



Universal Cloud Tap- Container Deployment Guide

GigaVUE Cloud Suite

Product Version: 6.6

Document Version: 1.1

Last Updated: Thursday, October 10, 2024

(See Change Notes for document updates.)

Copyright 2024 Gigamon Inc. All rights reserved.

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

Trademark Attributions

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

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

Change Notes

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

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

Contents

Universal Cloud Tap-Container Deployment Guide	1
Change Notes	3
Contents	4
Universal Cloud Tap - Container	6
Components of Universal Cloud Tap - Container	6
Architecture of Universal Cloud Tap - Container	7
UCT-C and GigaVUE-FM Interaction	8
UCT-C Registration	8
UCT-C Deregistration	8
UCT-C Heartbeats	9
Monitoring Domain and Traffic Policy	9
Get Started with Universal Cloud Tap - Container	9
Pre-requisites of UCT-C	10
License Information	10
Network Requirements	10
Compute Requirements	11
Kernel and CPU Requirements for Universal Cloud Tap - Container	12
Supported Platforms for UCT-C	12
Configure Universal Cloud Tap - Container	12
Create Secret to pull UCT-C image	13
Deploy UCT-C in Kubernetes	13
Deploy UCT-C Controller and Taps	14
Configure UCT-C through GigaVUE-FM	22
Launch GigaVUE-FM	23
Create Monitoring Domain	23
Create Source Selectors	25
Create Tunnel Specifications	27
Configure Traffic Policy	27
Precryption™	33
Secure Tunnels	40
Adding Certificate Authority	43
CA List	43

Configure UCT-C Settings	44
UCT-C General Settings	44
UCT-C Log Level Settings	45
Upgrade UCT-C	46
Steps to Delete and Redeploy UCT-C	47
Debuggability and Troubleshooting	48
Additional Sources of Information	51
Documentation	51
How to Download Software and Release Notes from My Gigamon	54
Documentation Feedback	54
Contact Technical Support	55
Contact Sales	56
Premium Support	56
The VÜE Community	56
Glossary	57

Universal Cloud Tap - Container

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

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

Following are the modules implemented in UCT-C:

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

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

Topics:

- [Architecture of Universal Cloud Tap - Container](#)
- [UCT-C and GigaVUE-FM Interaction](#)
- [Get Started with Universal Cloud Tap - Container](#)
- [Configure Universal Cloud Tap - Container](#)
- [Configure UCT-C Settings](#)
- [Precryption™](#)
- [Secure Tunnels](#)

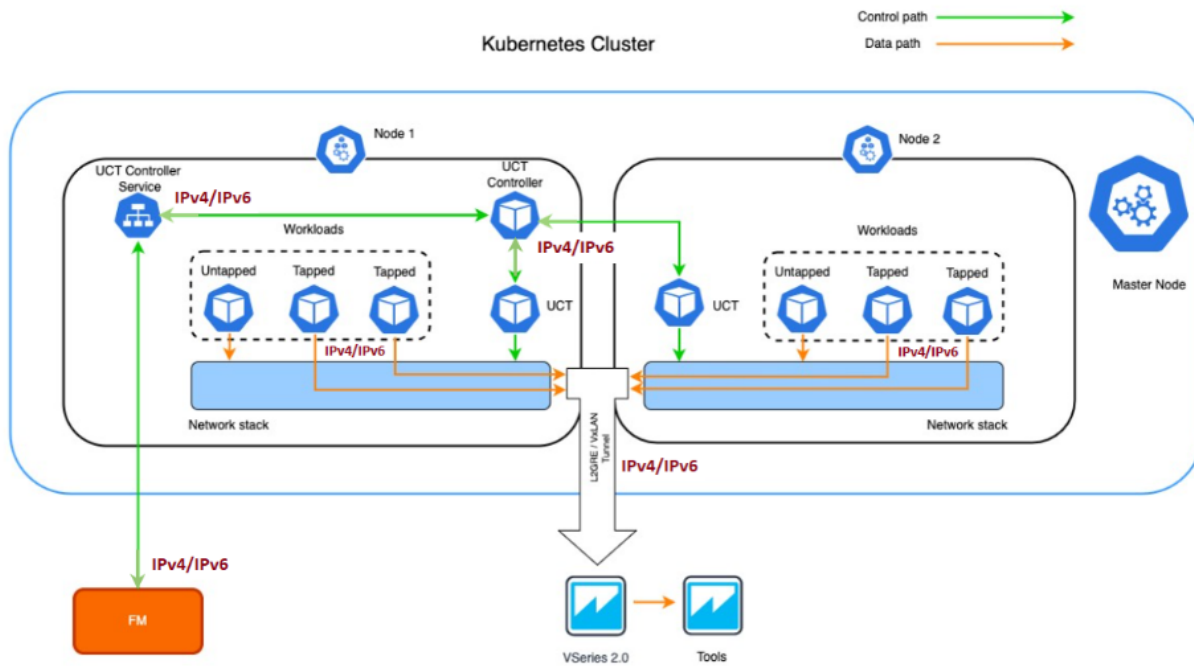
Components of Universal Cloud Tap - Container

The Universal Cloud Tap - Container works with the following components:

- **GigaVUE-FM fabric manager** 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-C.
- **UCT-C Tap** is the primary UCT-C module that collects the workload traffic, filters the traffic and tunnels the filtered traffic directly to the tools or through the GigaVUE V Series Nodes. UCT-C Tap also sends the traffic policy statistics and heartbeats to UCT-C Controller. UCT-C Tap should run as a **privileged pod**.
- **UCT-C Controller** is the management component of UCT-C to control and communicate with UCT-C Tap. UCT-C Controller collects the data from UCT-C Taps and sends the collected statistics and heartbeats to GigaVUE-FM.

Architecture of Universal Cloud Tap - Container

The following diagram illustrates the architecture of Universal Cloud Tap - Container environment.



1. UCT-Ccontroller registers with GigaVUE-FM.
2. The UCT-C Tap is registered with GigaVUE-FM through the UCT-C Controller
3. GigaVUE-FM deploys the traffic policy on the UCT-Cs.
Communication of configuration, data, and statistics to and from UCT-C is performed through the UCT-C Controller Service. GigaVUE-FM communicates with the UCT-C Taps through the UCT-C Controller. GigaVUE-FM deploys the traffic policy on UCT-C and receives the statistics from UCT-C tap through UCT-C controller.
4. 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.
5. The UCT-C Controller collects the data from UCT-C Taps and sends the collected statistics and heartbeats to GigaVUE-FM.

UCT-C and GigaVUE-FM Interaction

Following are the interactions between UCT-C and GigaVUE-FM:

- [UCT-C Registration](#)
- [UCT-C Deregistration](#)
- [UCT-C Heartbeats](#)
- [Monitoring Domain and Traffic Policy](#)

UCT-C Registration

When UCT-C comes up in the Kubernetes environment, UCT-C registers itself with GigaVUE-FM.

Check the network requirements for the registration to be successful. For more information, refer to [Network Requirements](#).

Starting from software version 6.6.00, UCT-C supports IPv6 along with the IPv4 protocol. For more information, refer to [Deploy UCT-C in Kubernetes](#).

UCT-C Deregistration

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

UCT-C Heartbeats

Periodically, UCT-C sends heartbeats to GigaVUE-FM. By default, the status of UCT-C is marked as **Connected**. The following are the various scenarios where the UCT-C 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-C 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-C in GigaVUE-FM. For more information, refer to [Configure UCT-C through GigaVUE-FM](#)

Refer to the [GigaVUE API Reference](#) for detailed information on the REST APIs of UCT-C.



- 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 Cloud Tap - Container

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

Refer to the following sections for details:

- [Pre-requisites of UCT-C](#)
- [Components of Universal Cloud Tap - Container](#)
- [License Information](#)
- [Network Requirements](#)
- [Compute Requirements](#)

Pre-requisites of UCT-C

The following are the pre-requisites of UCT-C:

- Deploy the GigaVUE-FM (FM) on the subnet where Kubernetes cluster is deployed.
- GigaVUE-FM and Kubernetes Cluster should be up and running.
- To work with UCT-C, you must have knowledge in the following platforms:
 - Kubernetes
 - GigaVUE-FM
 - Knowledge to work in any platform such as AWS EKS, Azure AKS, and RedHat OpenShift where the Kubernetes clusters are deployed.

License Information

All the UCT-C Taps deployed in your environment periodically report the statistics to UCT-C Controller. Then the UCT-C Controller periodically reports the collective statistics of UCT-C 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 accounting purpose. GigaVUE-FM tracks the total amount of data processed by the UCT-C, 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-C to work efficiently.

Direction	Type	Protocol	Port	CIDR	Purpose
Universal Cloud Tap - Container deployed inside Kubernetes worker node					
Outbound	HTTPS	TCP	443	Any IP address	Allows UCT-C Controller to communicate with GigaVUE-FM

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

The following table describes the ports that should be opened on GigaVUE-FM:

Direction	Port	Purpose
Inbound	443	GigaVUE-FM REST service port.
Outbound	8443	Allows GigaVUE-FM to communicate with UCT-C Controller.
Inbound	5671	Allows UCT-C to send statistics to GigaVUE-FM through Rabbit-MQ port.

