Universal Container Tap Guide

GigaVUE Cloud Suite

Product Version: 6.2

Document Version: 1.0

Last Updated: Wednesday, May 24, 2023

(See Change Notes for document updates.)

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
6.2.00	1.0	02/15/2023	Original release of this document with 6.2.00 GA.

Contents

Universal Container Tap

Universal Container Tap (UCT) is a containerized component that provides the network broker features in a containerized form. UCT can perform traffic acquisition, basic filtering, and tunneling support. UCT is deployed as a Pod in the given worker node where the workloads are running.

The UCT is deployed by Kubernetes orchestrator and not by GigaVUE-FM. UCT initiates the traffic acquisition process with UCT Taps.

Following are the modules implemented in UCT:

- **Traffic Acquisition**: UCT supports traffic acquisition by replicating the traffic from the worker pods..
- **Filtering Module** - UCTprovides basic filtering based on 5-Tuple. The filtering configuration is pushed by the GigaVUE-FM.
- **Tunneling Modules** - UCT supports L2GRE and VXLAN tunneling to sent the tapped traffic to the GigaVUE V Series or tools.

This guide provides an overview of Universal Container Tap and describes how to install and deploy UCT components in your Pods.

Topics:

- Architecture of Universal Container Tap
- UCT and GigaVUE-FM Interaction
- Get Started with Universal Container Tap
- Configure Universal Container Tap
- Configure UCT Settings

Components of Universal Container Tap

The Universal Container Tap works with the following components:

- **GigaVUE® Fabric Manager (GigaVUE-FM)** is a web-based fabric management and orchestration interface that provides a single pane of glass visibility, management, and orchestration of both the physical and virtual traffic that form the UCT.

- **UCT Tap** is the primary UCT module that collects the workload traffic, filters the traffic and tunnels the filtered traffic directly to the tools or through the GigaVUE V Series 2 nodes. UCT Tap also sends the statistics and heartbeats to UCT Controller. For tapping, don't select the taps which have **true** for the option **HostName**. UCT Tap should run as a **privileged pod**.
- **UCT Controller** is the management component of UCT to control and communicate with UCT Tap. UCT Controller collects the data from UCT Taps and sends the collected statistics and heartbeats to GigaVUE-FM.

Architecture of Universal Container Tap

The following diagram illustrates the architecture of Universal Container Tap environment.
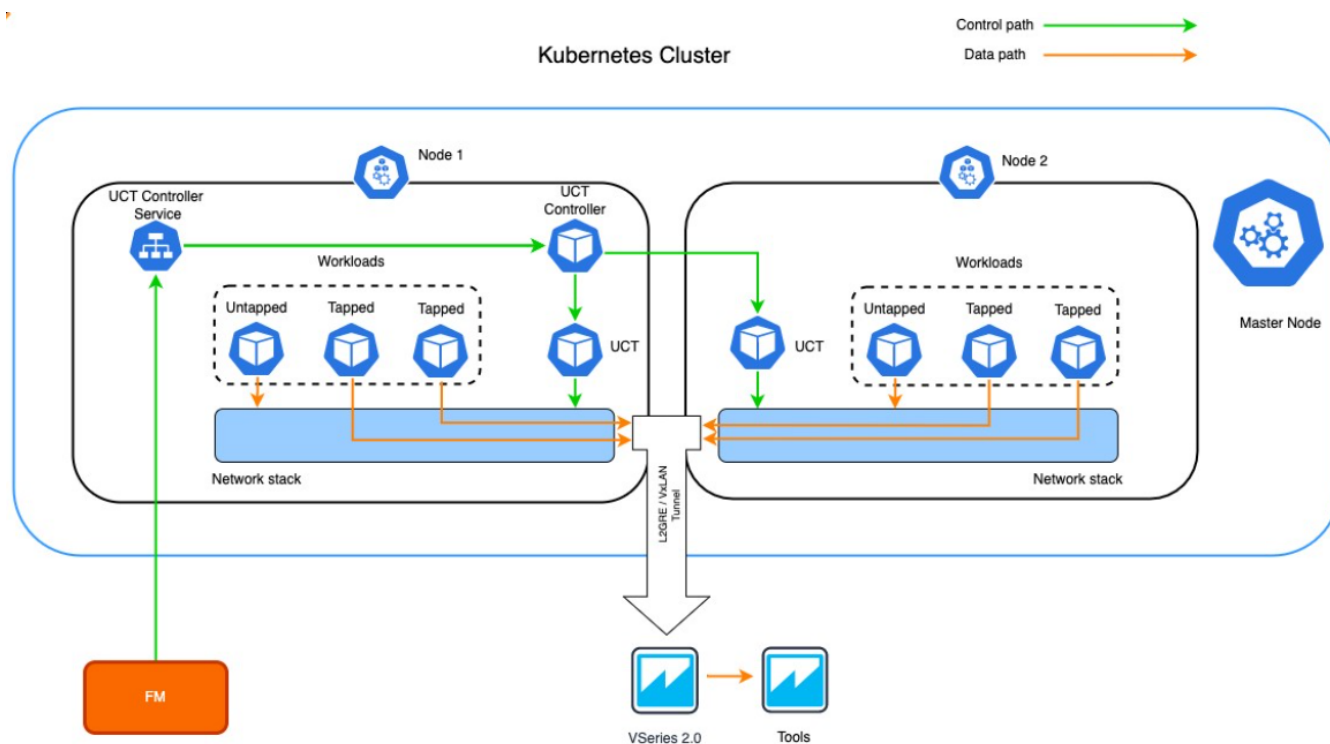
1. The UCT Tap is registered with GigaVUE-FM through the UCT Controller
2. GigaVUE-FM deploys the traffic policy on the UCTs.
   Communication of configuration, data, and statistics to and from UCT is performed through the UCT Controller Service. GigaVUE-FM communicates with the UCT Taps through the UCT Controller. GigaVUE-FM deploys the traffic policy on UCT and receives the statistics from UCT tap through UCT controller.

