GigaVUE-FM/Venafi Trust Protection Platform Integration Guide

GigaVUE-FM 5.9

Documentation Version: 1.0
Documentation Date: September 4, 2020

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

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:

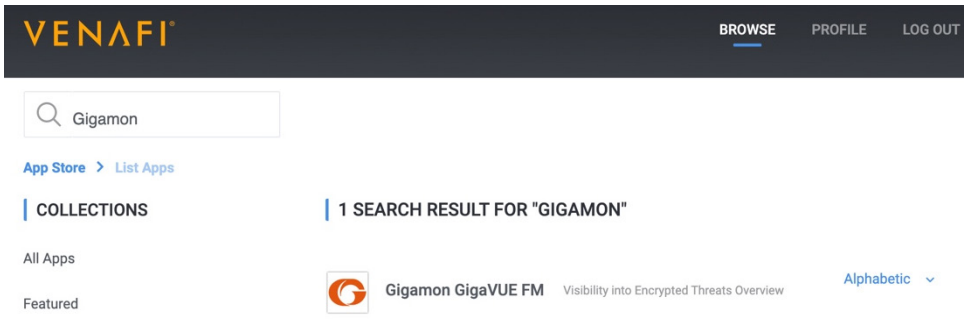
Before you begin

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

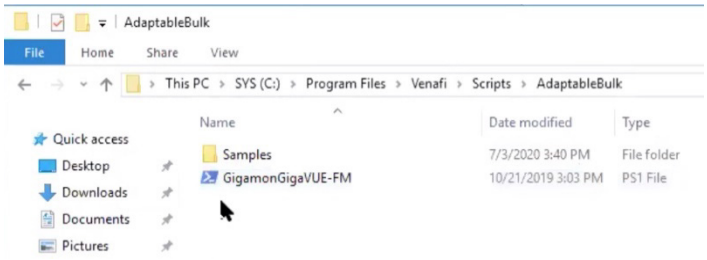
- GigaVUE-FM hostname/network address and port number
- GigaVUE-FM logon credentials
- List of GigaVUE Node/Cluster Names to be provisioned
- Mapping of certificates-to-GigaVUE nodes/clusters

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

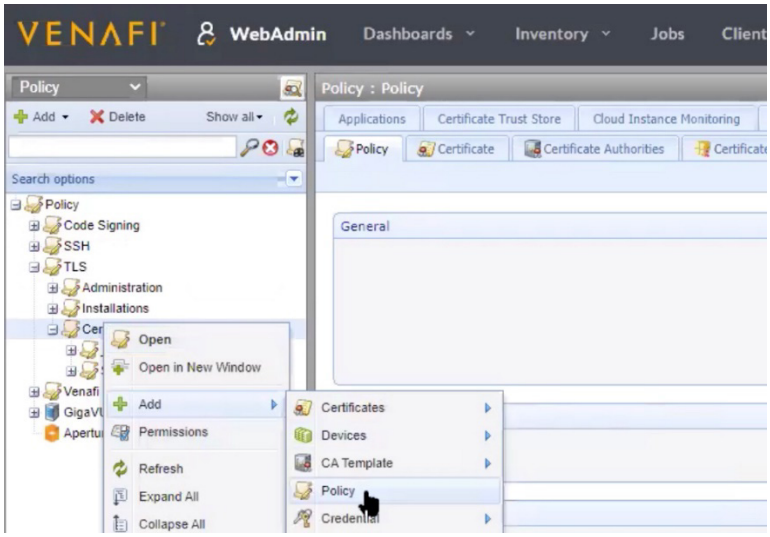


Step 2: Set up the Gigamon policy hierarchy

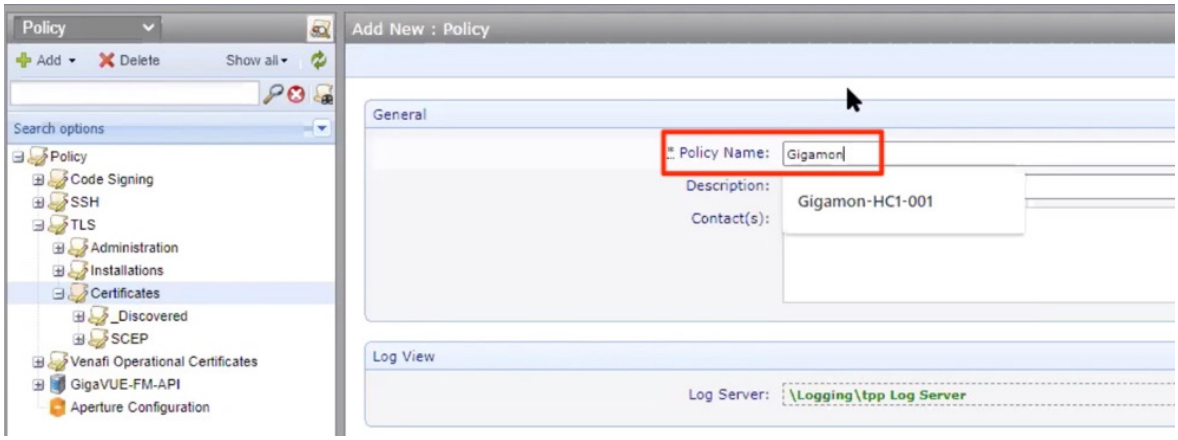
NOTE: TPP supports a flexible policy hierarchy and will likely differ from one environment to the next. This guide section provides the following sample hierarchy:

- Policy
  - TLS
    - Certificates
      - Gigamon
        - Device (GigaVUE-FM)
        - Gigamon Credential

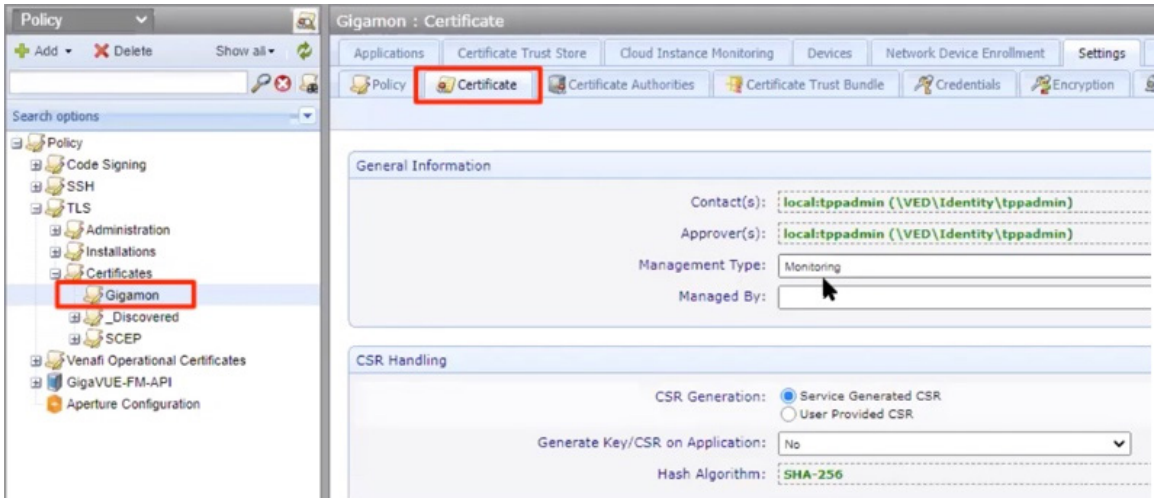
1. Log in to Venafi TPP Web Admin Console.
2. Set up a new policy under the appropriate TLS Certificate section based on the environment.
3. In the left navigation, navigate to **Policy > TLS > Certificates**.
4. Right-click on Certificates and select **Add > Policy**.