Compute Requirements

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

Compute Instances	vCPU	Memory	Disk Space
UCT-C Controller	1 vCPU	refer to the table below	—
UCT-C Tap	1 vCPU	1GB	—
GigaVUE V Series Node	4 vCPUs	8GB	20GB
GigaVUE V Series Proxy	1 vCPU	1GB	2GB
GigaVUE-FM	4 vCPUs	16GB	41GB

Compute Instances	Memory	Cluster Size
UCT-C Controller	256MB	less than 1000 pods
UCT-C Controller	512MB	2000 pods
UCT-C Controller	1GB	up to 3000 pods

Kernel and CPU Requirements for Universal Cloud Tap - Container

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-C Tap - 1Vcpu and 1G
- UCT-C Controller - 1Vcpu and 1G

Supported Platforms for UCT-C

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-C.

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

Platform	Kubernetes Version	CRI	CNI
Amazon Elastic Kubernetes Service (EKS)	1.26	Containerd	VPC
Azure Kubernetes Service (AKS)	1.24	Containerd	Azure CNI
VMware Tanzu	1.20	Containerd	Antrea and Calico
Red Hat OpenShift	1.22	CRI-O	OVN
Native Kubernetes	1.26, 1.28, 1.29	Containerd	Flannel, Cilium, and Calico

Configure Universal Cloud Tap - Container

Setting up UCT-C involves the following two steps:

- [Deploy UCT-C in Kubernetes](#)
- [Configure UCT-C through GigaVUE-FM](#)



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

Create Secret to pull UCT-C image

To create secret, follow these steps:

1. Get the **username/key/password** from support team and encode using the command:

```
echo -n <<user name>>:<<keys>> | base64
```

2. Update the keys in the following content and save it as a JSON file:

```
{
  "auths": {
    "https://index.docker.io/v1/": {
      "auth": "<<keys>>"
    }
  }
}
```

3. Create secret using the following command (regcred is used as name of the secret in this doc):

```
kubectl create secret generic <<name of the secret>> --from-
file=.dockerconfigjson=<<json file path >>
--type=kubernetes.io/dockerconfigjson -n <<namespace where UCT-C Controller
and tap will be deployed>>
```

Deploy UCT-C in Kubernetes

To fully deploy UCT-C, 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-C Controller and GigaVUE-FM.
2. Ensure that the firewall rules on Kubernetes nodes are met according to the [Network Requirements](#).
3. YAML files or HELM charts are available as part of the UCT-C images. You should untar the UCT-C image to get the readme files.

4. Add the UCT-C 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-C instances based on your traffic load.
5. Deploy UCT-C Controller and Taps using YAML files or Helm Charts. Refer to [Deploy UCT-C Controller and Taps](#).

Deploy UCT-C Controller and Taps

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

- [Using YAML files](#)
- [Using Helm Charts](#)

Using YAML files

Starting from software version 6.4.00, YAML files will be available for each and every release build in the Gigamon software portal. Download the respective UCT-C release build from the repository and untar the **.tgz** file. After you finish untarring the file, you can extract the YAML file and further update the following fields in **uctc-controller.yaml** and **uctc-tap.yaml** file.

NOTE: [Contact Technical Support](#) or [Contact Sales](#) for information on downloading the respective UCT-C build from the Gigamon software portal.

Deployment of UCT-C Controller

Follow these steps to deploy the UCT-C Controller:

- Use the below command to Unzip and Untar the .tgz file:

```
gunzip <name of the UCT-C Controller .tgz file>
tar -xvf <name of the UCT-C Controller .tar file>
```

After extracting the tar file, navigate to the YAML folder in the newly created **uctc-ctrlr-<image version>-<build number>** folder and update the details given in the below steps.

- Provide the created **secret** in the following section of the YAML file:

```
imagePullSecrets:
- name: <secret>
```

- Provide the **FM IP address** in the following section of the YAML file:

```
command:
- /uct-controller
- <FM IPv4 or FM IPv6 or FM IPv4,FM IPv6(both with comma-separation notation)>
- '443'
- '8443'
```

- '0'
- "/etc/gcbcerts"
- "gcb-cert.pem"
- "gcb-pvt-key.pem"
- "gcb-ca-root-cert.pem"

Refer to the below examples:

- ```
example1: 192.168.0.10 (IPv4)
example2: 2001:db8:abcd:ef01::5 (IPv6)
example3: 192.168.0.10,2001:db8:abcd:ef01::5 (IPv4,IPv6)
```

- If you provide both IPv4 and IPv6 addresses in the above argument, the following configurations will be used:
  - name: UCTC\_CNTLR\_FM\_IP\_CONFIG  
value: IPv4 or IPv6
  - name: UCTC\_CNTLR\_FALLBACK\_CONFIG  
value: True or False

**IP CONFIG** option allows the user to provide the preferred IP version. If the user does not provide any value, default value IPv4 will be used.

When the preferred IP version fails to connect (example: IPv6), **FALLBACK CONFIG** will be used to connect to the other available IP version (example: IPv4). Default value True will be used to consider the Fallback mechanism.



**Note**

- Fallback configuration will be used during node registration phase only.
- Controller FM IP and FALLBACK configurations will be used only if you provide both IPv4 and IPv6.
- If you provide IPv4 alone, only IPv4 connections will be considered, and FM IP and FALLBACK configurations will be disregarded. Similarly, if IPv6 alone is provided, only IPv6 connections will be considered.
- Default values will be used if you do not provide any options.

- Provide **UCT-C Cntrl External IP** and **Kubernetes Cluster API URL** in the following section of the YAML file:

- ```
env:
- name: UCTC_CNTLR_SERVICE_NAME
value: "GIGAMON_UCTC_CNTLR_SERVICE"
- name: UCTC_CNTLR_EXT_IP_DNS
value: "<external IPv4 or external IPv6 or external IPv4,IPv6 (both with comma-separation notation) or DNS"
```

Refer to the below examples:

- ```
example1: 192.168.0.10 (IPv4)
example2: 2001:db8:abcd:ef01::5 (IPv6)
example3: 192.168.0.10,2001:db8:abcd:ef01::5 (IPv4,IPv6)
example4: gigamon.example.com
```

```
- name: K8S_CLUSTER_ENDPOINT
value: <K8s Cluster API URL>
Refer to the below example:
example: https://10.10.10.13:6443
- name: FM_FQDN
value: www.fm.gigamon.com
```

- Update the namespace in the YAML file as required and run the following command:

```
kubectl create -f uctc-controller.yaml
```

Following the execution of the above command, when UCT-C Controller pod is created successfully, the output (sample) will be as below:

```
gigamon@controller-2:~$kubectl create -f uctc-controller.yaml
service/gigamon-uctc-cntlr-service created
deployment.apps/uctc-cntlr-v1 created
clusterrole.rbac.authorization.k8s.io/pods-list created
clusterrolebinding.rbac.authorization.k8s.io/pods-list created
```

## Deployment of UCT-C Tap

Follow these steps to deploy the UCT-C Tap:

- Use the below command to Unzip and Untar the .tgz file:

```
gunzip <name of the UCT-C Tap .tgz file>
tar -xvf <name of the UCT-C Tap .tar file>
```

After extracting the tar file, navigate to the YAML folder in the newly created **uctc-tap-<image version>-<build number>** folder and update the details given in the below steps.

- Feed the created **secret** in the below section of YAML file

```
imagePullSecrets:
- name: <secret>
```

- Update the namespace in the below section of YAML file as required. This should be same as the namespace in which UCT-C controller is deployed.

```
- name: UCTC_CNTLR_SVC_DNS
value: gigamon-uctc-cntlr-service.<namespace>.svc.cluster.local
```


- When UCT-C TAP gets both IPv4 and IPv6 from the above controller service DNS, the following configurations will be used:

```
- name: UCTC_TAP_IP_CONFIG
value: IPv4 or IPv6
- name: UCTC_TAP_FALLBACK_CONFIG
value: True or False
```

**IP CONFIG** option allows the user to provide the preferred IP version. If the user does not provide any value, default value IPv4 will be used.



When the preferred IP version fails to connect (example: IPv6), **FALLBACK CONFIG** will be used to connect to the other available IP version (example: IPv4). Default value True will be used to consider the Fallback mechanism.

 **Note**

- Fallback configuration will be considered during node registration only.
- If IPv4 alone is provided, only IPv4 connections will be considered, and IP and FALLBACK configurations will be disregarded. Similarly, if IPv6 alone is provided, only IPv6 connections will be considered.
- Default values will be used if TAP gets dual IP's from the controller service DNS.