3. The customer workload collects the network traffic and sends the network packets to the Kernel space.
4. The Kernel space filters the packets based on the rules and filters.
5. The filtered network packets are tunneled directly to the Tools or through the GigaVUE V Series nodes running on any supported GigaVUE Cloud Suite on cloud environment.
6. The UCT Controller collects the data from UCT Taps and sends the collected statistics and heartbeats to GigaVUE-FM.

UCT and GigaVUE-FM Interaction

Following are the interactions between UCT and GigaVUE-FM:

- UCT Registration
- UCT Deregistration
- UCT Heartbeats
- Monitoring Domain and Traffic Policy

UCT Registration

When UCT comes up in the Kubernetes environment, UCT registers itself with GigaVUE-FM. When GigaVUE-FM is unreachable, UCT tries to connect with five retries of increasing time periods. If the GigaVUE-FM is unreachable even after the retries, Kubernetes deployment of UCT fails. UCT only supports IPv4 protocol. For more information, refer to Deploy GCB in Kubernetes.

UCT Deregistration

When UCT is terminated normally, UCT sends the deregistration message to GigaVUE-FM. If UCT goes down abnormally, it will get deregistered when the GigaVUE-FM misses to receive couple of heartbeats.

UCT Heartbeats

Periodically, UCT sends heartbeats to GigaVUE-FM. By default, the status of UCT is marked as **Connected**. The following are the various scenarios where the UCT status changes:

- If 3 consecutive heartbeats are missed, GigaVUE-FM marks the status as **Disconnected**.
- If 2 consecutive heartbeats are missed, GigaVUE-FM marks the status as **Pending**.
- GigaVUE-FM purges disconnected or terminated UCT taps after 30 days.

Monitoring Domain and Traffic Policy

You can configure and manage the Monitoring Domains, Connections, Source Inventories, and Traffic Policies of UCT in GigaVUE-FM. For more information, refer to Configure UCT through GigaVUE-FM

Refer to the GigaVUE API Reference for detailed information on the REST APIs of UCT.

> - A Traffic Policy is a combination of Rules and Tunnels.
> - A rule contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the target instances and the (egress or ingress) direction of tapping the network traffic.
> - A tunnel is a communication path in which the traffic matching the filtered criteria is routed to the destination.

Get Started with Universal Container Tap

This section describes how to initiate UCT and GigaVUE-FM deployment with the required licenses and network requisites.

Refer to the following sections for details:

- Components of Universal Container Tap
- License Information
- Network Requirements
- Compute Requirements

License Information

All the UCT Taps deployed in your environment periodically report the statistics to UCT Controller. Then the UCT Controller periodically reports the collective statistics of UCT Taps to GigaVUE-FM for Volume-Based Licensing.

In the Volume-Based Licensing scheme, a license entitles specific applications on your devices to use a specified amount of total data volume over the term of the license. The distribution of the license to individual nodes or devices becomes irrelevant for Gigamon's accounting purpose. GigaVUE-FM tracks the total amount of data processed by the UCT, and tracks the overuse if any.

Volume-based licensing has a service period of 1 month. Service period is the period of time for which the total usage or overage is tracked. There is a grace period for each license that is encoded in the license file. The license effectively provides data allowance for this additional time after the official end time of the license.

For purchasing licenses with the Volume-Based License (VBL) option, contact our Sales. Refer to Contact Sales.

Network Requirements

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

Direction	Type	Protocol	Port	CIDR	Purpose
Universal Container Tap deployed inside Kubernetes worker node					
Outbound	HTTPS	TCP	443	Any IP address	Allows UCT Controller to communicate with GigaVUE-FM
Inbound	HTTPS	TCP	8443 (configurable)	Any IP address	Allows GigaVUE-FM to communicate with UCT Controller.
Outbound	HTTPS	TCP	42042	Any IP address	Allows GigaVUE-FM to communicate with UCT to send statistical data.

Compute Requirements

The following table describes the minimum compute network requirements for UCT.

Compute Instances	vCPU	Memory	Disk Space
Universal Container Tap (UCT)	1 vCPU	64MB	——
UCT Controller	1 vCPU	64MB	——
GigaVUE V Series Node	4 vCPUs	8GB	20GB
GigaVUE V Series Proxy	1 vCPU	1GB	2GB
GigaVUE-FM	4 vCPUs	16GB	41GB

Supported Platforms for UCT

The following tables list the different platforms and their Kubernetes version, Container Run-time Interface (CRI), and Container Network Interface (CNI) that are qualified and supported for UCT.

> **NOTE:** As the end user, you must have an understanding and knowledge of your container services.

Platform	Kubernetes Version	CRI	CNI
Amazon Elastic Kubernetes Service (EKS)	1.22, 1.23	Containerd	VPC
Azure Kubernetes Service (AKS)	1.22, 1.23	Containerd	Azure CNI
VMware Tanzu	1.20	Containerd	Antrea and Calico
Red Hat OpenShift	1.22	CRI-O	OVN
Native Kubernetes	1.22	Docker	Flannel and Calico

Configure Universal Container Tap

Setting up UCT involves the following two steps:

- Deploy UCT in Kubernetes
- Configure UCT through GigaVUE-FM

> The Red Hat supported base images of the UCT applications are built on the top of Red Hat Universal Base Image or Red Hat Enterprise Linux Image. The UCT images are **Red Hat Certified** for Red Hat OpenShift platform.

Kernel and CPU Requirements:

The kernel requirements for different platforms are as follows:.

