

# GigaVUE-FM/Venafi Trust Protection Platform Integration Guide

## GigaVUE-FM 5.9

Documentation Version: 1.0 Documentation Date: September 4, 2020

#### COPYRIGHT

Copyright © 2020 Gigamon. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without Gigamon's written permission.

#### TRADEMARK ATTRIBUTIONS

Copyright © 2020 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at http://www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners

## How to Deploy Bulk Certificate Provisioning from Venafi TPP to GigaVUE-FM

This document provides instructions to configure Bulk Certificate Provisioning from Venafi Trust Protection Platform (TPP) to GigaVUE-FM (FM).

#### CONTENTS:

- Overview
- GigaVUE-FM Setup
- Venafi TPP Setup

### **Overview**

As part of deploying and maintaining a GigaVUE-OS TLS/SSL decryption solution, you may want to perform bulk certificate provisioning from an external platform. The integration between Venafi TPP and GigaVUE-FM makes this possible.

While known as certificate provisioning, the digital certificate and associated private key must both be provisioned as part of the operation. Certificate/key pairs are stored in the Key Store on GigaVUE nodes, where the decryption processing occurs.

Provisioning does not occur directly between Venafi TPP and the GigaVUE node. The GigaVUE-FM API serves as the interface point for external systems to indirectly provision a GigaVUE node. For any GigaVUE node to receive provisioning data, it must be managed by the GigaVUE-FM instance where the API resides.

An HTTPS connection is required from Venafi TPP to the FM API. Each provisioning operation includes a parameter that identifies the specific GigaVUE node to receive the provisioning data.

## **GigaVUE-FM Setup**

Each GigaVUE node includes a protected Key Store. Prior to adding certificate/key pairs, the key store must be unlocked by entering the Keychain Password.

Adding a certificate/key pair to the Key Store does not enable decryption by default. The certificate/key pair must be associated with a decryption profile to enable decryption of traffic for the server associated with the key pair. To enable this behavior, set the **Auto Enable New Certificate** global option to "true."

When provisioning an updated certificate/key pair to replace an existing pair, you may want to automatically delete existing certificate/key pairs for the same entity. To control this behavior, set the **Auto Delete Certificates with Same Entity** global option to "true."

While not tied directly to provision, the **Auto Delete Expired Certificates** global option should also be considered at this time.

For each GigaVUE HC Series appliance to be provisioned:

- 1. Unlock the Key Store
- 2. Set the Auto Enable New Certificates parameter to "true"
- 3. Set the Auto Delete Certificates with Same Entity parameter to "true"
- 4. Set the Auto Delete Expired Certificates parameter to "true"

## Venafi TPP Setup

**NOTE**: The majority of TPP configuration occurs via the Web Admin user interface, while the Bulk Provisioning jobs are configured via the Aperture user interface.

In some scenarios, the same set of certificates may be provisioned to multiple GigaVUE HC Series. In other cases, different sets of certificates may be provisioned to different GigaVUE HC Series appliances. It is important to identify the certificate-to-appliance mapping prior to provisioning.

#### STEPS:

- Before you begin
- Step 1: Install the Gigamon driver
- Step 2: Set up the Gigamon policy hierarchy
- Step 3: Set up the device object for GigaVUE-FM API
- **Step 4**: Set up a policy object for provisioning jobs.
- Step 5: Create certificates to provision (Skip if preexisting)
- **Step 6**: Set up a bulk provisioning job
- Step 7: Verify that certificates have been pushed to the desired device

#### Before you begin

Gather the information needed to complete the Venafi TPP set up.