- Edit the following **volumeMounts** as per your container Runtime.

```

volumeMounts:
 - name: socket
 mountPath: /var/run/containerd/containerd.sock

volumes:
 - name: socket
 hostPath:
 Path: /var/run/containerd/containerd.sock

```

Below are the socket location for commonly used CRIs,

```

docker - /var/run/docker.sock
containerd - /var/run/containerd/containerd.sock
cri-o - /var/run/crio/crio.sock

```

- Run the following command for deploying UCT-C Tap:

```
kubectl create -f uctc-tap.yaml -n <namespace where UCT-C tap has to be deployed>
```

Following the execution of the above command, when UCT-C Tap pod is created successfully, the output (sample) will be as below:

```

gigamon@controller-2:~$ kubectl create -f uctc-tap.yaml -n uctc
daemonset.apps/gigamon-uctc created

```

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-C Controller REST service port number.                                                                                                                                                                             |
| Port: 42042               | This port must be port 42042. Allows UCT-C to send statistics information to UCT-Ccontroller.                                                                                                                              |
| GigaVUE-FM IP             | The IP address of the GigaVUE-FM with which your UCT-C is connected.                                                                                                                                                       |
| UCT-C-Cntrl REST SVC Port | The UCT-C 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-C Controller.<br>Example: 8443 (configurable) |
| FM REST Svc Port          | The FM REST service port number. This must be opened on your Kubernetes to allow outbound traffic. This allows UCT-C Controller to communicate with GigaVUE-FM.                                                            |

| Field Values                                               | Description                                                                                                                                                                                                     |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                            | Example: 443                                                                                                                                                                                                    |
| Ports:<br>containerPort:<br>443<br>containerPort:<br>42042 | Two ports must be opened. The first container port must be the same as UCT-C-Cntlr REST SVC Port. The second container port must be port 42042. This allows UCT-C to send statistical data to UCT-C controller. |
| External LB balancer IP                                    | The external load balancer IP/DNS value to allow GigaVUE-FM to communicate with UCT-C Controller within Kubernetes.                                                                                             |
| K8S cluster end-point                                      | Kubernetes cluster end point for GigaVUE-FM to access the control plane.<br>Example: https://<kubernetesapiserverurl>:6443                                                                                      |

## Using Helm Charts

Starting from software version 6.4.00, Helm Charts will be available for each and every release build in the Gigamon software portal. Download the respective UCT-C release build from the repository and untar the **.tgz** file. After you finish untarring the file, you can extract the Helm Charts (**uct-cntlr-<version>.tgz** and **uct-tap-<version>.tgz**) and further update the following fields before deployment.

**NOTE:** [Contact Technical Support](#) or [Contact Sales](#) for information on downloading the respective UCT-C build from the Gigamon software portal.

### Deploy using Single Helm Chart

Starting from software version 6.6.00, you can deploy UCT-C Controller and Taps using single Helm Chart. Follow the steps listed below to deploy the solution.

- Use the below command to Unzip and Untar the .tgz file:

```
gunzip <name of the UCT-C .tgz file>
tar -xvf <name of the UCT-C .tar file>
```

After extracting the tar file, navigate to the Helm folder in the newly created **uctc-<image version>-<build number>** folder and update the details given in the below steps.

- Update the **imagePullSecrets**, **namespace**, **GigaVUE-FM IP**, **external load balancer IP** and **Kubernetes API URL** in the following section of the **values.yaml** file present in the UCT-C directory.

```
imagePullSecrets: [{name: regcred}]
namespace: uct
```

If you provide IPv4 alone and not IPv6, then GigaVUE-FM will consider only IPv4 address for communication.

```
fm_ip: "<FM IPv4>"
```

If you provide IPv6 alone and not `fm_ip`, then GigaVUE-FM will consider only IPv6 address for communication.

```
fm_ipv6: "<FM IPv6>"
```

If both IPv4 and IPv6 are provided, `UCTC_CNTL_R_FM_IP_CONFIG` will be used to choose the preferred IP stack.

```
ext_load_balancer: "<FM IPv4 or FM IPv6 or FM IPv4,FM IPv6(both with comma-separation notation)>"
```

Refer to the below examples:

```
example1: 192.168.0.10 (IPv4)
```

```
example2: 2001:db8:abcd:ef01::5 (IPv6)
```

```
example3: 192.168.0.10,2001:db8:abcd:ef01::5 (IPv4,IPv6)
```

```
k8s_cluster_url: "<url>"
```

```
example: https://10.10.10.12:6443
```

- If you provide two IP's, IPv4 and IPv6 in the `fm_ip` argument, the following configurations will be used:

```
values: <IPv4 | IPv6>
```

```
uctc_tap_ip_config: "IPv4"
```

```
values: <true | false>
```

```
uctc_tap_fallback_config: "false"
```

**IP CONFIG** option allows the user to provide the preferred IP version. If the user does not provide any value, default value IPv4 will be used.

When the preferred IP version fails to connect (example: IPv6), **FALLBACK CONFIG** will be used to connect to the other available IP version (example: IPv4). Default value True will be used to consider the Fallback mechanism.



#### Note

- Fallback configuration will be used during node registration phase only.
- Controller FM IP and FALLBACK configurations will be used only if you provide both IPv4 and IPv6.
- Default values will be used if you do not provide any options.

- Edit the following **volumeMounts** as per your container Runtime:

```
crisocketvolume:
```

```
mountPath: /var/run/containerd/containerd.sock
```

```
name: socket
```

The socket location for commonly used CRIs are as follows:

```
docker - /var/run/docker.sock
```

```
containerd - /var/run/containerd/containerd.sock
```

```
cri-o - /var/run/crio/crio.sock
```

- Run the below command in the location where UCT-C folder is present.

```
helm install uctc ./uctc -n <Namespace>
```

- Run the below command to validate the deployment and check for any failures.  
`helm test uctc`

## Deploy using Two Helm Charts

### Deployment of UCT-C Controller

- Use the below command to Unzip and Untar the .tgz file:

```
gunzip <name of the UCT-C Controller .tgz file>
tar -xvf <name of the UCT-C Controller .tar file>
```

After extracting the tar file, navigate to the Helm folder in the newly created **uctc-cntlr-*<image version>-<build number>*** folder and update the details given in the below steps.

- Update the **imagePullSecrets, namespace, GigaVUE-FM IP, external load balancer IP** and **Kubernetes API URL** in the following section of the **values.yaml** file present in UCT-C-cntlr directory.

```
imagePullSecrets: [{name: regcred}]
namespace: uct
fm_ip: "<FM IPv4 or FM IPv6 or FM IPv4,FM IPv6(both with comma-separation notation>"
ext_load_balancer: "<FM IPv4 or FM IPv6 or FM IPv4,FM IPv6(both with comma-separation notation>"
```

Refer to the below examples:

```
example1: 192.168.0.10 (IPv4)
example2: 2001:db8:abcd:ef01::5 (IPv6)
example3: 192.168.0.10,2001:db8:abcd:ef01::5 (IPv4,IPv6)
k8s_cluster_url: "<url>"
example: https://10.10.10.12:6443
```

- If you provide IPv6 address alone in the fm\_ip argument, the following configuration will be used.

```
- name: UCTC_CNTLR_IP_CONFIG
value: 'IPv6'
```

- If you provide both IPv4 and IPv6 addresses in the fm\_ip argument, the following configurations will be used:

```
- name: UCTC_CNTLR_FM_IP_CONFIG
value: IPv4 or IPv6
- name: UCTC_CNTLR_FALLBACK_CONFIG
value: True or False
```

**IP CONFIG** option allows the user to provide the preferred IP version. If the user does not provide any value, default value IPv4 will be used.

When the preferred IP version fails to connect (example: IPv6), **FALLBACK CONFIG** will be used to connect to the other available IP version (example: IPv4). Default value True will be used to consider the Fallback mechanism.



Note

- Fallback configuration will be used during node registration phase only.
- Controller FM IP and FALLBACK configurations will be used only if you provide both IPv4 and IPv6.
- If you provide IPv4 alone, only IPv4 connections will be considered, and FM IP and FALLBACK configurations will be disregarded.
- Default values will be used if you do not provide any options.

- Run the below command in the location where UCT-C-cntlr folder is present to bring up UCT-C Controller.

```
helm install uctc-cntlr ./uctc-cntlr -n <Namespace>
```

Following the execution of the above command, when UCT-C Controller pod is created successfully, the output (sample) will be as below:

```
gigamon@controller-2:~$ helm install uctc-cntlr ./uctc-cntlr -n uctc
NAME: uctc-cntlr
LAST DEPLOYED: Sat Feb 3 13:11:11 2024
NAMESPACE: uctc
STATUS: deployed
REVISION: 1
TEST SUITE: None
```

- In dual stack cluster, update the following fields in **uctc-cntlr-service** to deploy dual stack setup.

```
Spec:
ipFamilies:
- Ipv4
- IPv6
ipFamilyPolicy: PreferDualStack
```

**Deployment of UCT-C Tap**

- Use the below command to Unzip and Untar the .tgz file:

```
gunzip <name of the UCT-C Tap .tgz file>
tar -xvf <name of the UCT-C Tap .tar file>
```

After extracting the tar file, navigate to the Helm folder in the newly created **uctc-tap-<image version>-<build number>** folder and update the details given in the below steps.

- Update the **imagePullSecrets, namespace** in the following section of **values.yaml** file present in UCT-C-tap directory. This should be same as the namespace in which UCT-C- Controller is deployed.

```
imagePullSecrets: [{name: regcred}]
namespace: uct
```

- If you provide IPv6 address alone in the fm\_ip argument, the following configuration will be used.

```
- name: UCTC_TAP_IP_CONFIG
value: 'IPv6'
```

- If you provide both IPv4 and IPv6 addresses in the `fm_ip` argument, the following configurations will be used:

```
- name: UCTC_TAP_IP_CONFIG
value: IPv4 or IPv6
- name: UCTC_TAP_FALLBACK_CONFIG
value: True or False
```

**IP CONFIG** option allows the user to provide the preferred IP version. If the user does not provide any value, default value IPv4 will be used.

When the preferred IP version fails to connect (example: IPv6), **FALLBACK CONFIG** will be used to connect to the other available IP version (example: IPv4). Default value True will be used to consider the Fallback mechanism.

