatically injecting Gigamon-curated reference documents into the AI context—without requiring complex retrieval infrastructure. Refer to Gigamon Insights Post Deployment Configurations in GigaVUE-FM.
GigaSMART	Artificial Intelligence (AI) Traffic Insights Artificial Intelligence (AI) Traffic Intelligence Application Intelligence supports monitoring usage of new AI apps (5) including MCP protocol accessed via web browser or desktop/mobile app for Governance, Risk and Compliance (GRC). In addition, it includes expanded coverage for Web API based classification (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. Simplified Deployment and AI Experience with a Unified Prompt Library
	Identity Enrichment using Zscaler Private Access GigaVUE Enriched Metadata (GEM) now provides identity-based enrichment through integration with Zscaler Private Access (ZPA). By correlating Application Metadata Intelligence (AMI) flow records with User Activity Logs from the ZPA Log Streaming Service (LSS), it delivers per-flow visibility into who accessed which application, when, and from where, along with the associated network policy context. This eliminates the need for separate correlation of network telemetry and supports continuous monitoring and faster troubleshooting of Zero Trust policy enforcement. Refer to: • Application Metadata Exporter • Configure Identity Enrichment Metadata using Zscaler Private Access (ZPA) • Zscaler Private Access (ZPA) Attributes

Product Area	Feature Summary
	Reload GigaSMART engine ports in a GigaSMART group Perform a soft reload of one or more GigaSMART engine ports in a specific gsgroup from the GigaVUE-OS CLI or GigaVUE-FM. This provides an alternative to card reload and helps limit the impact on unrelated traffic and groups. When a GigaSMART group associated with inline traffic is reloaded, a warning is displayed to inform the user that traffic on that group will be temporarily affected. Supported on Gen3 GigaSMART cards of GigaVUE HC Series platforms only. Refer to: • Reload GigaSMART engine ports in a group • gsgroup
	Recurring TLS Server Name Export in Application Metadata Intelligence Application Metadata Intelligence (AMI) now supports exporting Server Name for the lifetime of TLS flows. By default, Server Name is exported at the beginning of a TLS flow. You can turn on this feature by enabling Server Name option under Recurring Attributes in AMI Settings. This feature is supported on GigaVUE HC Series Gen3 GigaSMART module through the Traffic Policy workflow and on GigaVUE V Series only Refer to • Application Intelligence Field References • Application Metadata Intelligence
	GigaVUE-FM Ansible Automation 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

Product Area	Feature Summary
	GigaVUE-FM, refer to the GigaVUE-FM Ansible Users Guide .
GigaVUE-OS	Upgrade Prerequisite for Unified GigaVUE-TA Image The software image for GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-TA200, GigaVUE-TA200E, GigaVUE-TA400, and GigaVUE-TA400E will be provided as a single unified GigaVUE-TA image. GigaVUE-TA devices (GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-TA200, GigaVUE-TA200E, GigaVUE-TA400, GigaVUE-TA400E) running software versions earlier than 6.12.01 must first be upgraded to 6.12.01 or 6.13.01 before upgrading to the unified GigaVUE-TA image version 6.14.00. Upgrade attempts from versions lower than 6.12.01 directly to 6.14.00 will fail. Refer to Supported Upgrade Path—Standalone Nodes.
	Configuring TLS and Cryptographic Settings on the Management Interface You can configure the TLS versions, cipher suites, and curves used on the management interface. This feature helps align with internal security policies and reduces audit or scan findings by allowing you to disable unapproved cryptographic options while maintaining secure, approved settings across management protocols such as HTTPS, CURL, ACME, and secure LDAP. It also supports standardizing cryptography across your environment for greater consistency and compliance. Refer to: • Web • system
Hardware	Support for Optics Dual-Rate Active Optical Cables (AOC) CBL-505A and CBL-510A supporting 40Gb/100Gb speeds. • For details about the optics, refer to Transceivers. • For the supported platforms and GigaVUE-OS versions, refer to Compatibility and Interoperability Matrix.
	New DC Power Cable For GigaVUE-TA25E The DC power cable, PCD-00061, complies with the AS/NZS 5000 and AS/NZS 3015 standards applicable in the Australia and New Zealand region. This specification supports the GigaVUE-TA25E DC-powered platform. Refer to Transceivers.