5. Name the policy “Gigamon” for ease of reference and click **Save**.

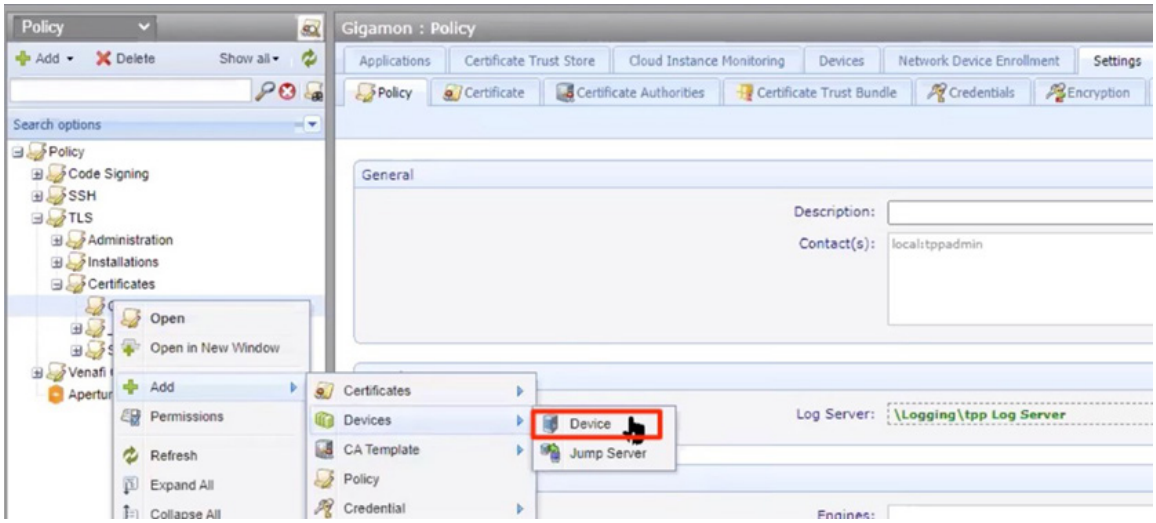


6. After creating the policy, it will appear in the Venafi left navigation under **Policy > TLS > Certificates**.



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

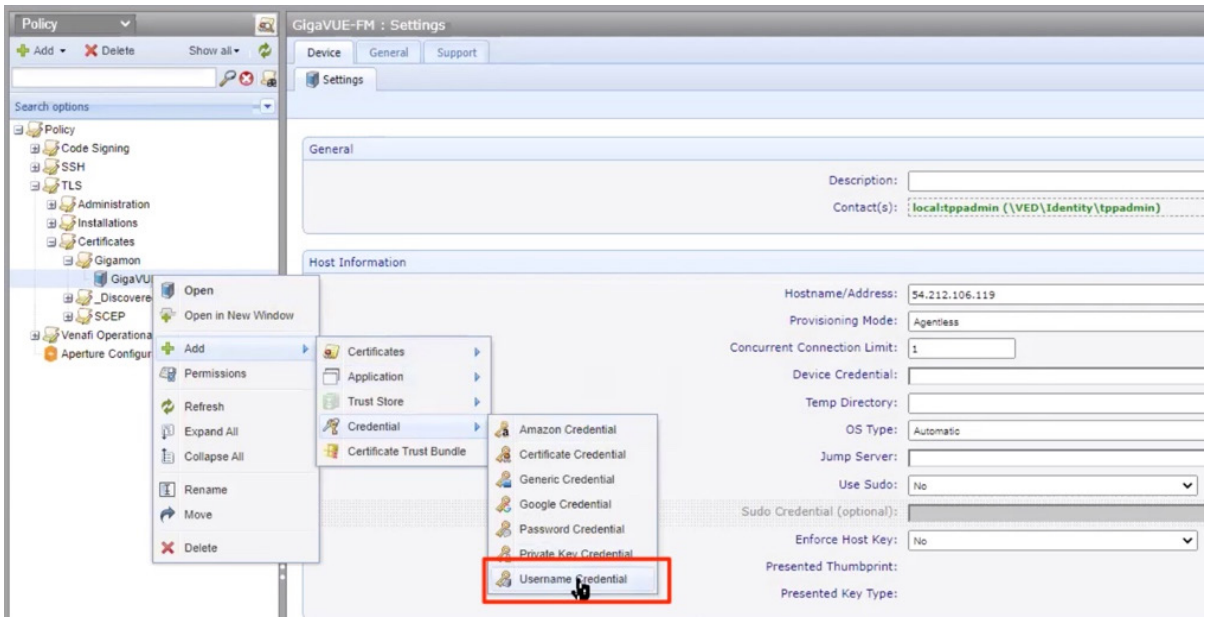
1. To set up the device, select the Gigamon policy folder you just created and select **Add > Devices > Device**.



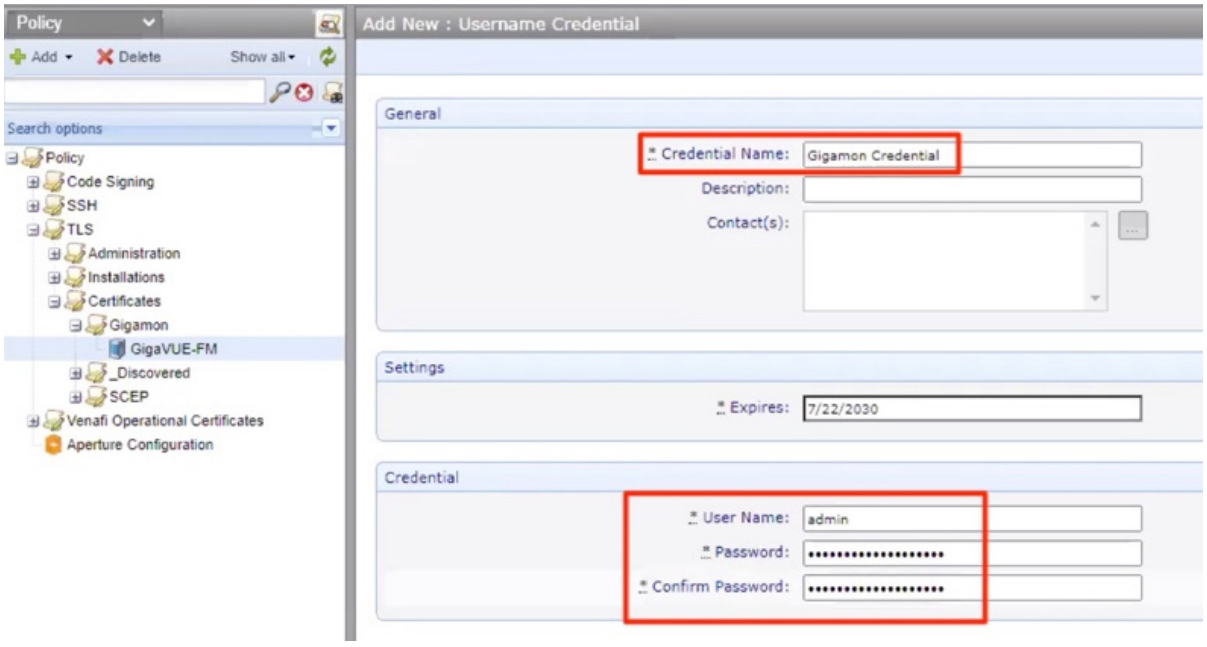
2. For the **Device Name**, specify a meaningful name for the GigaVUE node.
3. For the **IP address**, enter the GigaVUE-FM IP address.