- Edit the following **volumeMounts** as per your container Runtime:

```
crisocketvolume:
mountPath: /var/run/containerd/containerd.sock
name: socket
```

The socket location for commonly used CRIs are as follows:

```
docker - /var/run/docker.sock
containerd - /var/run/containerd/containerd.sock
cri-o - /var/run/crio/crio.sock
```

- Run the below command in the location where UCT-C-tap directory is present to bring up UCT-C Tap.

```
helm install uctc-tap ./uctc-tap -n <namespace>
```

Following the execution of the above command, when UCT-C Tap pod is created successfully, the output (sample) will be as below:

```
gigamon@controller-2:~$ helm install uctc-tap ./uctc-tap -n uctc
NAME: uctc-tap
LAST DEPLOYED: Sat Feb 3 13:11:14 2024
NAMESPACE: uctc
STATUS: deployed
REVISION: 1
TEST SUITE: None
```

## Configure UCT-C through GigaVUE-FM

This section describes how to configure UCT-C 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 Node supported cloud environment. For assistance, [Contact Technical Support](#) of Gigamon or refer to GigaVUE Cloud Suite for more information on GigaVUE V Series 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 Cloud Tap - Container > Monitoring Domains**. The **Monitoring Domain** page appears.
2. In the **Monitoring Domain** page, click **New**. The **New Monitoring Domain** wizard appears.
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-C connection  |
| Cluster Name           | Enter a name for the cluster           |
| URL                    | Enter the URL of the API server        |

- Click  to add another connection and click  to remove an existing connection.
4. Click **Save** to create a monitoring domain.

**NOTE:** If the connecting UCT-C Tap does not send 3 continuous heart beats, it is marked as disconnected and it is shown on the monitoring domain page as per the interval configured in the UCT-C Purge (the default purge interval is 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-C and controllers:

- Monitoring Domain
- URL
- Connection
- Cluster Name
- Cluster Version
- Controller / TAP
- UCT-C UUID
- Management IP
- Version
- Node Name
- Node Kernel Version
- Status -If you enable Secure Tunnel, its status can be viewed in Monitoring Domain page.
- Discovered Sources

**NOTE:** You need to refresh pages manually in UCT-C Monitoring Domain and Policy Page as the automatic GUI refresh is disabled.

Use the following buttons to manage your Monitoring Domain:

| Button  | Description                                                                                                                                                                                                              |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| New     | Use to create new connection                                                                                                                                                                                             |
| Actions | Provides the following options: <ul style="list-style-type: none"> <li>▪ <b>Edit</b>- Edit the monitoring domain</li> <li>▪ <b>Delete Domain</b> - Delete the monitoring domain</li> </ul>                               |
| Filter  | Filters the monitoring domain based on the following options: <ul style="list-style-type: none"> <li>▪ <b>Connected</b></li> <li>▪ <b>Pending</b></li> <li>▪ <b>Disconnected</b></li> <li>▪ <b>Terminated</b></li> </ul> |

 **Notes:**

- You can click on the **Discovered Sources** link to view the source details. In the Discovered Sources window, you can enable the **Show System Pods** button to view the information related to the system pods that are not monitored.
- Gigamon cannot tap traffic if hostnetworks are set to true in pods.







## 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                                                                                                                              |
| <b>Include Filters (Criteria 1)</b>                                                                                                                                                                                                                                                                                                 |                                                                                                                                                          |
| You can select any one of the following options                                                                                                                                                                                                                                                                                     |                                                                                                                                                          |
| <ul style="list-style-type: none"> <li>• <b>All Sources</b> - Select this option to acquire traffic from all names, all pods and containers within the selected cluster(s). Depending on the size of the cluster(s), volume of traffic may be larger.</li> <li>• <b>Criteria1</b>- You must enter the following options:</li> </ul> |                                                                                                                                                          |
| Object Property                                                                                                                                                                                                                                                                                                                     | Select an object property to filter the traffic source.                                                                                                  |
| Operator                                                                                                                                                                                                                                                                                                                            | Select the operator.                                                                                                                                     |
| Values                                                                                                                                                                                                                                                                                                                              | Enter the values for the filter. Values are case-sensitive.                                                                                              |
| <p><b>On the Criteria, click  to add another Object and click  to remove an existing Object.</b></p>                                                            |                                                                                                                                                          |
| <b>Exclude Filters (Criteria 1)</b>                                                                                                                                                                                                                                                                                                 |                                                                                                                                                          |
| 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: <ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• startswith</li> <li>• endwith</li> </ul> |
| Values                                                                                                                                                                                                                                                                                                                              | Enter the values for the filter. Values are case-sensitive.                                                                                              |

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.



**Notes:** 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, VXLAN, or TLS-PCAPNG, can be created. The tunnel is an egress tunnel. For more information to create a tunnel of type TLS-PCAPNG, refer to [Secure Tunnels](#)

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**

**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, VXLAN, or TLS-PCAPNG 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-C Traffic Policy in GigaVUE-FM:

1. From the GigaVUE-FM left navigation pane, select **Traffic > CONTAINER > Universal Cloud Tap - Container**. The **Policies** page appears.
2. In the **Policies** page, click **Create**. You can create a maximum of eight policies per monitoring domain. 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. The name must be unique.                                                                                                     |
| Monitoring Domain | Select an existing monitoring domain. To create a new monitoring domain, refer to <a href="#">Create Monitoring Domain</a> section.                               |
| Connections       | Select one or more connections for the policy. Once traffic policy is created for monitoring domain, you cannot add or delete connections in a monitoring domain. |

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. You can configure a maximum of eight source selectors per policy.
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. You must select CA in the Monitoring Domain page to use secure tunnel in rules.

6.

| Fields                                                                                                                                                                                                                                                                                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Rules</b>                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| On the Ingress or Egress rules, click  to add another rule and click  to remove an existing rule. You must select CA in the Monitoring Domain page to use secure tunnel in rules. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Rule Name                                                                                                                                                                                                                                                                                                                                             | Enter a name for the rule.<br><br><b>NOTE:</b> Rule names ending with __I, __E, __RI, __RE are not recommended as the names are invalid in policy rules.                                                                                                                                                                                                                                                                                                                                                   |
| Enable                                                                                                                                                                                                                                                                                                                                                | Select <b>On</b> to enable the filter or select <b>Off</b> 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: <ul style="list-style-type: none"> <li>• 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.</li> <li>• Ingress- Taps the ingress traffic.</li> <li>• Egress - Taps the egress traffic.</li> <li>• Ingress Pass All - Taps all the ingress traffic.</li> <li>• Egress Pass All - Taps all the egress traffic.</li> </ul> |
| Priority                                                                                                                                                                                                                                                                                                                                              | Enter a priority value to specify the precedence.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Tunnel Specifications                                                                                                                                                                                                                                                                                                                                 | Select an existing tunnel or select <b>Create New</b> to create a new tunnel, refer to <a href="#">Create Tunnel Specifications</a> section for detailed information.                                                                                                                                                                                                                                                                                                                                      |
| <b>Filters</b>                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

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

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

**NOTE:** When there are two or more policies configured within the same tunnel, you cannot edit the tunnel specifications that are shared in the policies. In such cases, delete all the policies sharing the same tunnel specifications, modify the existing tunnel specifications, and create new policies for the policies that are deleted using the modified tunnel specifications.

## Traffic Policy Statistics

Traffic Policy Statistics in the GigaVUE-FM provides the visibility of the policies within a Monitoring Domain and displays the information of the policies and its rules statistics in the dashboard.

Rules are configured in the UCT-C to either forward the traffic to a Tunnel or drop the flow of the traffic.

The activities of the rules are reflected by the statistics counters. The statistics counters show how the policy statistics are 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 > UCT-C**. 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-C 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 : <ul style="list-style-type: none"> <li>• Success</li> <li>• Failure</li> <li>• No Target Selected</li> </ul> |
| UCT-C Deployment Details | Specifies the count of successful deployment along with the total number of deployment for a policy.                                                      |
| Ingress packets          | Total aggregate value of the ingress packets associated with the policy.                                                                                  |

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

You can view the following tabs along with the policy name:

- [Source Specifications](#)
- [Rules](#)

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-                         | Field         | Description                                                                                                                                       |
|------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Source Specifications</b> |               |                                                                                                                                                   |
| <b>Source Selector</b>       |               |                                                                                                                                                   |
|                              | Name          | Specifies the name of the Source selector.                                                                                                        |
| <b>Include Criteria</b>      |               |                                                                                                                                                   |
|                              | 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:                                                                                |

| Tab-Source Specifications | Field         | Description                                                                                                                                                  |
|---------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           |               | service                                                                                                                                                      |
|                           | Operator      | Specifies the operator used in the criteria.                                                                                                                 |
|                           | Value         | Specifies the value for the attributes in the criteria.                                                                                                      |
| <b>Exclude Criteria</b>   |               |                                                                                                                                                              |
|                           | Criteria Name | Specifies the exclude criteria for the source selector. Pod that matches the exclude criteria will be excluded from 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 excluded.                                                |
|                           | 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 excluded.                                                                           |

### Rules

You can view the aggregate value of all the rules the policy has been configured for the node in the UCT-C 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                                                                                                                                                                                          |
|--------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Rules</b> |                       |                                                                                                                                                                                                      |
|              | 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, 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                                                                                                                             |



| Tab-Rules | Field           | Description                                                                             |
|-----------|-----------------|-----------------------------------------------------------------------------------------|
| Rules     |                 | 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.           |

## Precription™

**License:** Requires **SecureVUE Plus** license.

Gigamon Precription™ technology<sup>1</sup> redefines security for virtual, cloud, and containerized applications, delivering plaintext visibility of encrypted communications to the full security stack, without the traditional cost and complexity of decryption.