- EKS – 5.4
- Native Kubernetes– 5.4, 4.19 (Photon+ OS)

The minimum CPU and RAM requirements for TAP and Controller are as follows:

- UCT-TAP — 1vcpu and 64Mi
- UCT-Controller— 1vcpu and 64Mi

Deploy UCT in Kubernetes

To fully deploy UCT, the following steps are required to be completed:

1. Implement external access to the Kubernetes environment (e.g., ingress, external public IPs, load balancers) to allow communication between UCT and GigaVUE-FM.

2. Ensure that the firewall rules on Kubernetes nodes are met according to the Network Requirements.

3. Add the UCT images to a private Docker registry or ensure that the files can be pulled from the Docker Hub registry. You can spin up or spin down the UCT instances based on your traffic load.

4. Deploy UCT Controller Service and Taps using YAML files or Helm Charts.

5. Deploy UCT Taps using YAML files or Helm Chart.

Refer to the following topics for UCT Controller and Taps:

- Deploy UCT Controller Service and Taps
- Deploy UCT Taps

Deploy UCT Controller Service and Taps

You can deploy the UCT Controller Service and Taps using the YAML files or the Helm Charts. Refer to the following sections for detailed information.

- Deploy UCT Controller Service and Taps using YAML files
- Deploy UCT Controller Service and Taps using Helm Chart

Deploy UCT Controller Service and Taps using YAML files

Deploy UCT Controller Service

Follow the instructions below to deploy UCT Controller Service in your Kubernetes environment using YAML file:

> **NOTE:** Contact Technical Support or Contact Sales for the UCT images and YAML files.

1. In your Kubernetes orchestrator, edit the UCT Controller image name, commands, and other required information into your YAML file. The following is sample data from the YAML file. Edit your YAML file based on the sample given below. <u>Do not</u> copy and paste this content into your YAML file:

```
apiVersion: v1
kind: Service
metadata:
  labels:
    app: gigamon-uct
    pod: uct-cntlr
    service: uct-cntlr-service
    # change the namespace to match your namespace
  name: uct-cntlr-service
spec:
  ports:
  - name: uct-rest
    port: 8443
    protocol: TCP
    targetPort: 8443
  - name: uct-stats
    port: 42042
    protocol: TCP
    targetPort: 42042
  selector:
    app: uct-cntlr
  type: ClusterIP
```

The following table gives a description of all the field values in the YAML file that are updated:

Field Values	Description
Port: 443	The UCT Controller REST service port number.
Port: 42042	This port must be port 42042. This allows GigaVUE-FM to communicate with UCT to send statistical data.

2. Using the YAML file, Kubernetes creates the UCT Controller Service.

Deploy UCT Controller Taps

Follow the instructions below to deploy UCT Controller Service in your Kubernetes environment using YAML file:

> **NOTE:** Contact Technical Support or Contact Sales for the UCT images and YAML files.

1. In your Kubernetes orchestrator, edit the UCT Controller image name, commands, and other required information into your YAML file. The following is sample data from the YAML file. Edit your YAML file based on the sample given below. <u>Do not</u> copy and paste this content into your YAML file:

```
name: uct-cntlr
image: gigamon/uct-cntlr:cntlr-<version>
command:
- # /uct-controller
- # <GigaVUE-FM IP>
- # <GigaVUE-FM REST Svc Port>
- # <UCT-Cntlr REST SVC Port>
env:
# Service name.Should match name specified in metadata section.
- name: UCT_CNTLR_SERVICE_NAME
 value: "GIGAMON_UCT_CNTLR_SERVICE"
# External LB balancer IP, for controller (FM) to connect to UCT-cntlr
- name: UCT_CNTLR_EXT_IP_DNS
 value: "<external IP for GigaVUE-FM to reach UCT CNTLR>"
# K8S cluster end-point (typically, master nodes with default port of 6443)
- name: K8S_CLUSTER_ENDPOINT
 value: <K8s Cluster API URL>
# Namespace of Pod
- name: UCT_CNTLR_Tap_NAMESPACE
 valueFrom:
      fieldRef:
          fieldPath: metadata.namespace
ports:
- containerPort: 8443
  protocol: TCP
- containerPort: 42042
  protocol: TCP
imagePullPolicy: Always
```

The following table gives a description of all the field values in the YAML file that are changed or updated:

Field Values	Description
/uct-cntlr (image name)	UCT Controller image name and version. Make sure to use the latest image version.
GigaVUE-FM IP	The IP address of the GigaVUE-FM with which your UCT is connected.
FM REST Svc Port	The FM REST service port number. This must be opened on your Kubernetes to allow outbound traffic. This allows UCT Controller to communicate with GigaVUE-FM. Example: 443
UCT-Cntlr REST SVC Port	The UCT Controller REST service port number. This must be opened on your GigaVUE-FM to allow inbound traffic to Kubernetes. This allows GigaVUE-FM to communicate with UCT Controller. Example: 8443 (configurable)
Ports:	Two ports must be opened. The first container port must

Field Values	Description
o containerPort: 443 o containerPort: 42042	be the same as UCT-Cntlr REST SVC Port. The second container port must be port 42042. This allows GigaVUE-FM to communicate with UCT to send statistical data.
External LB balancer IP	The external load balancer IP/DNS value to allow GigaVUE-FM to communication with UCT Controller within Kubernetes. The GigaVUE-FM IP entry may change when you upgrade or redeploy.
K8S cluster end-point	Kubernetes cluster end point for GigaVUE-FM to access the control plane.. Example: https://<kubernetesapiserverurl>:6443

2. Using the YAML file, Kubernetes automatically downloads the defined UCT Controller Taps and deploys it to the Kubernetes worker node.

Deploy UCT Controller Service and Taps using Helm Chart

Follow the instructions below to deploy UCT Controller Service and Taps in your Kubernetes environment using Helm Chart:

> **NOTE:**   Contact Technical Support or Contact Sales for the UCT images and Helm Charts (**uct-cntlr-<version>.tgz** and **uct-tap-<version>.tgz**).