- GigaVUE-FM hostname/network address and port number
- GigaVUE-FM logon credentials
- List of GigaVUE Node/Cluster Names to be provisioned
- Mapping of certificates-to-GigaVUE nodes/clusters

#### Step 1: Install the Gigamon driver

1. Download and obtain Gigamon Driver from the Venafi Marketplace (marketplace.venafi.com).



2. Place the driver in the Scripts/AdaptableBulk folder on the TPP server. C:/ProgramFiles/Venafi/Scripts/AdaptableBulk

📙   🛃 🔜 🖛   Ad	aptableBulk	c .		
File Home	Share	View		
← → • ↑ 🚺	> This PC	$\Rightarrow$ SYS (C:) $\Rightarrow$ Program Files $\Rightarrow$ Venafi $\Rightarrow$	Scripts > AdaptableBu	lk
✓ Quick access Desktop ↓ Downloads ☑ Documents ☑ Pictures	N * *	lame A Samples 2 GigamonGigaVUE-FM	Date modified 7/3/2020 3:40 PM 10/21/2019 3:03 PM	Type File folder PS1 File

#### Step 2: Set up the Gigamon policy hierarchy

**NOTE**: TPP supports a flexible policy hierarchy and will likely differ from one environment to the next. This guide section provides the following sample hierarchy:

- Policy
  - o TLS
    - Certificates
      - Gigamon
        - Device (GigaVUE-FM)
        - Gigamon Credential
- 1. Log in to Venafi TPP Web Admin Console.
- 2. Set up a new policy under the appropriate TLS Certificate section based on the environment.
- 3. In the left navigation, navigate to Policy > TLS > Certificates.
- 4. Right-click on Certificates and select Add > Policy.



5. Name the policy "Gigamon" for ease of reference and click Save.

Policy V	Add New : Policy
🕂 Add 🔹 🗙 Delete Show all 🔹 🗳	
20 5	
Search options	General
Policy	Policy Name: Gigamon
<ul> <li></li></ul>	Description: Contact(s): Gigamon-HC1-001
Certificates	
B 22 Venan Operational Certificates B I GigaVUE-FM-API C Aperture Configuration	Log Server: \Logging\tpp Log Server

After creating the policy, it will appear in the Venafi left navigation under Policy > TLS > Certificates.

Policy 🗸	Gigamon : Certificate							
💠 Add 🔹 💥 Delete Show all 🔹 🗳	Applications Certificate Trust Store Cloud Instance Monitoring	Devices	Network Device Enrollin	nent Settings				
20 🔓	Policy Certificate Certificate Authorities 📲 Cert	ificate Trust Bun	dle 🏾 🎢 Credentials					
Search options								
Policy     Code Signing	General Information							
	Contact(s):	nin (\VED\Identity\tpj	ED\Identity\tppadmin)					
Administration	Approver(s): local:tppadmin (\VED\Identity\tppadmin) Management Type: Monitoring							
Gigamon B J Discovered	Managed By:							
	CSR Handling							
GigaVUE-FM-API     GigaVUE-	CSR Generation:	Service Ger User Provid	nerated CSR ed CSR					
	Generate Key/CSR on Application:	No		~				
	Hash Algorithm:	SHA-256						

#### Step 3: Set up the device object for GigaVUE-FM API

1. To set up the device, select the Gigamon policy folder you just created and select **Add > Devices > Device**.

Policy	~		Gigamon : Po	olicy							
💠 Add 🔹 🗙	Delete Show all -	\$	Applications	Certificate Tr	rust Store	Cloud Instance	Monitoring	Devices	Network Device En	rollment Se	ettings
	80	3 😹	Policy	Certificate	Certifi	icate Authorities	- Certifica	ate Trust Bun	dle R Credentials	2 Encryp	ption
Search options											
Policy Decode S Decode S Decode S Decode S SSH Decode SSH Decode SSH D	igning inistration allations ificates Open	7	General					Description: Contact(s):	localitppadmin		
E Apertur	+ Add		Certificates	Þ							
	Permissions	0	Devices	Þ	Device	•	L	.og Server:	\Logging\tpp Log	Server	
	Refresh		CA Template Policy	•	Jump S	Server					
	Collapse All	28	Credential	•				Engines:			

- 2. For the **Device Name**, specify a meaningful name for the GigaVUE node.
- 3. For the IP address, enter the GigaVUE-FM IP address.