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

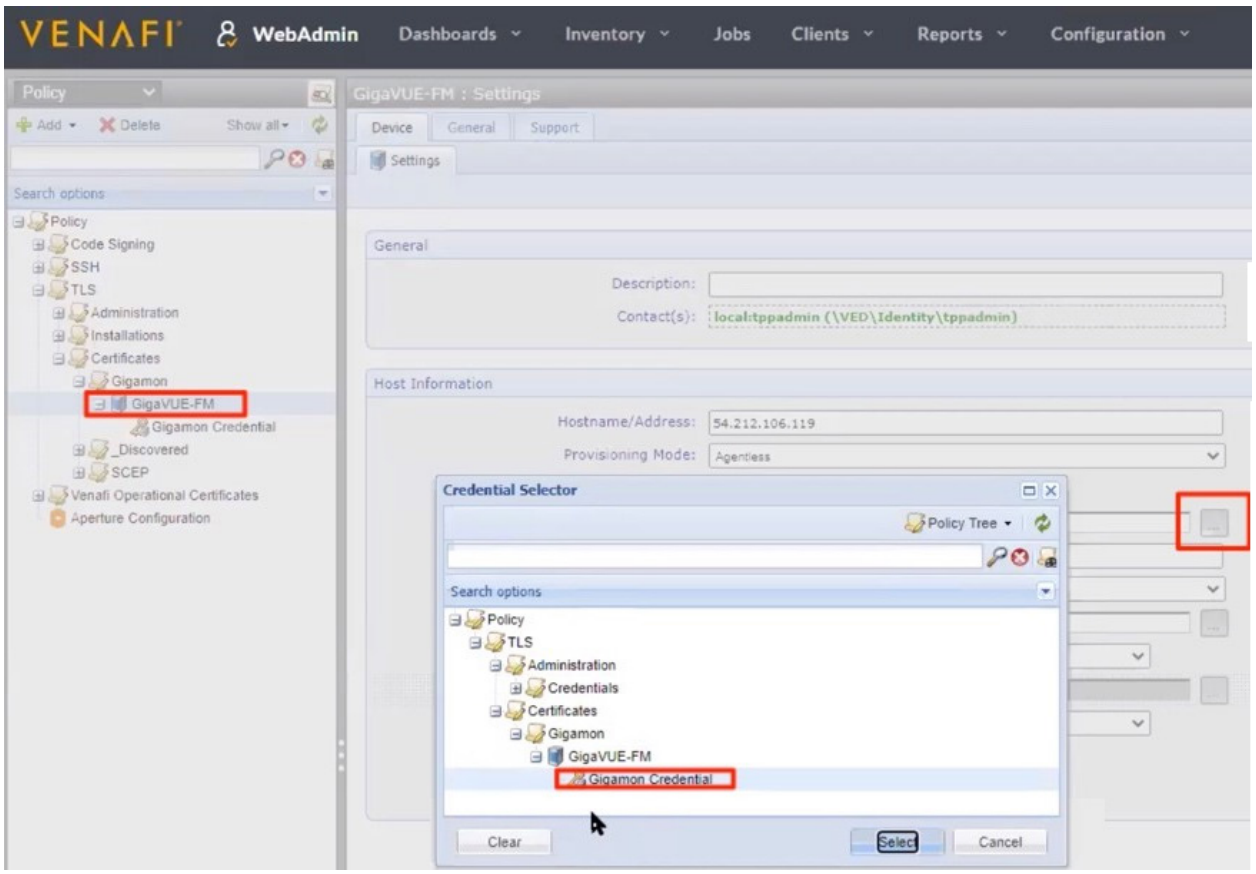
   NOTE: In this example, the device is named “GigaVUE-FM.”