1. On your Kubernetes orchestrator, extract the received UCT Controller (service and Tap) **.tgz** package.
   ```
   $ tar -xvf uct-cntlr-<version>.tgz
   ```
2. After extraction, navigate to the uct-cntlr folder and edit the **values.yaml** file as per your environment. Refer to Deploy UCT Controller Service and Deploy UCT Controller Taps for detailed information.
3. From the extracted uct-cntlr folder, install the UCT Controller Helm using the following command:
   ```
   $ helm install <Name for the UCT Controller> uct-cntlr <Extracted folder path> uct-cntlr/
   ```
4. Using the Helm file, Kubernetes creates the UCT Controller Service, automatically downloads the defined UCT Controller Taps and deploys it to the your worker node.

Deploy UCT Taps

You can deploy the UCT Taps using the YAML files or the Helm Charts. Refer to the following sections for detailed information.

- Deploy UCT Taps using YAML files
- Deploy UCT Taps using Helm Chart

Deploy UCT Taps using YAML files

Follow the instructions below to deploy UCT Taps in your Kubernetes environment using YAML file:

> **NOTE:** Contact Technical Support or Contact Sales for the UCT images and YAML files.

1. In your Kubernetes orchestrator, edit the UCT Tap image name, commands, and other required information in a YAML file. The following is sample data from the YAML file. Edit your YAML file based on the sample given below. <u>Do not</u> copy and paste this content into your YAML file:

```yaml
name: gigamon-uct
command:
- # /uctapp/uct
- # (1=> default, 0=> rule)
- # (1=> L2GRE, 3=> VXLAN)
env:
- name: LD_LIBRARY_PATH
 value: /usr/lib64
- name: UCT_DEBUG_MODE
 value: "0x0A000004"
- name: UCT_SERVICE_NAME
 value: "UCT_SERVICE"
- name: UCT_CNTLR_SVC_DNS
   #value: "<UCT-CNTLR-SVC-NAME.UCT-CNTLR-NAMESPACE>.svc.cluster.local"
   value: "uct-cntlr-service.default.svc.cluster.local"
- name: UCT_CNTLR_REST_SVC_PORT
# port used to receive configuration from FM
   value: '8443'
- name: UCT_WORKERNODE_NAME
valueFrom:
fieldRef:
fieldPath: metadata.namespace
image: gigamon/uct:<version>
```

The following table gives a description of all the field values in the YAML file that are changed or updated:

Field Value	Description
(1=> default, 0=> rule)	(0/1) Enter 1 to use the default destination IP, or enter 0 to use the rules configured by GigaVUE-FM
(1=> L2GRE, 3=> VXLAN)	(1/3) Enter 1 to use the L2GRE tunnel type or enter 3 to use the VXLAN tunnel type.
gigamon/uct-tap:<version>	UCT Controller image name and version. Make sure to use the latest image version.
UCT_DEBUG_MODE	The hex value for UCT debugging. This value must be in the **0xdd[aaaa][b][c]** format, where: • aaaa is a hex value for the number of pcap messages to maintain before rollover • b is 0 = do not create pcap or 1 = create pcap • c is level. Level with 1 =fatal, 2 =error, 3 =info, 4 =debug

Field Value	Description

	• dd is the log file size multiplier
	
	    • dd = 0|1 - means default log file size (default 100,000 lines)
	
	    • dd = 08 - means 8 * default log file size (default 8*100,0000 lines)
	
	    • dd = FF = 255 - means (255*100,000 lines)

UCT_CNTLR_SVC_DNS	UCT Controller Service Number. This value must match the metadata used for UCT Controller. Example: gigamon-uct-cntlr-service.default.svc.cluster.local
UCT_CNTLR_REST_SVC_PORT	The UCT Controller REST service port number. This must be opened on your GigaVUE-FM to allow inbound traffic to Kubernetes.

2. Using the YAML file, Kubernetes automatically downloads and deploys the defined UCT Taps.

Deploy UCT Taps using Helm Chart

Follow the instructions below to deploy UCT Taps in your Kubernetes environment using Helm Chart:

> **NOTE:** Contact Technical Support or Contact Sales for the UCT images and Helm Charts (**uct-cntlr-<version>.tgz** and **uct-tap-<version>.tgz**).

1. On your Kubernetes orchestrator, extract the received UCT Tap**.tgz** package.
   ```
   $ tar -xvf uct-tap-<version>.tgz
   ```
   After extraction, navigate to the uct-tap folder and edit the **values.yaml** file as per your environment. Refer to Deploy UCT Taps using YAML files for detailed information.

2. From the extracted uct-tapfolder, install the UCT Helm using the following command:
   ```
   $ helm install <Name for the UCT Tap> uct-tap<Extracted folder path> uct-tap/
   ```

3. Using the Helm file, Kubernetes creates the UCT Tap, automatically downloads the defined UCT Taps and deploys it to the Kubernetes worker node.

Configure UCT through GigaVUE-FM

This section describes how to configure UCT through GigaVUE-FM GUI. Refer to the following section for details.

- Launch GigaVUE-FM
- Create Monitoring Domain
- Create Source Selectors

- Create Tunnel Specifications
- Configure Traffic Policy
- Traffic Policy Statistics

Launch GigaVUE-FM

The recent GigaVUE-FM image files can be downloaded from Gigamon Customer Portal. After fetching the image, upload and launch GigaVUE-FM on your GigaVUE V Series 2 supported cloud environment. For assistance, Contact Technical Support of Gigamon or refer to GigaVUE Cloud Suites for more information on GigaVUE V Series 2 configuration on the supported cloud environments.

Create Monitoring Domain

To create a monitoring domain in GigaVUE-FM:

1. In GigaVUE-FM, on the left navigation pane, select **Inventory > CONTAINER > Universal Container Tap > Monitoring Domains**. The **Monitoring Domain** page appears.
2. In the **Monitoring Domain** page, click **New**. The **New Monitoring Domain** wizard appears.