Policy V	Add New : Device	
+ Add - 🗙 Delete Show all -		
Search options	General	
B Policy	.* Device Name: GigaVUE-FM	
Code Signing	Description:	
Administration	Contact(s): local:tppadmin (\VED\Identity\tppadmin)	
Certificates	Host Information	
Gigamon	Hostname/Address: 54.212.106.119	
	Provisioning Mode: Agentless	
Venafi Operational Certificates	Concurrent Connection Limit: 1	

- 4. Click **Save** when done.
- 5. To add the device credentials, right-click on the device and select **Add > Credentials > Username Credential**.

Policy V		igaVUE-FM : Settings		
💠 Add 👻 🗙 Delete	Show all 🔹 🗳	Device General Support		
	20 📓	Settings		
Search options				
Policy		General		
I Son			Description:	
Administration			Contact(s):	local:tppadmin (\VED\Identity\tppadmin)
Certificates		Host Information		
GigaVU GigaVU GigaVU GigaVU GigaVU SCEP	<ul> <li>Open</li> <li>Open in New Window</li> </ul>		Hostname/Address: Provisioning Mode:	54.212.106.119 Agentiess
Venafi Operationa Aperture Configur	💠 Add	Certificates	Concurrent Connection Limit:	1
	Permissions	Application	Device Credential:	
	🗇 Refresh	Trust Store	Temp Directory:	
	Expand All	R Credential	🔏 Amazon Credential OS Type:	Automatic
	Collapse All	Certificate Trust Bundle	2 Certificate Credential Jump Server:	
	I Rename		2 Generic Credential Use Sudo:	No <b>v</b>
	Move Move		Sudo Credential (optional):	
	X Delete		Enforce Host Key:	No
) í	•		Username Credential Presented Thumbprint: Presented Key Type:	

NOTE: In this example, the device is named "GigaVUE-FM."

6. Add GigaVUE-FM admin credentials used to login to GigaVUE-FM GUI anc click Save.

Add • X Delete Show all • 4							
PO General General							
earch options							
See Policy	Credential Name:	Gigamon Credential					
B Code Signing	Description:						
arge gash arge gash	Contact(s):		*				
GigaVUE-FM							
Geptime Configuration							
Credential	Credential						
	.* User Name:	admin					
	. <u>.</u> Password:						
	* Confirm Password:	•••••					

- 7. To assign these credentials to the device, click on the device (named "GigaVUE-FM" in this example) to view the device settings.
- 8. In the device settings, under Most Information, click the Credential Selector icon.
- 9. Select "Gigamon Credential" and click **Save** to set the credentials.

	GigaVUE-							
Add • 🗙 Delete Show all •	Device	General Support						
20	Setting	35						
Search options	-							
Policy								
E Code Signing	General	General						
		Description:						
Administration		Contact(s): [local:tppadmin (\VED\Identity\tppadmin)						
Gigamon	Host Inf	ormation						
Gigamon Credential		Hostname/Address: 54.212.106.119						
B Discovered		Provisioning Mode:	Agentiess	~				
Gerational Certificates		Credential Selector		_				
Aperture Configuration			🌄 Policy Tree 👻 💋					
			20 .					
		Search options		~				
		B Policy						
		B TLS		~				
		Administration						
	115-12-11-1	E Certificates						
		Gigamon		· · ·				
		GigavuE-FM	a					

#### Step 4: Set up a policy object for provisioning jobs.

All bulk provisioning jobs require a Jobs policy object (folder). This step may be skipped if an existing Jobs object will be used for the GigaVUE provisioning. Otherwise, create the Jobs object in the desired policy tree location.