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



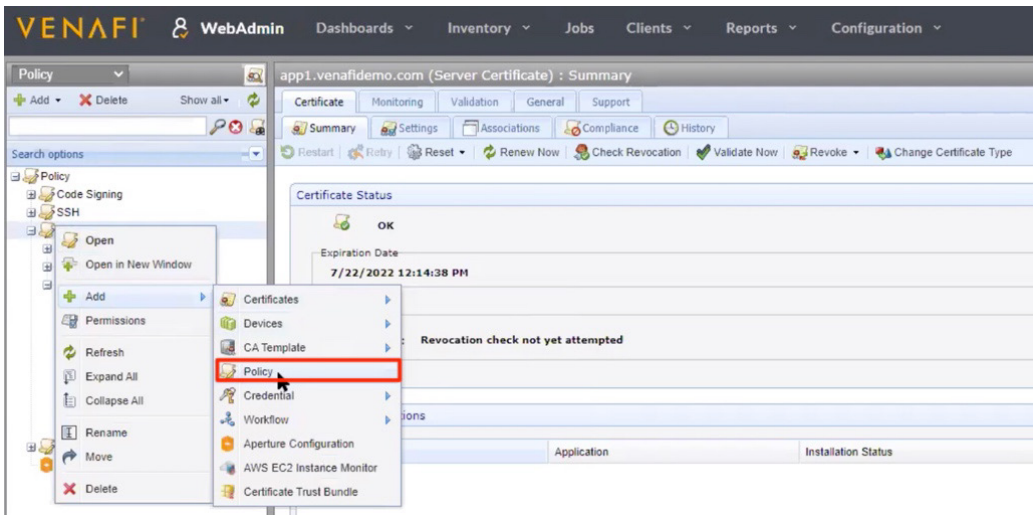
7. To assign these credentials to the device, click on the device (named “GigaVUE-FM” in this example) to view the device settings.
8. In the device settings, under Most Information, click the Credential Selector icon.
9. Select “Gigamon Credential” and click **Save** to set the credentials.



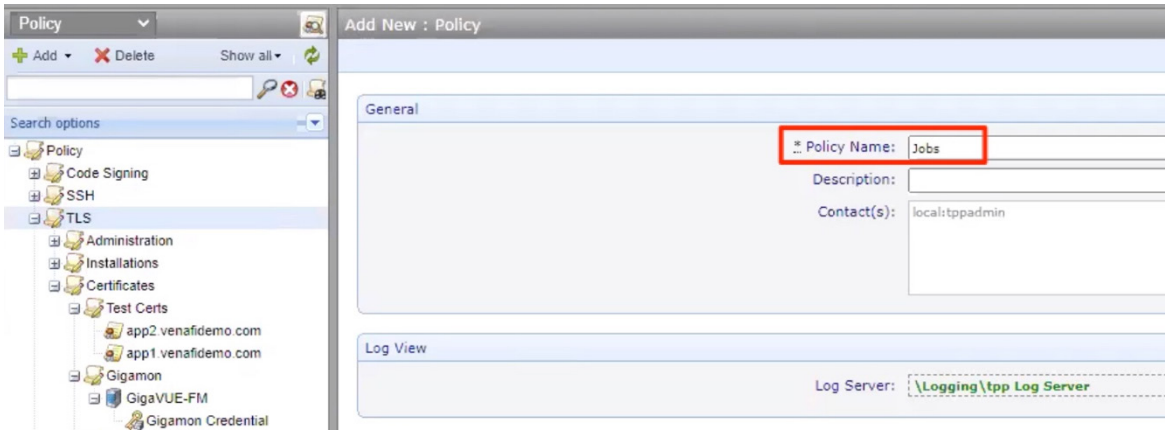
Step 4: Set up a policy object for provisioning jobs.

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**.