This section explains about:

- [How Gigamon Precription Technology Works](#)
- [Why Gigamon Precription](#)
- [Key Features](#)
- [Key Benefits](#)
- [Precription Technology on Single Node](#)
- [Precription Technology on Multi-Node](#)
- [Supported Platforms](#)

---

<sup>1</sup>**Disclaimer:** The Precription feature allows users to acquire traffic after it has been decrypted. This traffic can be acquired from both virtual machine (VM) and container-based solutions, and is then sent to the V Series product for further processing. The Precription feature provides an option to use encrypted tunnels for communication between the acquisition (via UCT or G-vTAP) of unencrypted traffic and the traffic processing (at the V Series) which will better safeguard the traffic while in transit. However, if a user does not use the option for encrypted tunnels for communication, decrypted traffic will remain unencrypted while in transit between the point of acquisition and processing.

Please note that this information is subject to change, and we encourage you to stay updated on any modifications or improvements made to this feature.

By using this feature, you acknowledge and accept the current limitations and potential risks associated with the transmission of decrypted traffic.

- [Prerequisites](#)

## How Gigamon Precryption Technology Works

Precryption technology leverages native Linux functionality to tap, or copy, communications between the application and the encryption library, such as OpenSSL.



In this way, Precryption captures network traffic in plaintext, either before it has been encrypted, or after it has been decrypted. Precryption functionality doesn't interfere with the actual encryption of the message nor its transmission across the network. There's no proxy, no retransmissions, no break-and-inspect. Instead, this plaintext copy is forwarded to the Gigamon Deep Observability Pipeline for further optimization, transformation, replication, and delivery to tools.

Precryption technology is built on GigaVUE® Universal Cloud Tap (UCT) and works across hybrid and multi-cloud environments, including on-prem and virtual platforms. As a bonus, UCT with Precryption technology runs independent of the application, and doesn't have to be baked into the application development lifecycle.

## Why Gigamon Precryption

GigaVUE Universal Cloud Tap with Precryption technology is a lightweight, friction-free solution that eliminates blind spots present in modern hybrid cloud infrastructure, providing East-West visibility into virtual, cloud, and container platforms. It delivers unobscured visibility into all encryption types including TLS 1.3, without managing and maintaining decryption keys. IT organizations can now manage compliance, keep private communications private, architect the necessary foundation for Zero Trust, and boost security tool effectiveness by a factor of 5x or more.

## Key Features

The following are the key features of this technology:

- Plaintext visibility into communications with modern encryption (TLS 1.3, mTLS, and TLS 1.2 with Perfect Forward Secrecy).
- Plaintext visibility into communications with legacy encryption (TLS 1.2 and earlier).
- Nonintrusive traffic access without agents running inside container workloads.

- Elimination of expensive resource consumption associated with traditional traffic decryption.
- Elimination of key management required by traditional traffic decryption.
- Zero performance impact based on cipher type, strength, or version.
- Support across hybrid and multi-cloud environments, including on-prem, virtual, and container platforms.
- Keep private communications private across the network with plaintext threat activity delivered to security tools.
- Integration with Gigamon Deep Observability Pipeline for the full suite of optimization, transformation, and brokering capabilities.

## Key Benefits

The following are the key benefits of this technology:

- Eliminate blind spots for encrypted East-West (lateral) and North-South communications, including traffic that may not cross firewalls.
- Monitor application communications with an independent approach that enhances development team velocity.
- Extend security tools' visibility to all communications, regardless of encryption type.
- Achieve maximum traffic tapping efficiency across virtual environments.
- Leverage a 5–7x performance boost for security tools by consuming unencrypted data.
- Support a Zero Trust architecture founded on deep observability.
- Maintain privacy and compliance adherence associated with decrypted traffic management.

## How Gigamon Precryption Technology Works

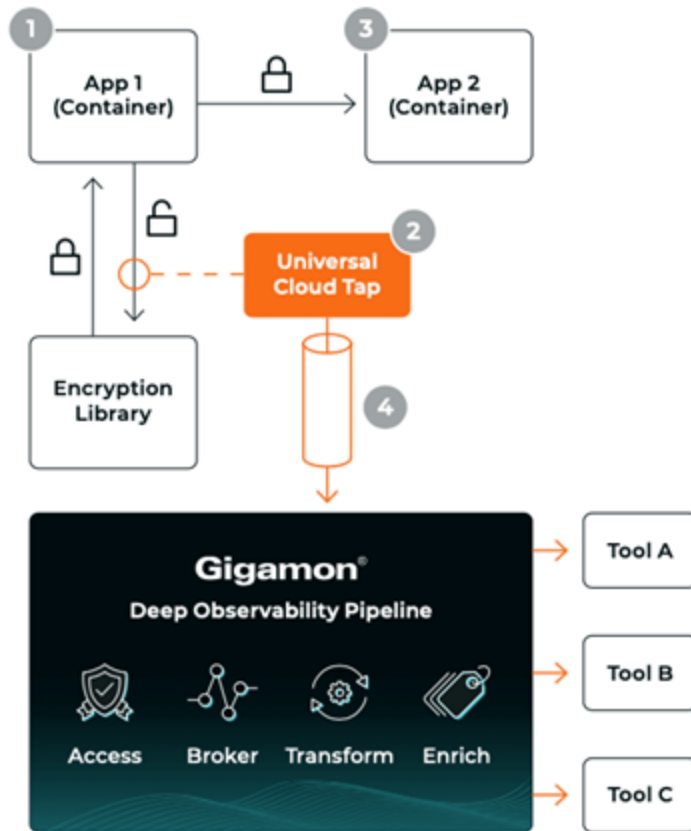
This section explains about how Precryption technology works on single node and multiple node in the following sections:

- [Precryption Technology on Single Node](#)
- [Precryption Technology on Multi-Node](#)

### **Precryption Technology on Single Node**

1. When any application needs to encrypt a message, it uses an encryption library, such as OpenSSL, to perform the actual encryption.
2. GigaVUE Universal Cloud Tap (UCT), enabled with Precryption technology, gets a copy of this message before it's encrypted on the network.
3. The encrypted message is sent to the receiving application, with unmodified encryption. No proxy, no re- encryption, no retransmissions.

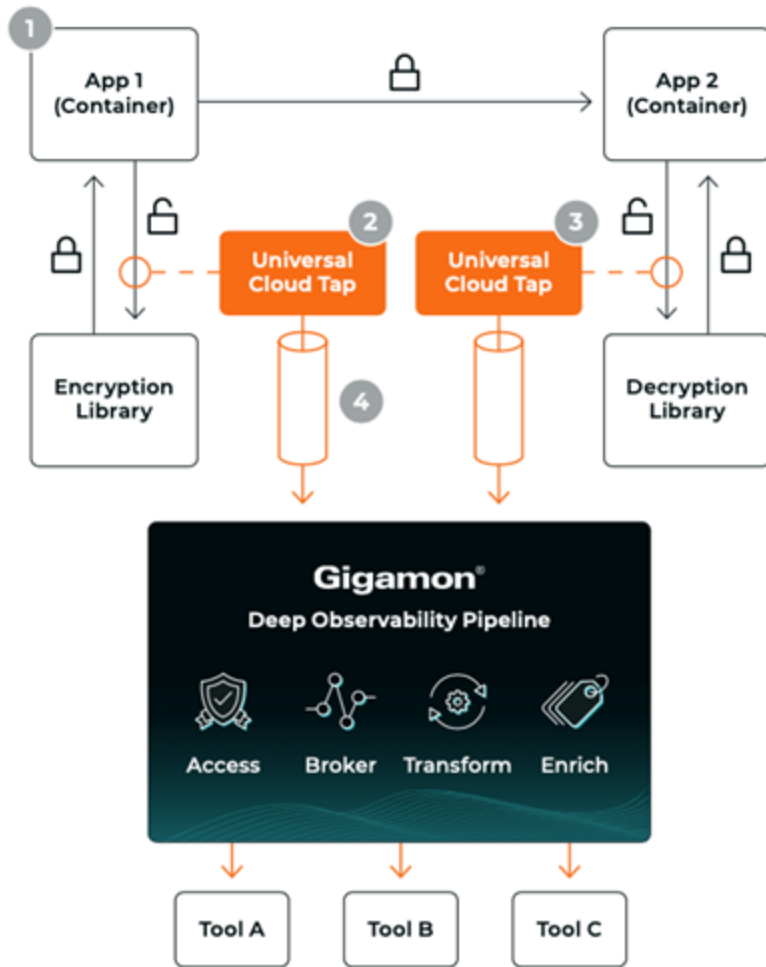
4. GigaVUE UCT creates packet headers as needed, encapsulates in a tunnel, and forwards to GigaVUE V Series in the deep observability pipeline. Gigamon further optimizes, transforms, and delivers data to tools, without need for further decryption



5.

### Pre-encryption Technology on Multi-Node

1. When any application needs to encrypt a message, it uses an encryption library, such as OpenSSL, to perform the actual encryption.
2. GigaVUE Universal Cloud Tap (UCT), enabled with Pre-encryption, gets a copy of this message before it's encrypted on the network.
3. Optionally, GigaVUE UCT enabled with Pre-encryption can also acquire a copy of the message from the server end, after the decryption.
4. GigaVUE UCT creates packet headers as needed, encapsulates in a tunnel, and forwards to V Series in the deep observability pipeline where it is further enriched, transformed, and delivered to tools, without further decryption.