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.

Announcements and Deprecation Notices

- **Support for Entrust/nCipher HSM**-Support for Entrust/nCipher HSM is going under a redesign and, as a result, is being temporarily removed from GigaVUE OS and GigaVUE FM. This change affects Gen2 DSSL HSM ncipher and Gen3 ncipher HSM support. Thales Luna HSM support on Gen3 devices remains unaffected by this change. Updates to version 6.14 are blocked if any nCipher HSM configuration is present. From 6.14 onward, GigaVUE-FM cannot configure or edit nCipher HSM settings on devices running 6.14 or later.

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	GigaVUE-OS Upgrade Guide	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	GigaVUE-FM Installation and Upgrade Guide	Instructions to install GigaVUE-FM on VMware ESXi, MS Hyper-V, AWS, Azure, OpenStack, Kubernetes, Nutanix and KVM.

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:

- Starting from 6.14, the software image for GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-TA200, GigaVUE-TA200E, GigaVUE-TA400, and GigaVUE-TA400E will be provided as a single unified GigaVUE-TA image. GigaVUE-TA devices (GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-TA200, GigaVUE-TA200E, GigaVUE-TA400, GigaVUE-TA400E) running software versions earlier than 6.12.01 must first be upgraded to 6.12.01 or 6.13.01 before upgrading to the unified GigaVUE-TA image version 6.14.00. Upgrade attempts from versions lower than 6.12.01 directly to 6.14.00 will fail.
- 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.
- 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.
- 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-OS 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.

The following table shows the recommended upgrade path for the device:

Table 1: GigaVUE-OS Upgrade Summary table

To upgrade to 6.14.xx from...	Use the recommended upgrade path for the device...
	GigaVUE HC Series, and G-TAP A Series 2
v6.13.xx	6.13.xx ► 6.14.xx
v6.12.xx (LTS)	6.12.xx ► 6.13.xx ► 6.14.xx
v6.11.xx	6.11.xx ► 6.12.xx ► 6.14.xx
v6.10.xx	6.10.xx ► 6.12.xx ► 6.14.xx
v6.9.xx (LTS)	6.9.xx ► 6.12.xx ► 6.14.xx
v6.8.xx	6.8.xx ► 6.9.xx ► 6.12.xx ► 6.14.xx
v6.7.xx	6.7.xx ► 6.9.xx ► 6.12.xx ► 6.14.xx
v6.6.xx	6.6.xx ► 6.9.xx ► 6.12.xx ► 6.14.xx

To upgrade to 6.14.xx from...	Use the recommended upgrade path for the device...
	GigaVUE HC Series, and G-TAP A Series 2
v6.5.xx (LTS)	6.5.xx ► 6.9.xx ► 6.12.xx ► 6.14.xx
v6.4.xx	6.4.xx ► 6.5.xx ► 6.9.xx ► 6.12.xx ► 6.14.xx
v6.3.xx	6.3.xx ► 6.5.xx ► 6.9.xx ► 6.12.xx ► 6.14.xx
v6.2.00.04	6.2.00.04 ► 6.5.xx ► 6.9.xx ► 6.12.xx ► 6.14.xx
v6.1.xx (LTS)	6.1.xx ► 6.5.xx ► 6.9.xx ► 6.12.xx ► 6.14.xx

The following table shows the recommended upgrade path for the GigaVUE TA Series devices:

To upgrade to 6.14.xx from...	GigaVUE TA Series
v6.13.xx	6.13.00 ► 6.13.01 ► 6.14.xx
v6.12.xx	6.12.00 ► 6.12.02 ► or 6.13.01 ► 6.14.xx
v6.11.xx	6.11.xx ► 6.12.02 ► or 6.13.01 ► 6.14.xx
v6.10.xx	6.10.xx ► 6.12.02 ► or 6.13.01 ► 6.14.xx
v6.9.xx	6.9.xx ► 6.12.02 ► or 6.13.01 ► 6.14.xx
v6.8.xx	6.8.xx ► 6.9.xx ► 6.12.02 ► or 6.13.01 ► 6.14.xx
v6.7.xx	6.7.xx ► 6.9.xx ► 6.12.02 ► or 6.13.01 ► 6.14.xx
v6.6.xx	6.6.xx ► 6.9.xx ► 6.12.02 ► or 6.13.01 ► 6.14.xx
v6.5.xx	6.5.xx ► 6.9.xx ► 6.12.02 ► or 6.13.01 ► 6.14.xx
v6.4.xx	6.4.xx ► 6.5.xx ► 6.9.xx ► 6.12.02 ► or 6.13.01 ► 6.14.xx
v6.3.xx	6.3.xx ► 6.5.xx ► 6.9.xx ► 6.12.02 ► or 6.13.01 ► 6.14.xx
v6.2.00.04	6.2.00.04 ► 6.5.xx ► 6.9.xx ► 6.12.02 ► or 6.13.01 ► 6.14.xx
v6.1.xx	6.1.xx ► 6.5.xx ► 6.9.xx ► 6.12.02 ► or 6.13.01 ► 6.14.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 6.14.xx from...	Use the recommended upgrade path for GigaVUE-FM
v6.13.xx	6.13.00 ► 6.14.xx
v6.12.xx (LTS)	6.12.xx ► 6.14.xx
v6.11.xx	6.11.xx ► 6.12.xx ► 6.14.xx

To upgrade to 6.14.xx from...	Use the recommended upgrade path for GigaVUE-FM
v6.10.xx	*6.10.02 ► 6.12.xx ► 6.14.xx
v6.9.xx	6.9.xx ► *6.10.02 ► 6.12.xx ► 6.14.xx
v6.8.xx	6.8.xx ► *6.10.02 ► 6.12.xx ► 6.14.xx
v6.7.xx	6.7.xx ► 6.8.xx ► *6.10.02 ► 6.12.xx ► 6.14.xx
v6.6.xx	6.6.xx ► 6.8.xx ► *6.10.02 ► 6.12.xx ► 6.14.xx
v6.5.xx	6.5.xx ► 6.7.xx ► 6.8.xx ► *6.10.02 ► 6.12.xx ► 6.14.xx
v6.4.xx	6.4.xx ► 6.6.xx ► 6.8.xx ► *6.10.02 ► 6.12.xx ► 6.14.xx
v6.3.xx	6.3.xx ► 6.5.xx ► 6.7.xx ► 6.8.xx ► *6.10.02 ► 6.12.xx ► 6.14.xx
v6.2.xx	6.2.00 ► 6.4.xx ► 6.6.xx ► 6.8.xx ► *6.10.02 ► 6.12.xx ► 6.14.xx
v6.1.xx	6.1.xx ► 6.3.xx ► 6.5.xx ► 6.7.xx ► 6.8.xx ► *6.10.02 ► 6.12.xx ► 6.14.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.

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	Prerequisites for GigaVUE-FM
Minimum Virtual Computing Requirements for GigaVUE-FM Installation	Computing Requirements for GigaVUE-FM
GigaVUE Cloud Suite System Requirements	
Nutanix Requirements	Minimum Requirements -Nutanix
OpenStack Requirements	Minimum Compute Requirements-OpenStack
Oracle Cloud Infrastructure Requirements	Minimum Compute Requirements-OCI
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 Tap - Container
Supported Platforms for UCT-C	Supported Platforms for UCT-C
Support and Compatibility	
GigaVUE-FM and GigaVUE-OS Compatibility	Manage Devices and Configurations
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)

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.