1. In the Venafi Policy interface, right-click on TLS and select **Add > Policy**.

VE	NAFE & v	WebAdmin Dashboard	is ~ Inventory ~ Jobs Clients ~ Reports ~ Configuration ~
Policy	~	app1.venafidem	o.com (Server Certificate) : Summary
🔶 Add 🔸	- X Delete Show	all - 🗳 Certificate Mo	unitoring Validation General Support
		PO 😹 🧕 🔊 Summary 🛔	Settings Associations Scompliance OHistory
Search op	otions	- 💽 💟 Restart   🌾 Retr	ry   🎡 Reset 🔹   🕏 Renew Now   🌷 Check Revocation   🖋 Validate Now   🤬 Revoke 🝷   🍓 Change Certificate Type
B Solo	icy Code Signing SSH	Certificate Statu	15
:	<ul> <li>Open</li> <li>Open in New Window</li> </ul>	Expiration Da	IK ato 22 12:14:38 PM
	💠 Add 🕨	Certificates	
	Permissions	i Devices	
	🗳 Refresh	CA Template	Kevocation check not yet attempted
	Expand All	Policy	
	Collapse All	Credential	
	I Rename	- Workflow	pons
H 🎝	Move	Aperture Configuration	Application Installation Status
	× Delete	AWS EC2 Instance Monitor     Certificate Trust Bundle	

2. Enter a name for the policy and click **Save**.

Policy 🗸	Add New : Policy		
🕂 Add 🔹 🗙 Delete Show all 🔹 🗳			
P 🕄 🍃	é		
Search options	General		
🖃 🌄 Policy		.* Policy Name:	Jobs
Code Signing		Description:	
		Contact(s):	local:tppadmin
🕀 疑 Administration			
Gertificates			
□ → Test Certs			
app2.venafidemo.com	Lee View		
a oigamon	Log view		
Gigarion		Log Server:	\Logging\tpp Log Server
A Gigamon Credential			

#### Step 5: Create certificates to provision (Skip if preexisting)

**NOTE**: This step can be skipped if you are planning to provision preexisting certificates to GigaVUE devices. However, when provisioning preexisting certificates, ensue that the certificate policy Management Type set to "Provisioning."

You can create a new policy or use an existing policy to create new certificates

1. To create a new policy, right-click on the certificate and select **Add > Policy**.

Policy	× 1		GigaVUE-FM : Settin	gs		
🕂 Add 👻 🗙	Delete Show all	*	Device General	Support		
Search options	10	- 82	Jettings			
Policy Code S	igning		General			
I SIN		- 1			Description:	
🗄 🌄 Adm 🕀 🌄 Insta	ninistration allations				Contact(s):	local:tppadmin (\VED\Identity\tppa
Cer	<ul><li>Open</li><li>Open in New Window</li></ul>		Host Information			
	🕂 Add 🕨	07	Certificates	•	Hostname/Address:	54.212.106.119
	Permissions	1	Devices	P	Provisioning Mode:	Agentless
🗄 冯 Venafi	A	1	CA Template		Concurrent Connection Limit:	1
C Apertu	Expand All	1	Policy	ή.	Device Credential:	\VED\Policy\TLS\Certificates\Gigamon\Gi
	E Collapse All	R	Credential	Þ	Temp Directory:	
		30	Workflow	•	OS Type:	Automatic
	1 Rename	0	Aperture Configuration		Jump Server:	
	Move	-	AWS EC2 Instance Monitor		Use Sudo:	No
	🗙 Delete	-	Certificate Trust Bundle		Sudo Credential (optional):	

2. Specify a meaningful name for the policy and click **Save**.

Policy V	_	<u>s</u>	Add New : Policy		
🕂 Add 👻 🗙 Delete	Show all -	\$			
	20	-	(		
Search options		•	General		
🕀 🌄 Policy				* Policy Name:	Test Certs
Code Signing				Description:	
TLS				Contact(s):	localitppadmin
Certificates					

3. To create new certificates under this policy, right-click on the policy and select Add > Certificates > Server Certificate.