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

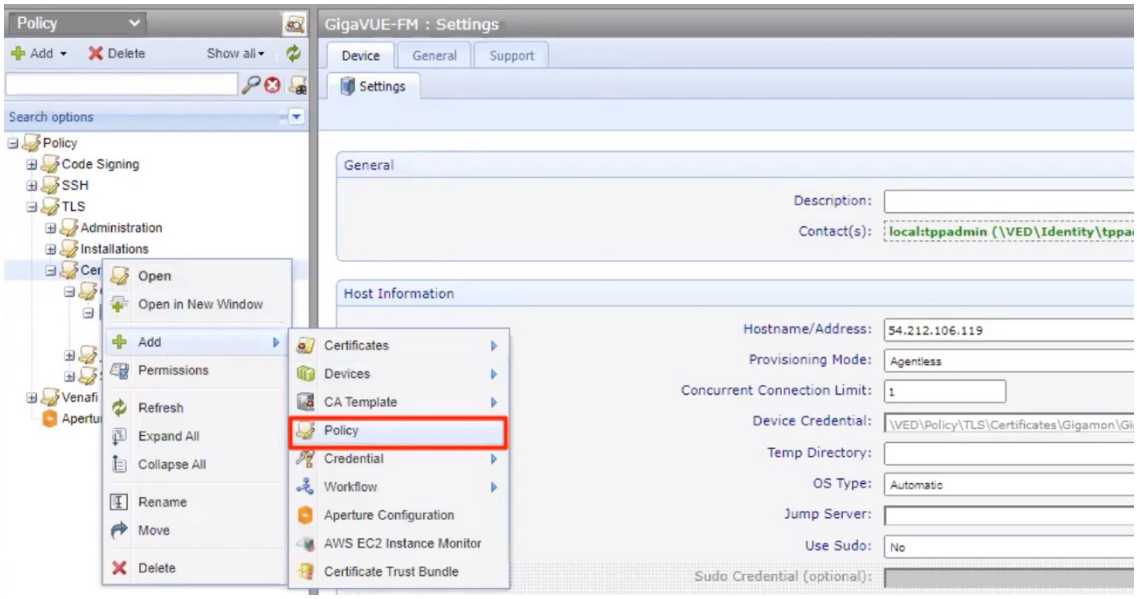


Step 5: Create certificates to provision (Skip if preexisting)

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."

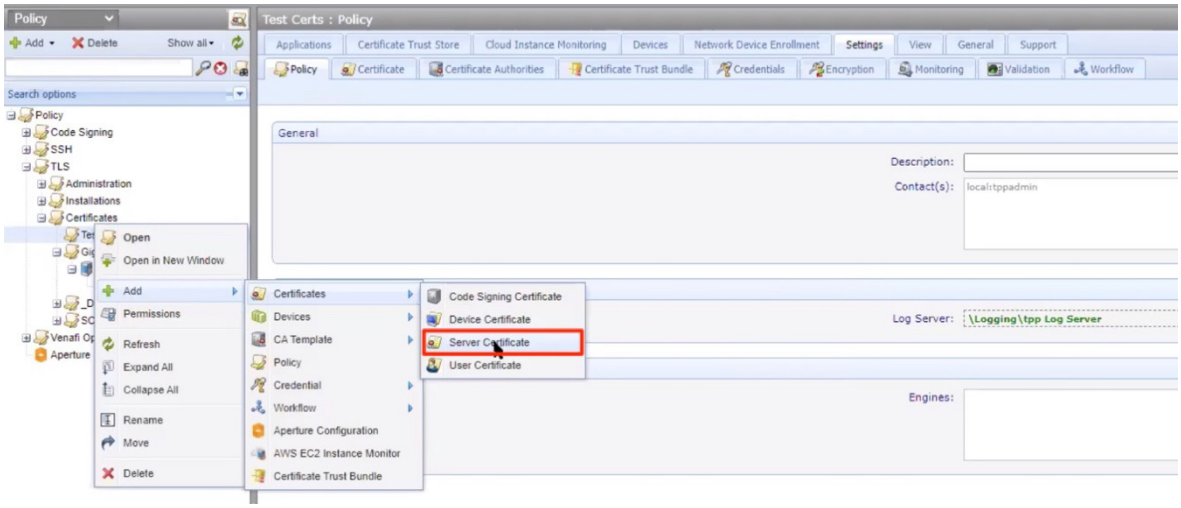
You can create a new policy or use an existing policy to create new certificates