New Monitoring Domain   Save   Cancel

Monitoring Domain Name

[Name]

Connections

Connection Name   Cluster Name

[Alias]   [Cluster Name]

URL   Authentication Type

[Enter URL   ⌄]   [Token]

Token   Inventory Discovery

[Enter Token]   ○ FM ● Upload ○ UCT Controller   ⊕

3. Enter or select the required information as described in the following table,

Fields	Description
Monitoring Domain Name	Enter a name for the monitoring domain
Connections	
Connection Name	Enter a name for the UCT connection
Cluster Name	Enter a name for the cluster
URL	Enter the URL of the API server
Authentication Type	Select token as the authentication type. By default, the authentication type is token.
Token	Enter the authentication token.

Inventory Discovery	Select any one of the following options:
	● FM - When you select FM, you need to enter the authentication token.
	
	NOTE: If you don't have an authentication token, the GigaVUE-FM can't pull the inventory. You can the other options mentioned below to include the inventory.
	
	References for POST and DELETE APIs:
	   o **POST**/cloud/kubernetes/inventory/pods/{connectionId} Add/Create UCT Kubernetes pods inventory.
	   o **DELETE**/cloud/kubernetes/inventory/pods/{connectionId} Delete UCT Kubernetes pods inventory.
	   o **POST**/cloud/kubernetes/inventory/services/{connectionId} Add/Create UCT Kubernetes services inventory in FM.
	   o **DELETE**/cloud/kubernetes/inventory/services/{connectionId} Delete UCT Kubernetes services inventory.
	   o **POST**/cloud/kubernetes/inventory/nodes/{connectionId} Add/Create UCT Kubernetes nodes inventory in FM.
	   o **DELETE**/cloud/kubernetes/inventory/nodes/{connectionId} Delete UCT Kubernetes nodes inventory.
	● Upload - You need to upload the inventory information into GigaVUE-FM. You must feed the inventory details through the REST APIs. Refer to the GigaVUE API Reference for detailed information.
	● UCT controller-UCT controller running as a POD in each Kubernetes cluster collects the inventory information and sends it to GigaVUE-FM.

Click ⊕ to add another connection and click ⊖ to remove an existing connection.

4. Click **Save** to create a monitoring domain.

> **NOTE:** When the cluster worker node restarts, the connecting UCT Tap is marked as disconnected and it is shown on the monitoring domain page for 30 days before the GigaVUE-FM cleans them up.

You can view the monitoring domain created in the list view. The list view shows the following information for UCT and controllers:

- Monitoring Domain
- URL
- Connection
- Cluster Name
- UCT UCCID
- Management IP
- Version
- Node Name
- Status
- Discovered Sources

> **NOTE:** Click the ⚙ to select the columns that should appear in the list view.

Create Source Selectors

When setting up a traffic flow, it is important to define the selection criteria for the sources of traffic. Use the Source Selectors page for configuring the sources of the traffic to be monitored.

To configure the Source Selectors:

1. Select **Inventory** > **Resources> Source Selectors**.
2. On the **Source Selectors** page, navigate to the **Container** tab and click **Create**. The **New Source Selector** wizard appears.

3. Enter or select the required information:

Field	Action
Name	Enter a name for the source
Include Filters (Criteria 1) On the Criteria, click ⊕ to add another Object and click ⊖ to remove an existing Object.	
Object Property	Select an object property to filter the traffic source.
Operator	Select the operator.
Values	Enter the values for the filter.
Exclude Filters (Criteria 1) On the Criteria, click ⊕ to add another Object and click ⊖ to remove an existing Object.	
Object Property	Select an object property to filter the traffic source.
Operator	Select any one of the operators: ● equals ● contains ● startswith ● endwith
Values	Enter the values for the filter.

On the Include or Exclude filters, click ⊕ to add another Criteria and click ⊖ to remove an existing Criteria.

4. Click **Save** to save the filter.

> **Note:** You can create multiple filter criteria. Within each criterion, you can configure multiple filters.
>
> - If you have configured multiple filters in a criterion, then the traffic will be filtered only if all the filter rules are true.
> - If you have configured multiple criteria, then the traffic will be filtered even if one of the criteria is true.

Create Tunnel Specifications

A tunnel of type L2GRE or VXLAN can be created. The tunnel is an egress tunnel.

To configure the tunnels:

1. Select **Inventory** > **Resources > Tunnel Specifications**.
2. On the **Tunnel Specifications** page, navigate to **Container** tab and click **Create**. The **Create Tunnel Specification** wizard appears.

Create Tunnel Specifications   Save   Cancel

Name

Description

Tunnel Type

Select   ⌄

Destination IP Address

Key

3. Enter or select the following information:

Field	Description
Name	The name of the tunnel endpoint.
Tunnel Type	Select L2GRE, or VXLAN tunnel type to create a tunnel.
Destination IP Address	Enter the IP address of the destination endpoint
Key	Enter a value for the tunnel key

4. Click **Save** to save the configuration.

Configure Traffic Policy

To create a UCT Traffic Policy in GigaVUE-FM:

1. From the GigaVUE-FM left navigation pane, select **Traffic > CONTAINER > Universal Container Tap**. The **Policies** page appears.

2. In the **Policies** page, click **Create**. The Create Policy wizard appears.

3. In the **General** tab, enter or select the required information as described in the following table:

Fields	Description
Policy Name	Enter a name for the Traffic Policy.
Monitoring Domain	Select an existing monitoring domain. To create a new monitoring domain, refer to Create Monitoring Domain section.
Connections	Select one or more connections for the policy.

4. Switch to the **Source Selectors** tab, select an existing source selector or select **Create New** to create a new source selector, refer to Create Source Selectors section for detailed information.