Policy	~		-	Test Certs : Poli	cy					
🕂 🔸 Add 🗣	Delete	Show all •	\$	Applications	Certificate Tri	ust Store Cloud Instance I	Monitoring Devices 1	Network Device Enrollment	Settings View	General Support
		20	3	Policy 🔬	Certificate	Certificate Authorities	🕂 Certificate Trust Bundle	R Credentials REno	ryption 🛛 🔍 Monitorin	g 💽 Validation 🕹 Workflow
earch options										
Policy D Gode S D GSSH	Signing			General						
🖃 🍶 TLS			- 1						Description:	
	ninistratio allations tificates	n							Contact(s):	local:tppadmin
		Dpen Open in New Window Add	, ) (s	Certificates	Þ	Code Signing Certificate				
H	SC 4	Permissions	1	Devices	÷.	Device Certificate			Log Server:	\Logging\tpp Log Server
⊞ 🥪 SC ⊕ 纋 Venafi Oj Og Aperture	ture	I Cr Refresh C A Template I D Expand All Policy C A Template D Policy C A Template D Policy C A Template D Policy D Pol		Server Certificate     User Certificate						
		Conapse All Rename Move	-	Workflow Aperture Configura AWS EC2 Instance	ition				Engines:	
	×	Delete	4	Certificate Trust Bu	indle					

- 4. Specify the appropriate certificate parameters.
- 5. For Management Type, set it to "Provisioning."

Policy 🗸	Add New : Server Certificate				
💠 Add 🔹 🗶 Delete Show all 🔹 🗳	🔅 Renew Now   😭 Download + 😭 Import 😭 Retrieve Certific	ate			
20 5	C				
Search options	General Informatic				
🕒 🌄 Policy	Certificate Name:	app1.venafidemo.com			
B Gode Signing	Description:				
	Contact(s):	local:tppadmin (\VED\Identity\tppadmin)			
H GAdministration	Approver(s):	local:tppadmin (\VED\Identity\tppadmin)			
Les Certificates	Processing Disabled:	0			
Test Certs	Management Type:	Monitoring 🗸			
금 🥪 Gigamon 금 👹 GigaVUE-FM - & Gigamon Credential 표 疑 _Discovered	Managed By:	Unassigned Kontonya Enrollment Provisioning			
<ul> <li>⇒ SCEP</li> <li>⇒ Venafi Operational Certificates</li> <li>Aperture Configuration</li> </ul>	CSR Generation: Generate Key/CSR on Application:	Service Generated CSR     User Provided CSR     No     Vo			
	Hash Algorithm:	SHA-256			
	Subject DN				
	Common Name:	app1.venafidemo.com			

- 6. Click **Save** when done.
- 7. To activate certificates just created, click **Renew Now** after selecting the certificate.

Policy 🗸	2	app1.venafidemo.com (Server Certificate) : Summary
🖶 Add 👻 🗙 Delete S	Show all 🔹 🗳	Certificate Monitoring Validation General Support
	20 🔓	😹 Summary 🙀 Settings 🗍 Associations 🚜 Compliance 🕓 History
Search options	-•	😇 Restart   🦧 Retry   🎒 Reset 🔹   🔣 Renew Now 🛛 😞 Check Revocation   🖋 Validate Now   👰 Revoke 👻   🍓 Change Certif
Policy     Policy     Code Signing     SSH     TLS     Administration     Gradinations     Gradinations		Certificate Status Certificate Status Certificate Status Certificate Status Certificate Status Cifecycle Stage none
G Gigamon	o.com	Revocation Validation Last Check: Last Check:

- 8. Repeat the previous steps to create all other certificates for this policy.
- 9. Verify the certificates are created.