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

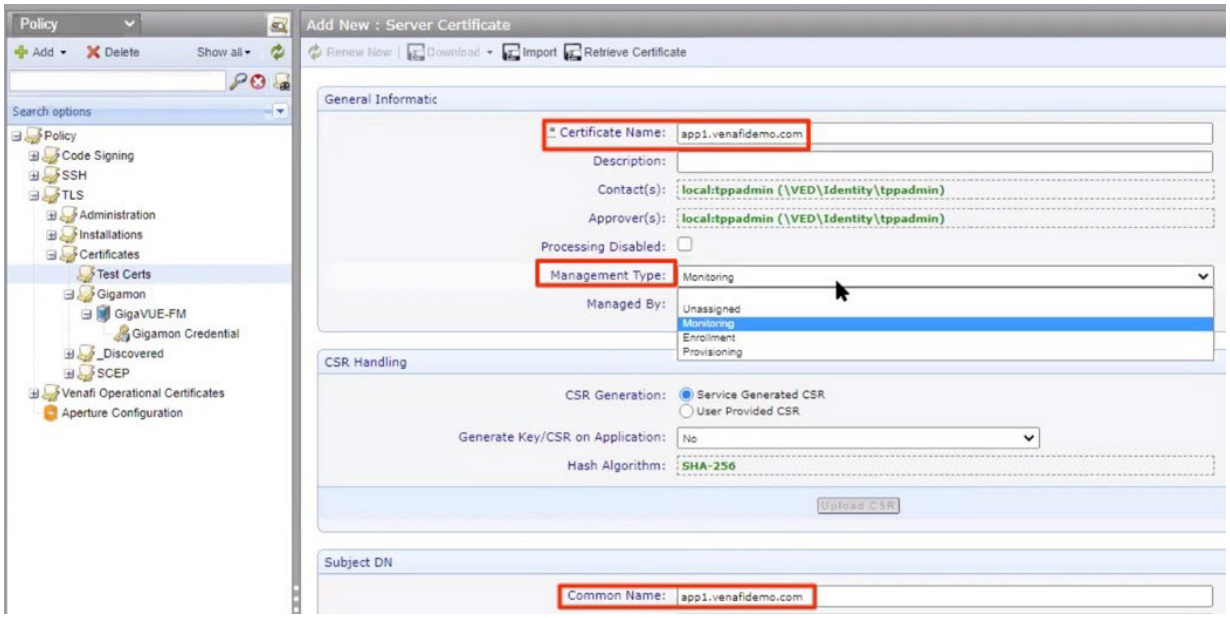


2. Specify a meaningful name for the policy and click **Save**.

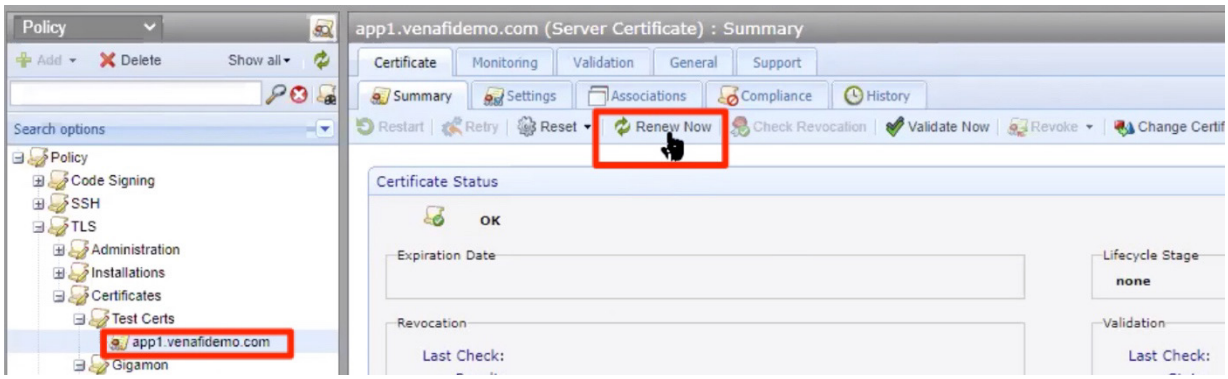
3. To create new certificates under this policy, right-click on the policy and select **Add > Certificates > Server Certificate**.



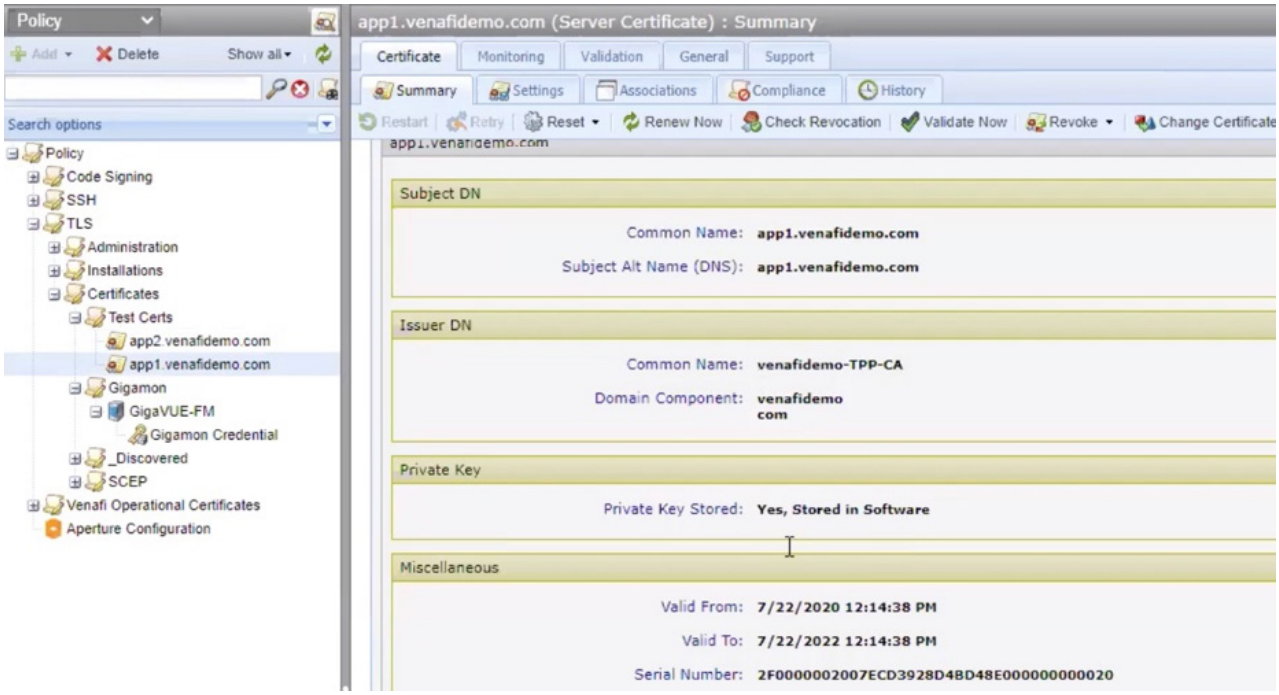
4. Specify the appropriate certificate parameters.
5. For Management Type, set it to “Provisioning.”