### Supported Platforms

**VM environments:** Precryption™ is supported on the following VM platforms where UCT-V is supported:

| Platform Type        | Platform                                                                                                                                                                               |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Public Cloud</b>  | <ul style="list-style-type: none"> <li>• AWS</li> <li>• Azure</li> <li>• GCP (via Third Party Orchestration)</li> </ul>                                                                |
| <b>Private Cloud</b> | <ul style="list-style-type: none"> <li>• OpenStack</li> <li>• VMware ESXi (via Third Party Orchestration only)</li> <li>• VMware NSX-T (via Third Party Orchestration only)</li> </ul> |

**Container environments:** Precryption™ is supported on the following container platforms where UCT-C is supported:

| Platform Type | Platform                                                                                        |
|---------------|-------------------------------------------------------------------------------------------------|
| Public Cloud  | <ul style="list-style-type: none"> <li>EKS</li> <li>AKS</li> </ul>                              |
| Private Cloud | <ul style="list-style-type: none"> <li>OpenShift</li> <li>Native Kubernetes (VMware)</li> </ul> |

## Prerequisites

### Deployment Prerequisites

- OpenSSL version 1.0.2, version 1.1.0, version 1.1.1, and version 3.x
- For GigaVUE-FM, to capture the statistics, you must add the port 5671 in the security group
- Port 9900 should be enabled in security group settings on the UCT-V controller to receive the statistics information from UCT-V agent
- For UCT-C, you must add the port 42042 and port 5671 in the security group

### License Prerequisite

- Precription™ requires SecureVUE Plus license.

### Supported Kernel Version

Precription is supported for Kernel Version 5.4 and above for all Linux and Ubuntu Operating Systems. For the Kernel versions below 5.4, refer to the following table:

| Kernel Version               | Operating System              |
|------------------------------|-------------------------------|
| 4.18.0-193.el8.x86_64        | RHEL release 8.2 (Ootpa)      |
| 4.18.0-240.el8.x86_64        | RHEL release 8.3 (Ootpa)      |
| 4.18.0-305.76.1.el8_4.x86_64 | RHEL release 8.4 (Ootpa)      |
| 4.18.0-348.12.2.el8_5.x86_64 | RHEL release 8.5 (Ootpa)      |
| 4.18.0-372.9.1.el8.x86_64    | RHEL release 8.6 (Ootpa)      |
| 4.18.0-423.el8.x86_64        | RHEL release 8.7 Beta (Ootpa) |
| 4.18.0-477.15.1.el8_8.x86_64 | RHEL release 8.8 (Ootpa)      |
| 5.3.0-1024-kvm               | ubuntu19.10                   |
| 4.18.0-305.3.1               | Rocky Linux 8.4               |
| 4.18.0-348                   | Rocky Linux 8.5               |
| 4.18.0-372.9.1               | Rocky Linux 8.6               |
| 4.18.0-425.10.1              | Rocky Linux 8.7               |
| 4.18.0-477.10.1              | Rocky Linux 8.8               |

| Kernel Version              | Operating System |
|-----------------------------|------------------|
| 4.18.0-80.el8.x86_64        | centos 8.2       |
| 4.18.0-240.1.1.el8_3.x86_64 | centos 8.3       |
| 4.18.0-305.3.1.el8_4.x86_64 | centos 8.4       |
| 4.18.0-408.el8.x86_64       | centos 8.5       |

### Note

- See the [Configure Precryption in UCT-V](#) section for details on how to enable Precryption™ in VM environments.
- See the [Configure Precryption in UCT-C](#) section for details on how to enable Precryption™ in container environments.
- See how [Secure Tunnels](#) feature can enable secure delivery of precrypted data.

## Configure Precryption in UCT-C

GigaVUE-FM allows you to enable or disable the Precryption feature.

### Rules and Notes

The following are the memory limits to be applied to UCT-C:

- The memory limit changes depending on the numbers of vCPUs in the worker node. For example, if the worker node has 16 vCPUs, then the Precryption feature consumes around 1GB of memory (16 \* 64 MB).
- When you deploy secure tunnels, it requires additional (16 \*64 MB) memory. Hence, a total memory that you must allocate for the TAP is 1 GB.
- Protocol version IPv4 and IPv6 are supported.
- If you wish to use IPv6 tunnels, your GigaVUE-FM and the fabric components version must be 6.6.00 or above.

The YAML configuration option allows you to choose the amount of buffer size.

To configure the Precryption feature in UCT-C, follow these steps:

1. Go to **Traffic > CONTAINER > Universal Cloud Tap - Container**. The Policies page appears.
2. In the Policies page, click **Create**.
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. The name must be unique.                                                                                                                                                                 |
| Monitoring Domain  | Select an existing Monitoring Domain.<br><br>To create a new monitoring domain, refer to Create Monitoring Domain section in the UCT configuration guide.<br><br>Only one Precryption Policy is allowed per Monitoring Domain |
| Connections        | Select one or more connections for the policy. Once traffic policy is created for a Monitoring Domain, you cannot add or delete connections in the Monitoring Domain.                                                         |
| Precryption Policy | Click the radio button <b>Yes</b> , to enable the <b>Precryption Policy</b> ,                                                                                                                                                 |

After enabling the Precryption, configure the **Source Selectors**, and the **Rules**. In this release, for Rules, Pass All option is supported.

## Secure Tunnels

Secure Tunnel securely transfers the cloud captured packets on UCT-V and UCT-C to a GigaVUE V Series Node or Tool (only in case of UCT-C). The data from UCT-V and UCT-C are encapsulated in PCAPng format, and the encrypted data is sent over a TLS connection to a GigaVUE V Series Node.

Secure Tunnel can also transfer the cloud captured packets from a GigaVUE V Series Node to another GigaVUE V Series Node.

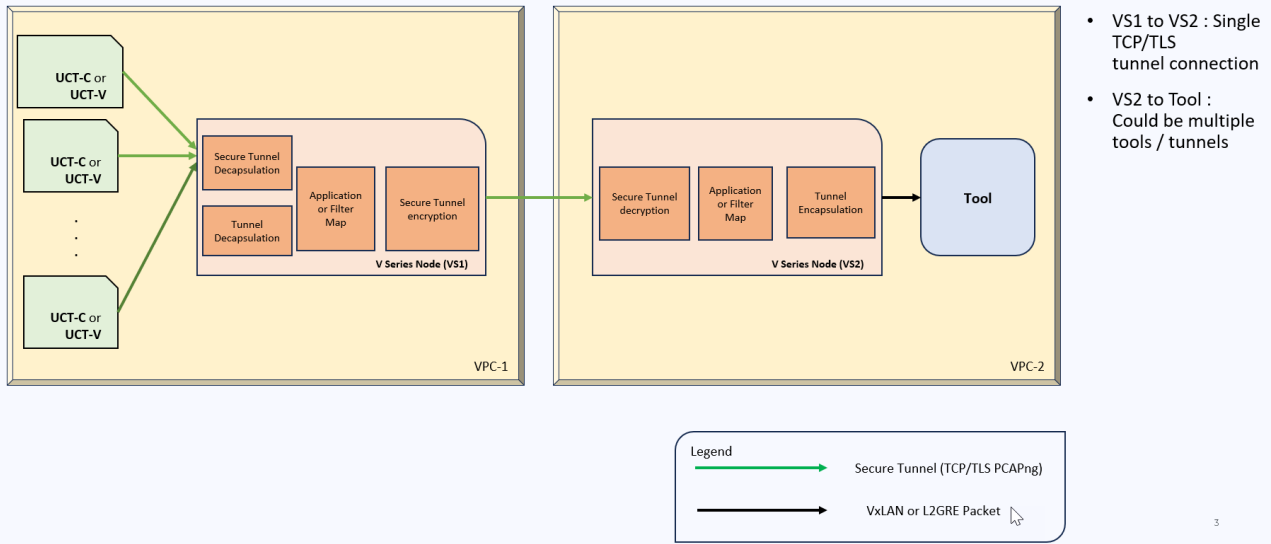
In case of GigaVUE V Series Node to GigaVUE V Series node, the traffic from the GigaVUE V Series Node 1 is encapped using PCAPng format and transported to GigaVUE V Series Node 2 where the traffic is decapped. The secure tunnels between V Series Node to V Series Node have multiple uses cases.

The GigaVUE V Series Node decapsulates and processes the packet per the configuration. The decapsulated packet can be sent to the application such as De-duplication, Application Intelligence, Load balancer and to the tool. The Load Balancer on this node can send the packets to multiple V series Nodes, in this case the packets can be encapsulated again and sent over a secure tunnel.



## Secure Tunnel Use Case

Tool in remote Virtual Private Cloud (VPC) – Single V Series Node



## Supported Platforms

Secure tunnel is supported on:

- OpenStack
- Azure
- AWS
- VMware NSX-T (only for Third Party Orchestration)
- VMware ESXi (only for Third Party Orchestration)
- Nutanix (only for Third Party Orchestration)
- Google Cloud Platform (only for Third Party Orchestration)

For information about how to configure secure tunnels, refer to the section [Configure Secure Tunnel](#).

## Configure Secure Tunnel

Secure tunnel can be configured on:

- [Preencrypted Traffic](#)
- [Mirrored Traffic](#)

### Preencrypted Traffic

You can send the preencrypted traffic through secure tunnel. When secure tunnel for Preencryption is enabled, packets are framed and sent to the TLS socket. PCAPng format is used to send the packet.