Policy 🗸	app1.venafidemo.com (Server Certificate) : Summary
😤 Add 👻 🗶 Delete Show all 🔹 🗳	Certificate Monitoring Validation General Support
20 😹	Summary Settings Associations Scompliance OHistory
Search options	🕲 Restart   🦧 Refry   🎲 Reset 🔹   🗳 Renew Now   🍔 Check Revocation   🖋 Validate Now   🤬 Revoke 🔹   🍕 Change Certificate
🖃 🍶 Policy	app1.venatidemo.com
⊞ 🚽 Code Signing ⊕ 🍶 SSH	Subject DN
TLS  Administration  Solution  Certificates	Common Name: app1.venafidemo.com Subject Alt Name (DNS): app1.venafidemo.com
🖃 🌄 Test Certs	Issuer DN
ag) app2. venafidemo.com ag app1. venafidemo.com ag ag Gigamon ag ag GigaVUE-FM ag Gigamon Credential	Common Name: venafidemo-TPP-CA Domain Component: venafidemo com
	Private Key
GOLFP     Golf Venafi Operational Certificates     Aperture Configuration	Private Key Stored: Yes, Stored in Software
	Miscellaneous
	Valid From: 7/22/2020 12:14:38 PM Valid To: 7/22/2022 12:14:38 PM
	Serial Number: 2F0000002007ECD3928D4BD48E00000000020

Step 6: Set up a bulk provisioning job

- 1. Open the Aperture Interface.
- 2. Click Jobs.

V	ENAFL	🎨 Aperture	Dashboards	~ Inv	entory ~	Jobs	Clients ~	Reports ~	Configuration ~	
	All Certificates Dashboard									
	Certificate Totals	+								
	My Certificates	Expiring within	n 30 days	In Error		Key Size < 2 RSA keys	2048	Weak Signing Algorithm	m Validity Period	d > 8;
	8		1	(	)		0	0		0

3. Click **Create New Job** on the top right.

⊘ ▦	Q			
+ Create New Job	[			
0 Jobs				
		Priority =	Results	Type =

4. Select "Bulk Provisioning" and click Start.



5. Select the jobs policy created earlier or use an existing one. Click Next.

New Bulk Provisioni	ng Job	
	Details Tar	gets
То	get started, give us a few details about your Bulk Provisioning job. Job Details Parent Folder* Policy \TLS \ Jobs	
	Name * Gigamon Provisioning Description	
	Contacts Search for an identity	
	Cancel Next	

- 6. Under Job Details, specify
  - Target: set the GigaVUE-FM Device (GigaVUE-FM in this example) as the target
  - **Source**: specify the policy folder that contains the certificates to be provisioned to the GigaVUE-FM Device

**NOTE**: There may be one or many different policy folders containing the application certificates. The policy Management Type for these folders/certificates must be set to Provisioning.

**NOTE**: These certificates will be provisioned to a specific Gigamon node, which is specified in the Cluster ID parameter later in this section. You will need to create and run a separate job for each Gigamon node.

New Bulk Provisioning Job	
Details Next, let's define the source, target, and options for your Bulk Provisioning jo	Targets
Target   Devices*   Policy \TL\$ \ Certificates \ Gigamon \ GigaVUE-FM ×   Source    Folders that contain certificates*   Policy \TL\$ \ Certificates \ Test Certs ×    Options     Include certificates that expired in the last 30 days   Include revoked certificates   Include historical certificates   Certificate batch size 200	

- 7. Select the appropriate options for your environment and click Next.
- 8. Select the appropriate frequency for the provisioning job to run and click **Next**.

New Bulk Provisioning Job						
Details	Targets					
Next, let's define when you would like this job to run?						
Frequency *						
Manually run Every week Every month Every year						
Cancel Back Next						

- 9. For **Powershell Script**, select the Gigamon GigaVUE-FM driver that was installed earlier.
- 10. For **Cluster ID**, enter the hostname or IP address of the Gigamon device that requires provisioned certificates, and then click **Next**.