5. Switch to the **Rules** tab, enter or select the required information for the **Ingress Rules** and the **Egress Rules** as described in the following table:

Fields	Description
Rules On the Ingress or Egress rules, click ⊕ to add another rule and click ⊖ to remove an existing rule.	
Rule Name	Enter a name for the rule. **NOTE:** Rule names ending with __I, __E, __RI, __RE are not recommended as the names are invalid in policy rules.
Enable	Select **On** to enable the filter or select **Off** to disable the filter
Action	Select Pass to allow the packets or select Drop to block the packets based on the filters.
Direction	Select any one of the following directions: • Bi-directional - Taps the traffic in both directions. The maximum number of rules supported per direction is 8. Also, each directional rule will add 2 ingress rules and 2 egress rules. • Ingress- Taps the ingress traffic. • Egress - Taps the egress traffic.
Direction	Select any one of the following directions: • Bi-directional - Taps the traffic in both directions. The maximum number of rules supported per direction is 32. Also, each directional rule will add 2 ingress rules and 2 egress rules. • Ingress- Taps the ingress traffic. • Egress - Taps the egress traffic.
Priority	Enter a priority value to specify the precedence.
Tunnel Specifications	Select an existing tunnel or select **Create New** to create a new tunnel, refer to Create Tunnel Specifications section for detailed information.
Filters On the rule section, click ⊕ to add another filter and click ⊖ to remove an existing filter.	
Filter Type	Select a filter type
Filter Name	Enter a name for the filter
Value	Enter a value for the filter

6. Switch to the **Deploy** tab, click **Deploy** and the selected traffic policy rules get deployed to the required UCT taps present on the nodes corresponding to the source pods selected for monitoring.

The Traffic Policy processes the customer workload traffic and UCT forwards the traffic to the tunnel destination IP address.

Traffic Policy Statistics

Traffic Policy Statistics in the GigaVUE-FM provides the visibility of the policies within a Monitoring Domain and displays the trending information of the policies and its rules statistics in the dash-board. It also allows visualization and performance at every container level of the Policy Deployment.

Rules are configured in the UCT to either forward the traffic to a Tunnel or drop the flow of the traffic. In the Policies page, along with the UCT policy and its rules, you can also view the aggregated statistics of all the source selectors which are part of the policy.

The activities of the rules are reflected by the statistics counters. The statistics counters show how the policy statistics is directly co-related to the policy and its rules being configured through the GigaVUE-FM.

Viewing Policy Statistics

To view the statistics of the traffic policy configured in the GigaVUE-FM, do the following steps:

1. Go to **Traffic**> **Container** > **Universal Container Tap**. The **Policies** page appears. In the policy page, you can view various details related to a policy such as **Name**, **Monitoring Domain**, **Connection**, **Status**, etc., For each policy, the value correspond to the aggregate value of UCT taps associated with that policy. The fields and the description of the field names are given in the following table:

Table 1:

Field	Description
Name	Name of the Policy
Monitoring Domain	Monitoring Domain associated with the Policy.
Connection	The connection associated with the policy.
Status	Specifies whether the policy deployment is : healthy unhealthy
UCT Deployment	Specifies the count of successful deployment along with the total number of deployment for a policy.
Rx packets	Total aggregate value of the ingress packets associated with the policy.
Tx packets	Total aggregate value of the egress packets associated with the policy.
Egress packets	Total aggregate value of the egress packets associated with the policy.
Rx Dropped	Total aggregate value of the ingress packets dropped associated with the policy

Field	Description
Tx Dropped	Total aggregate value of the egress packets dropped associated with the policy.
Ingress Bytes	Total aggregate value of the ingress bytes associated with the policy.
Egress Bytes	Total aggregate value of the egress bytes associated with the policy.
Ingress Errors	Total aggregate value of the ingress errors associated with the policy.

> **NOTE:** Click the Gear icon ⚙ to add or remove column or columns as per your requirement.

2. Click the **name** of a policy to view the statistics of the policy. The statistics appears on the bottom of the **Policies** page as shown in the figure.
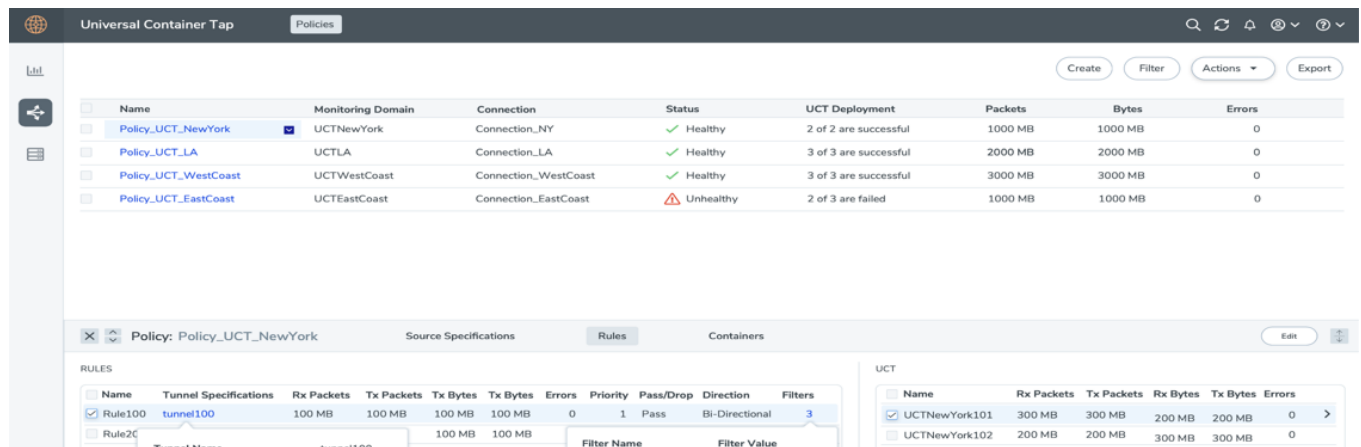
You can view the following three tabs along with the policy name:

- Source Specifications
- Rules
- Container

You can scroll each of the tables to view more columns. The fields and description for the tab that appears when you click the tabs are described in the topics respectively.