When you enable the secure tunnel option for both regular and Precryption packets, then two TLS secure tunnel sessions are created.

It is recommended to always enable secure tunnels for precrypted traffic to securely transfer the sensitive information.

For more information about PCAPng, refer to [PCAPng Application](#).

### **Mirrored Traffic**

You can enable the Secure Tunnel for mirrored traffic. By default, Secure Tunnel is disabled.

### **Prerequisites**

While creating Secure Tunnel, you must provide the following details:

- SSH key pair
- CA certificate

### **Notes**

- Protocol version IPv4 and IPv6 are supported.
- If you wish to use IPv6 tunnels, your GigaVUE-FM and the fabric components version must be 6.6.00 or above.

### **Configure Secure Tunnel from UCT Container to GigaVUE V Series Node**

To configure a secure tunnel in a UCT Container, you must configure one end of the tunnel to the UCT and the other end to a GigaVUE V Series node. You must configure CA certificates in UCT Container, and the private keys and SSL certificates in the GigaVUE V Series node. Refer to the following steps for configuration:

| S. No       | Task                                                                                                                  | Refer to                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |        |       |                       |             |                                                   |
|-------------|-----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|-------|-----------------------|-------------|---------------------------------------------------|
| 1           | Upload a Custom Certificate                                                                                           | <p>You must upload a CA to UCT Container for establishing a connection with the GigaVUE Cloud Suite V Series node.</p> <p>To upload the CA using GigaVUE-FM follow the steps given below:</p> <ol style="list-style-type: none"> <li>Go to <b>Inventory &gt; Resources &gt; Security &gt; CA List</b>.</li> <li>Click <b>New</b>, to add a new Certificate Authority. The <b>Add Certificate Authority</b> page appears.</li> <li>Enter or select the following information. <table border="1" data-bbox="737 554 1446 749"> <thead> <tr> <th>Field</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Alias</td> <td>Alias name of the CA.</td> </tr> <tr> <td>File Upload</td> <td>Choose the certificate from the desired location.</td> </tr> </tbody> </table> </li> <li>Click <b>Save</b>.</li> </ol> <p>For more information, refer to the section <a href="#">Adding Certificate Authority</a></p> | Field | Action | Alias | Alias name of the CA. | File Upload | Choose the certificate from the desired location. |
| Field       | Action                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |        |       |                       |             |                                                   |
| Alias       | Alias name of the CA.                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |        |       |                       |             |                                                   |
| File Upload | Choose the certificate from the desired location.                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |        |       |                       |             |                                                   |
| 2.          | Upload a SSL Key                                                                                                      | You must add a SSL key to GigaVUE Cloud Suite V Series node. To add SSL Key, follow the steps in the section <a href="#">SSL Decrypt..</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |       |                       |             |                                                   |
| 3           | Selecting the SSL Key when you create a monitoring domain and configure the fabric components in GigaVUE-FM.          | To select the SSL Key follow the steps in the section                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |        |       |                       |             |                                                   |
| 4           | Selecting the CA certificate when you create a monitoring domain and configuring the fabric components in GigaVUE-FM. | You should select the added Certificate Authority (CA) in UCT-V Controller. To select the CA certificate, follow the steps in the section <a href="#">UCT-C and GigaVUE-FM Interaction</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |        |       |                       |             |                                                   |
| 5.          | Creating and adding the secure tunnel when you configure the traffic policy.                                          | To create and add the secure tunnel while configuring in , in UCT Container refer to the <a href="#">Configure Traffic Policy</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |        |       |                       |             |                                                   |

## Adding Certificate Authority

This section describes how to add Certificate Authority in GigaVUE-FM.

### CA List

The Certificate Authority (CA) List page allows you to add the root CA for the devices.

To upload the CA using GigaVUE-FM follow the steps given below:

1. Go to **Inventory > Resources > Security > CA List**.
2. Click **Add**, to add a new Custom Authority. The **Add Certificate Authority** page appears.
3. Enter or select the following information.

| Field       | Action                                            |
|-------------|---------------------------------------------------|
| Alias       | Alias name of the CA.                             |
| File Upload | Choose the certificate from the desired location. |

4. Click **Save**.

## Configure UCT-C Settings

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

- [UCT-C General Settings](#)
- [Configure UCT-C Settings](#)

### UCT-C General Settings

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

**NOTE:** GigaVUE-FM generates an alarm for the disconnected UCT-C When three consecutive heartbeats are missed. Refer to "Alarms" topic in the *GigaVUE Administration Guide* for detailed information on Alarms.

To edit the UCT-C general settings:

1. In GigaVUE-FM, navigate to **Inventory > CONTAINER > Universal Cloud Tap - Container > Settings**, the **Settings** page appears with the existing General settings and UCT-C information.
2. On the **Settings** page, on the **General** section, click **Edit**. The Edit General Setting's quick view appears.
3. To exclude the pods from monitoring, provide the source criteria. In **Criteria 1**, from the drop-down list box, select any of the following **Object Property** to exclude them from the monitoring domain, and provide the value for the property selected in the **Value** field:
  - o pod name
  - o pod ip

- o pod labels
- o node name
- o namespace

**NOTE:** By default pods in kube-system namespace, metallb-system namespace and pod name containing nginx are excluded from monitoring.

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

| Field                                                     | Description                                                                   |
|-----------------------------------------------------------|-------------------------------------------------------------------------------|
| <b>Maximum number of connections allowed</b>              | Enter the maximum number of connections allowed in the UCT-C solution         |
| <b>Purge time interval for disconnected UCT-Cs (days)</b> | Enter a value for the purge time interval for the disconnected UCT-Cs in days |

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

### UCT-C Log Level Settings

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

To view or edit the UCT-C log level settings:

1. In GigaVUE-FM, navigate to **Inventory > CONTAINER > Universal Cloud Tap - Container > Settings**, the **Settings** page appears with the existing General settings and UCT-C information.
2. On the **Settings** page, on the **UCT-C** section, on any monitoring domain, click on the UCT-C fabric. The UCT-C setting's quick view appears.

The screenshot shows a configuration window for a UCT. At the top, there is a title bar with 'X UCT: [ID]' and 'Cancel' and 'Save' buttons. Below the title bar, there is a section titled 'Individual Settings'. A blue informational box states: 'Individual setting will apply to this UCT only. When applying settings to a group try to consider the performance impact.' Under the 'LOGGING' section, there are two settings: 'Log Level' is set to 'DEBUG' with a dropdown arrow and a 'Reset' button; 'Log File Size' is set to '1000000' with a 'Reset' button.

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

| Field                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Level</b>     | Select one of the following: <ul style="list-style-type: none"> <li>• <b>DEBUG</b>—fine-grained log information for application debugging</li> <li>• <b>INFO</b>—coarse-grained log information for highlighting application progress</li> <li>• <b>WARN</b>—log information of potentially harmful situations</li> <li>• <b>ERROR</b>—log information of the error events that allows the application to run continuously</li> <li>• <b>FATAL</b>—log information of very severe error events that presumably lead the application to abort.</li> </ul> |
| <b>Log File Size</b> | Enter a value for the number of lines in the UCT-C log file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

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

## Upgrade UCT-C

To upgrade UCT-C, you must perform the following steps:

1. **Upgrade to GigaVUE-FM 6.6.00:** Before upgrading GigaVUE-FM from versions earlier than 6.4.00.03, delete the UCT-C Monitoring Domain, Policy, UCT-C Controller and UCT-C Tap, and then upgrade GigaVUE-FM to 6.6.00. To upgrade the GigaVUE-FM in respective cloud platforms, refer to [GigaVUE-FM Installation and Upgrade guide](#).
2. **Upgrade to UCT-C 6.6.00:** To upgrade UCT-C to 6.6.00, you must delete the older versions and deploy UCT-C 6.6.00 version. To deploy UCT-C, refer to [Steps to Delete and Redeploy UCT-C](#). GigaVUE-FM 6.6.00 is compatible only with UCT-C 6.6.00.