New Bulk Provisioning Job				
Finally, you need to get up you	Details	<b>T</b> argets	Occurrence	Installation Settings
Sottings	provisioning script.			
PowerShell Script*		GigamonGigaVUE-FM		~
Cluster ID *		10.115.46.169		
Enable Debug Logging		● No OYes	Ŋ	
Cancel Back Create	e & Run Create Job			

- 11. Click Create Job.
- 12. You can wait for the job to run on the specified schedule or click **Run Now** to run the job immediately.

Gigamon Provisioning		Pup Now
Policy/TLS\Jobs\		Kun Now
Results	Job Details	
Details and Targets	Parent Folder"	
Schedule	Policy \ TLS \ Jobs	× *
ermissions		
	Name *	
	Gigamon Provisioning	
	Description	
	Contacts	
	Search for an identity	
	Target	
	Devices "	Create New Devices
	Policy \ TLS \ Certificates \ Gigamon \ GigaVUE-FM x	
	Source	
	Folders that contain certificates "	
	Policy \ TLS \ Certificates \ Test Certs ×	
	Options	
	Include certificates that expired in the last 30 days	
	Include revoked certificates	
	Include historical certificates	
	Certificate batch size 200	

#### 13. Click **Results** to see if the job completes successfully.

Gigamon Provision	ning			
Policy\TLS\Jobs\				
Results Results				
Details and Targets	Status	Complete		
Schedule	Last Run	7/22/2020 12:29 PM (-06:00 UTC)		
Permissions	Certificates To Provision	2		
	Provisioned Certificates via Full Run	2		
	Provisioned Certificates via Express Run	0		
	Devices			
	In Progress	0		
	In Retry	0		
	Failed	0		
	Completed	1		

14. Repeat the steps in this section to create a separate bulk certificate provisioning job for each GigaVUE Node that must be provisioned.

**IMPORTANT**: It is important to understand this last step, above. Certificates cannot be provisioned to multiple GigaVUE Nodes via a single job. A separate job is required for each physical GigaVUE Node that must be provisioned.

#### **Step 7**: Verify that certificates have been pushed to the desired device

- 1. Navigate to **GigaVUE-FM > Physical Device** and select the desire device (GigaVUE Node).
- 2. From the device, navigate to GigaSMART > InlineSSL > KeyStore.
- 3. Verify the certificate information.
- 4. Note that the **Key Alias** is derived from the certificate common name and thumbprint. This supports the addition and identification of multiple certificates with the same common name.
- 5. Type should indicate a check mark beside both the Certificate and Private Key
- 6. **Health Status** will indicate if the certificate is or is not participating in a flow, depending on the Auto Enable New Certificates setting.

GigaVUE-FM	jigamon-9a0b3	7 ip-10	-115-46-169.us-we	st-2.compute	e.internal (H	Series) Last synced
	Inline SSL SSL Profiles Ke			Key Store	Signing CA	A Trust Store
	Session St	Monitor Statistics	Certificat	te Statistics		
🔒 Overview	• Filtered By : <b>none</b>				Ke	eychain Password
௺ Workflows						
📥 Node Topology	Key A	lias		Туре		Health Status
	app1.v	venafidemo	.com-3DB2A702D753	🗸 Certi	ficate, 🗸	(i) Certificate not
	app1.v	venafidemo	.com-8CCF7E94A8E2.	🗸 Certi	ficate, 🗸	(i) Certificate not
📥 Ports 🔷 🔺	app2.v	venafidemo	.com-D95E0FCF39A3.	🗸 Certi	ficate, 🗸	i) Certificate not
Ƴ Maps ∧						
互 GigaSMART® 🛛 🗸						
GigaSMART Oper						
GigaSMART Grou						
Virtual Ports						
NetFlow/IPFIX Ge						
Inline SSL						
Passive SSL						