Source Specifications

You can view the criteria based on which a pod is selected for tapping.

The fields and descriptions of the source specifications tab are described in the following table:

Table 2:

Tab- Source Specifications	Field	Description
Source Selector		
	Name	Specifies the name of the Source selector.
Include Criteria		
	Criteria Name	Specifies the include criteria for the source selector. Pod that matches the include criteria is part of the source for the given traffic policy.
	Property	Specifies the attributes of the pod. The available attributes are: service
	Operator	Specifies the operator used in the criteria.
	Value	Specifies the value for the attributes in the criteria.
Exclude Criteria		
	Criteria Name	Specifies the exclude criteria for the source selector. Pod that matches the exclude criteria will be part of the source for the given traffic policy.
	Property	Specifies the property in the exclude criteria based on which the pod associated with the source is tapped.
	Operator	Specifies the operator involved in the exclude criteria in tapping the traffic in the pod.
	Value	Specifies the value in the criteria based on which traffic in the pod is tapped.

Rules

You can view the aggregate value of all the rules the policy has been configured for the node in the UCT tap present in a cluster. The fields and descriptions of the source specifications tab are described in the following table:

Table 3:

Tab-Rules	Field	Description
Rules		
	Name	Specifies the name of the rules in which the traffic is filtered in the pod
	Tunnel Specifications	Specifies the tunnel details which is associated with the rules to send the traffic out. When you hover over the tunnel specification value,

Tab-Rules	Field	Description
		you can view the details of the tunnel in a message box
	Priority	Specifies the priority assigned for the rule.
	Pass/Drop	Specifies whether to pass or drop the rule.
	Filters	Specifies the parameters used in the rule. When you hover over the filter value, you can view the details of the filters in a message box.
	Direction	Specifies the direction of the flow of traffic is ingress, egress, or in both direction.
	Ingress Packets	Specifies the aggregate value of the ingress packets associated with the rules.
	Egress Packets	Specifies the aggregate value of the egress packets associated with the rules.
	Ingress Dropped	Specifies the aggregate value of the ingress packets dropped associated with the rules.
	Egress Dropped	Specifies the aggregate value of the egress packets dropped associated with the rules.
	Ingress Errors	Specifies the aggregate value of the ingress errors associated with the rules.
	Egress Errors	Specifies the aggregate value of the egress errors associated with the rules.
UCT		
	Name	Name of the UCT associated with the rule.
	Ingress Packets	Specifies the aggregate value of the ingress packets associated with the rules for an UCT.
	Egress Packets	Specifies the aggregate value of the egress packets associated with the rules for an UCT.
	Ingress Bytes	Specifies the total aggregate value of the ingress bytes associated with the rules for an UCT.
	Egress Bytes	Specifies the total aggregate value of the egress bytes associated with the rules for an UCT.
	Ingress Dropped	Specifies the aggregate value of the ingress packets dropped associated with the rules for an UCT.
	Egress Dropped	Specifies the aggregate value of the egress packets dropped associated with the rules for an UCT.
	Ingress Errors	Specifies the aggregate value of the ingress errors associated with the rules for an UCT.
	Egress Errors	Specifies the aggregate value of the egress errors associated with the rules for an UCT.
Container		
	Pod ID	Specifies the Pod ID associated with the rules .
	Ingress Packets	Specifies the aggregate value of the ingress packets associated with

Tab-Rules Rules	Field	Description
		the ruled for a pod in the UCT.
	Egress Packets	Specifies the aggregate value of the egress packets associated with the ruled for a pod in the UCT.
	Ingress Bytes	Specifies the total aggregate value of the ingress bytes associated with the rules for an UCT.
	Egress Bytes	Specifies the total aggregate value of the egress bytes associated with the rules for an UCT.
	Ingress Dropped	Specifies the total aggregate value of the ingress bytes dropped associated with the rules for an UCT.
	Egress Dropped	Specifies the total aggregate value of the egress bytes dropped associated with the rules for an UCT.
	Ingress Errors	Specifies the total aggregate value of the ingress errors associated with the rules for an UCT.
	Egress Errors	Specifies the total aggregate value of the egress errors associated with the rules for an UCT.

Container

You can view the aggregate value of the packets for a container, and also the rules associated with a container.

The fields and descriptions of the source specifications tab are described in the following table:

Table 4:

Tab- Container Box	Field	Description
UCT		
	Name	Specifies the name of the UCT associated with the rule.
	Ingress packets	Specifies the aggregate value of the ingress packets associated with the pod in a UCT
	Egress packets	Specifies the aggregate value of the egress packets associated with the pod in a UCT
	Ingress Bytes	Specifies the aggregate value of the ingress packets associated with the rules for a pod in the UCT.
	Egress Bytes	Specifies the aggregate value of the egress packets associated with the rules for a pod in the UCT.