## Steps to Delete and Redeploy UCT-C

1. Delete the UCT Controller deployment.

```
kubectl get deployment -A
kubectl delete deployment <uct-controller name> -n <namespace>
```

2. Delete the UCT Tap daemonset.

```
kubectl get daemonset -A
kubectl delete daemonset <uct-tap-name> -n <namespace>
```

3. Delete the UCT controller service.

```
kubectl get services -A
kubectl delete services <uct-cntlr-service-name> -n <namespace>
```

4. Deploy the UCT controller/UCT Tap using helm chart or YAML file.

- a. To install using Helm chart:

```
helm install uctc-cntlr uctc-cntlr/
helm install uctc-tap uctc-tap/
```

- b. To install using YAML.

```
kubectl apply -f <uctc_controller_yaml_file>
kubectl apply -f <uctc_tap_yaml_file>
```

5. Delete the ingress rule and redeploy it using YAML to point to the right service (uctc-cntlr-service).

```
kubectl get ingress -A
kubectl delete ingress <uct-cntlr-ingress-name> -n <namespace>
uctc-ingress.yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
 annotations:
 kubernetes.io/ingress.class: nginx-uct-ns
 nginx.ingress.kubernetes.io/backend-protocol: HTTPS
 nginx.ingress.kubernetes.io/proxy-connect-timeout: "360000"
 nginx.ingress.kubernetes.io/proxy-read-timeout: "360000"
 nginx.ingress.kubernetes.io/proxy-send-timeout: "360000"
 nginx.ingress.kubernetes.io/rewrite-target: /
 nginx.ingress.kubernetes.io/secure-backends: "false"
 nginx.ingress.kubernetes.io/ssl-passthrough: "true"
 generation: 1
 name: uctc-cntlr-ingress
 namespace: uct-ns
spec:
 rules:
 - http:
 paths:
 - backend:
 service:
 name: uctc-cntlr-service
 port:
 number: 8443
 path: /
 pathType: ImplementationSpecific
 status:
 loadBalancer: {}
 kubectl apply -f <ingress_rule_yaml_file>
```

6. Restart the nginx controller and backend.

```
kubectl get pods -A
kubectl rollout restart deployment nginx-controller -n <namespace>
kubectl rollout restart deployment nginx-ingress-default-backend -n
<namespace>
```

7. Redeploy the policy.

## Debuggability and Troubleshooting

- For analyzing the issues, log into the UCT-C controller /UCT-C tap pod using the following command and verify the logs present pod-data folder.

```
kubectl -it exec <<pod name>> -n <<namespace>> --bash
```



- 503 Service Temporarily Unavailable-** When UCT tap or inventories are not discovered during Monitoring Domain deployment, verify whether **503 Service Temporarily Unavailable (refer the log messages below)** error messages are observed in vmm.log of FM. If the error messages are available, check and update the UCT controller service name or port number (as shown in the **nginx.yaml**) used in ingress resource.

```

nginx.yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
annotations:
 kubernetes.io/ingress.allow-http: "false"
 kubernetes.io/ingress.class: nginx-uct
 nginx.ingress.kubernetes.io/backend-protocol: HTTPS
 nginx.ingress.kubernetes.io/configuration-snippet: proxy_set_header
Authorization
 $http_authorization;
 nginx.ingress.kubernetes.io/rewrite-target: /
 nginx.ingress.kubernetes.io/secure-backends: "true"
 nginx.ingress.kubernetes.io/ssl-passthrough: "true"
name: uct-cntlr-ingress
namespace: uct
spec:
 rules:
 - http:
 paths:
 - backend:
 service:
 name: gigamon-uctc-cntlr-service
 port:
 number: 8443
path: /
pathType: ImplementationSpecific

```

#### Log-Snippet

```

2023-07-26 09:05:12,866 ERROR [kubernetesInventory-7]
UctRestClientImplV13 - collectInventory : getURL :
https://10.115.83.95:8443/api/v1.3/inventory/nodes :
HttpStatusCodeException : 503 Service Temporarily Unavailable:
"<html><EOL><EOL><head><title>503 Service Temporarily
Unavailable</title></head><EOL><EOL><body><EOL><EOL><center><h1>503
Service Temporarily
Unavailable</h1></center><EOL><EOL><hr><center>nginx</center><EOL><EOL><
/body><EOL><EOL></html><EOL><EOL>"
2023-07-26 09:05:12,866 ERROR [Thread-8935] UctRestClientImplV13 -
updateUctControllerSettings : HttpStatusCodeException : 503 Service
Temporarily Unavailable: "<html><EOL><EOL><head><title>503 Service
Temporarily
Unavailable</title></head><EOL><EOL><body><EOL><EOL><center><h1>503
Service Temporarily
Unavailable</h1></center><EOL><EOL><hr><center>nginx</center><EOL><EOL><
/body><EOL><EOL></html><EOL><EOL>"
2023-07-26 09:05:12,866 INFO [Thread-8935]
UctKubernetesInvMonitorServiceImpl - updateUctControllerSettings REST API

```

```
call: Status code : 503 SERVICE_UNAVAILABLE
2023-07-26 09:05:12,866 INFO [kubernetesInventory-7]
UctRestClientImplV13 - collectInventory : controllerIP : 10.115.83.95
controllerPort : 8443
2023-07-26 09:05:12,866 ERROR [Thread-8935]
UctKubernetesInvMonitorServiceImpl - updateUctControllerSettings REST API
call failed: Connection ID b067e0dc-272f-4f45-afea-c676ae89fa37 : Uct
controller 73d5c0cf-ffc2-4688-8e1c-17f2cb7d0ad4 Status code : 503
SERVICE_UNAVAILABLE Response <html>
<head><title>503 Service Temporarily Unavailable</title></head>
<body>
<center><h1>503 Service Temporarily Unavailable</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

- UCT-C controller not discovered by GigaVUE-FM - When UCT-Ccontroller is not discovered by GigaVUE-FM, check the following:
  - Kubernetes cluster URL is updated properly in the yaml file
  - Mismatch in the Kubernetes cluster URL in Monitoring Domain
- UCT-C tap not discovered by GigaVUE-FM- When UCT-C tap is not discovered by GigaVUE-FM, verify whether the namespace in uctc-tap yaml file (as shown in the following uctc-tap.yaml) is same as that of UCT-C controller yaml file.

**uct-tap.yaml**

```
Value need to match me tadata used for gcb-cntlr
value: "<UCT-CNTRLR-SVC-NAME.UCT-CNTRLR-NAMESPACE>.svc.cluster.local"
- name: UCTC_CNTRLR_SVC_DNS
value: gigamon-uctc-cntlr-service.<<namespace>>.svc.cluster.local ==>
This should be same as that of the namespace in which uctc-controller is
deployed.
```

- **Modify External Load Balancer IP of UCT-C Controller:** You need to update the External Load Balancer IP in Controller YAML or HELM chart, and redeploy UCT-C Controller.
- UCT-C controller should be started as "root"/admin/privileged user if it is using port less than 1024. This is a requirement of Linux/OS and not of Gigamon.

# 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 6.6 Hardware and Software Guides
<p><b>DID YOU KNOW?</b> 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 <b>Edit &gt; Advanced Search</b> from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.</p>
<p><b>Hardware</b></p> <p>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</p>
<b>GigaVUE-HC1 Hardware Installation Guide</b>
<b>GigaVUE-HC3 Hardware Installation Guide</b>
<b>GigaVUE-HC1-Plus Hardware Installation Guide</b>
<b>GigaVUE-HCT Hardware Installation Guide</b>
<b>GigaVUE-TA25 Hardware Installation Guide</b>
<b>GigaVUE-TA25E Hardware Installation Guide</b>

<b>GigaVUE Cloud Suite 6.6 Hardware and Software Guides</b>	
<b>GigaVUE-TA100 Hardware Installation Guide</b>	
<b>GigaVUE-TA200 Hardware Installation Guide</b>	
<b>GigaVUE-TA200E Hardware Installation Guide</b>	
<b>GigaVUE-TA400 Hardware Installation Guide</b>	
<b>GigaVUE-OS Installation Guide for DELL S4112F-ON</b>	
<b>G-TAP A Series 2 Installation Guide</b>	
<b>GigaVUE M Series Hardware Installation Guide</b>	
<b>GigaVUE-FM Hardware Appliances Guide</b>	
<b>Software Installation and Upgrade Guides</b>	
<b>GigaVUE-FM Installation, Migration, and Upgrade Guide</b>	
<b>GigaVUE-OS Upgrade Guide</b>	
<b>GigaVUE V Series Migration Guide</b>	
<b>Fabric Management and Administration Guides</b>	
<b>GigaVUE Administration Guide</b>	covers both GigaVUE-OS and GigaVUE-FM
<b>GigaVUE Fabric Management Guide</b>	how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
<b>Cloud Guides</b>	
how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms	
<b>GigaVUE V Series Applications Guide</b>	
<b>GigaVUE V Series Quick Start Guide</b>	
<b>GigaVUE Cloud Suite Deployment Guide - AWS</b>	
<b>GigaVUE Cloud Suite Deployment Guide - Azure</b>	
<b>GigaVUE Cloud Suite Deployment Guide - OpenStack</b>	
<b>GigaVUE Cloud Suite Deployment Guide - Nutanix</b>	
<b>GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)</b>	
<b>GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)</b>	
<b>GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration</b>	

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

## How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

## Documentation Feedback


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

<b>For Online Topics</b>	<b>Online doc link</b>	<i>(URL for where the issue is)</i>
	<b>Topic Heading</b>	<i>(if it's a long topic, please provide the heading of the section where the issue is)</i>
<b>For PDF Topics</b>	<b>Document Title</b>	<i>(shown on the cover page or in page header )</i>
	<b>Product Version</b>	<i>(shown on the cover page)</i>
	<b>Document Version</b>	<i>(shown on the cover page)</i>
	<b>Chapter Heading</b>	<i>(shown in footer)</i>
	<b>PDF page #</b>	<i>(shown in footer)</i>
<b>How can we improve?</b>	<b>Describe the issue</b>	<i>Describe the error or issue in the documentation. (If it helps, attach an image to show the issue.)</i>
	<b>How can we improve the content?</b> <b>Be as specific as possible.</b>	
	<b>Any other comments?</b>	

## 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](mailto:support@gigamon.com).

## Contact Sales

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

**Telephone:** +1.408.831.4025

**Sales:** [inside.sales@gigamon.com](mailto:inside.sales@gigamon.com)

**Partners:** [www.gigamon.com/partners.html](http://www.gigamon.com/partners.html)

## Premium Support

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

## The VÜE Community

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

Visit the VÜE Community site to:

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

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

**Register today at** [community.gigamon.com](http://community.gigamon.com)

**Questions?** Contact our Community team at [community@gigamon.com](mailto: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)