Tab- Container Box	Field	Description
	Ingress Dropped	Specifies the aggregate value of the ingress packets dropped associated with the rules for an UCT.
	Egress Dropped	Specifies the aggregate value of the egress packets dropped associated with the rules for an UCT.
	Ingress Errors	Specifies the aggregate value of the ingress errors associated with the rules for an UCT.
	Egress Errors	Specifies the aggregate value of the egress errors associated with the rules for an UCT.
Container		
	Pod ID	Specifies the Pod ID associated with the policy. To support pod name, following section should be added under deployment: name: UCT_POD_NAME valueFrom: field Ref: field Path: metadata.name
	Ingress packets	Specifies the aggregate value of the ingress packets associated with the rule for a pod in the UCT.
	Egress packets	Specifies the aggregate value of the egress packets associated with the rule for a pod in the UCT.
	Ingress Bytes	Specifies the aggregate value of the ingress bytes associated with the rule for a pod in the UCT.
	Egress Bytes	Specifies the aggregate value of the egress bytes associated with the rule for a pod in the UCT.
	Ingress Dropped	Specifies the aggregate value of the ingress packets dropped associated with the rules for an UCT.
	Egress Dropped	Specifies the aggregate value of the egress packets dropped associated with the rules for an UCT.
	Ingress Errors	Specifies the aggregate value of the ingress errors associated with the rules for an UCT.
	Egress Errors	Specifies the aggregate value of the egress errors associated with the rules for an UCT.
Rules	Name	Specifies the rules associated with the container
	Tunnel Specifications	Specifies the tunnel associated with the rules
	Priority	Specifies the priority assigned for the rule.
	Pass/Drop	Specifies whether to pass or drop the rule.
	Filters	
	Direction	Specifies whether the direction of the flow of traffic

Tab- Container Box	Field	Description
		is ingress or egress
	Ingress packets	Specifies the aggregate value of the ingress packets associated with the rules.
	Egress packets	Specifies the aggregate value of the egress packets associated with the rules
	Tunnel Specifications	Specifies the tunnel associated with the rules
	Priority	Specifies the priority assigned for the rule.

Configure UCT Settings

You can configure the following UCT settings in GigaVUE-FM:

- UCT General Settings
- Configure UCT Settings

UCT General Settings

In GigaVUE-FM, you can control the number of permitted connections, refresh intervals and purge time intervals of the UCT solution. You can specify the purge interval to automatically remove the UCTs that are disconnected for a long duration.

> **NOTE:** GigaVUE-FM generates an alarm for the disconnected UCT when the UCT heartbeats are not received for more than 15 minutes. Refer to "Alarms" topic in the *GigaVUE Administration Guide* for detailed information on Alarms.

To edit the UCT general settings:

1. In GigaVUE-FM, navigate to **Inventory > CONTAINER > Universal Container Tap > Settings**, the **Settings** page appears with the existing General settings and UCT information.

2. On the **Settings** page, on the **General** section, click **Edit**. The Edit General Setting's quick view appears.

3. Edit the required values in the **General Settings** section.

Field	Description
Maximum number of connections allowed	Enter the maximum number of connections allowed in the UCT solution
Refresh interval for Container target selection inventory (secs)	Enter a value for the refresh interval for container target selection inventory in seconds
Purge time interval for disconnected UCTs (days)	Enter a value for the purge time interval for the disconnected UCTs in days

4. Click **Save** to save the updates made on the General Settings.

UCT Log Level Settings

In GigaVUE-FM, you can control the level of logs created at each individual UCT for troubleshooting. The regular UCT log file name format is **uct_http2.log**.

To view or edit the UCT log level settings:

1. In GigaVUE-FM, navigate to **Inventory > CONTAINER > Universal Container Tap > Settings**, the **Settings** page appears with the existing General settings and UCT information.

2. On the **Settings** page, on the **UCT** section, on any monitoring domain, click on the UCT fabric. The UCT setting's quick view appears.

3. Edit the required UCT log values in the **LOGGING** section.

Field	Description
Log Level	Select one of the following: • DEBUG—fine-grained log information for application debugging • INFO—coarse-grained log information for highlighting application progress • WARN—log information of potentially harmful situations • ERROR—log information of the error events that allows the application to run continuously • FATAL—log information of very severe error events that presumably lead the application to abort.
Log File Size	Enter a value for the number of lines in the UCT log file.

On any of the above fields, click **Reset** to reset the value to default.

Upgrade UCT

To upgrade UCT, you must perform the following steps:

1. **Upgrade GigaVUE-FM 6.0.00 to GigaVUE-FM 6.1.00**: Before you upgrade UCT 6.0.00 to UCT 6.1.00, you must upgrade GigaVUE-FM 6.00 to GigaVUE-FM 6.1.00. To upgrade the GigaVUE-FM in respective cloud platforms, refer to GigaVUE-FM Installation and Upgrade guide.

2. **Upgrade UCT 6.0.00 to Upgrade UCT 6.1.00**: To upgrade UCT 6.1.00, you must delete the UCT 6.0.00 version and deploy UCT 6.1.00 version. To deploy UCT, refer to Deploy UCT Controller Service and Taps

NOTE: Controller Inventory feature is compatible only with UCT 6.1.00, and it works only when both GigaVUE-FM 6.0.00 and UCT 6.0.00 is upgraded to GigaVUE-FM 6.1.00 and UCT 6.1.00 respectively.

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 Cloud Suite 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 Cloud Suite 6.2 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 Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide

GigaVUE Cloud Suite 6.2 Hardware and Software Guides
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-TA100 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 Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW
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 for AWS–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for Azure–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for OpenStack–GigaVUE V Series 2 Guide
*GigaVUE Cloud Suite for Nutanix Guide—GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for VMware—GigaVUE V Series Guide
*GigaVUE Cloud Suite for Third Party Orchestration
GigaVUE Cloud Suite for AnyCloud Guide
Universal Container Tap Guide

Additional Sources of Information
Documentation

GigaVUE Cloud Suite 6.2 Hardware and Software Guides
Gigamon Containerized Broker Guide
GigaVUE Cloud Suite for AWS–GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for Azure–GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for OpenStack–GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide
GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide
GigaVUE Cloud Suite for AWS Secret Regions Guide
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 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 & Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

Documentation Feedback Form		
About You	**Your Name**	
	Your Role	
	Your Company	

For Online Topics	Online doc link	*(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 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 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)