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

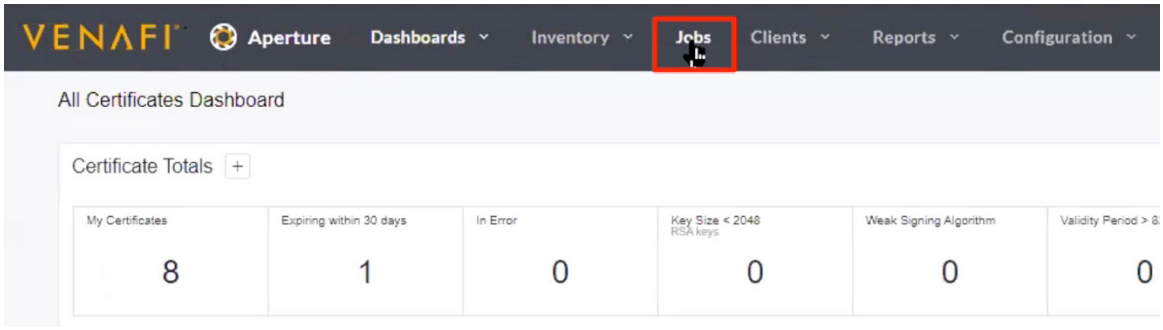


8. Repeat the previous steps to create all other certificates for this policy.
9. Verify the certificates are created.

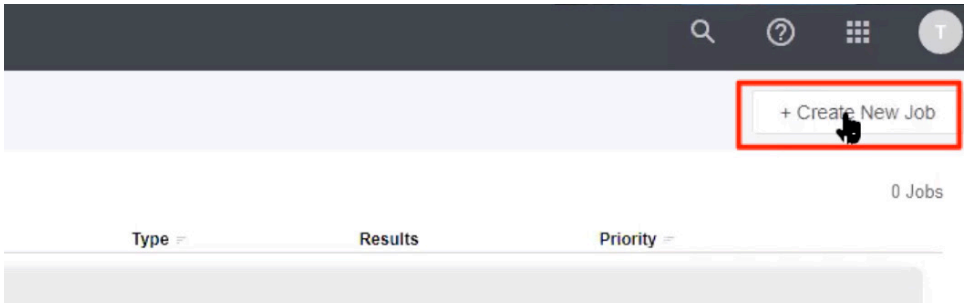


Step 6: Set up a bulk provisioning job

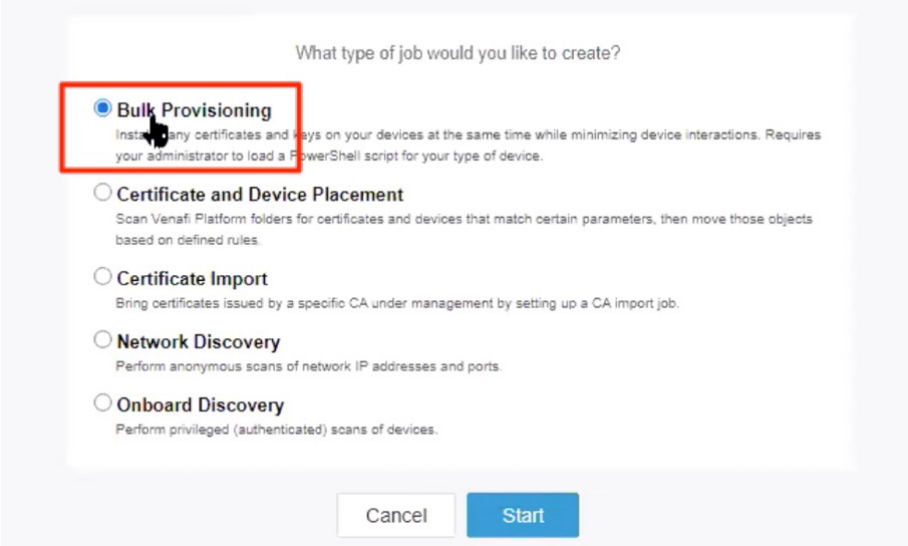
1. Open the Aperture Interface.
2. Click **Jobs**.



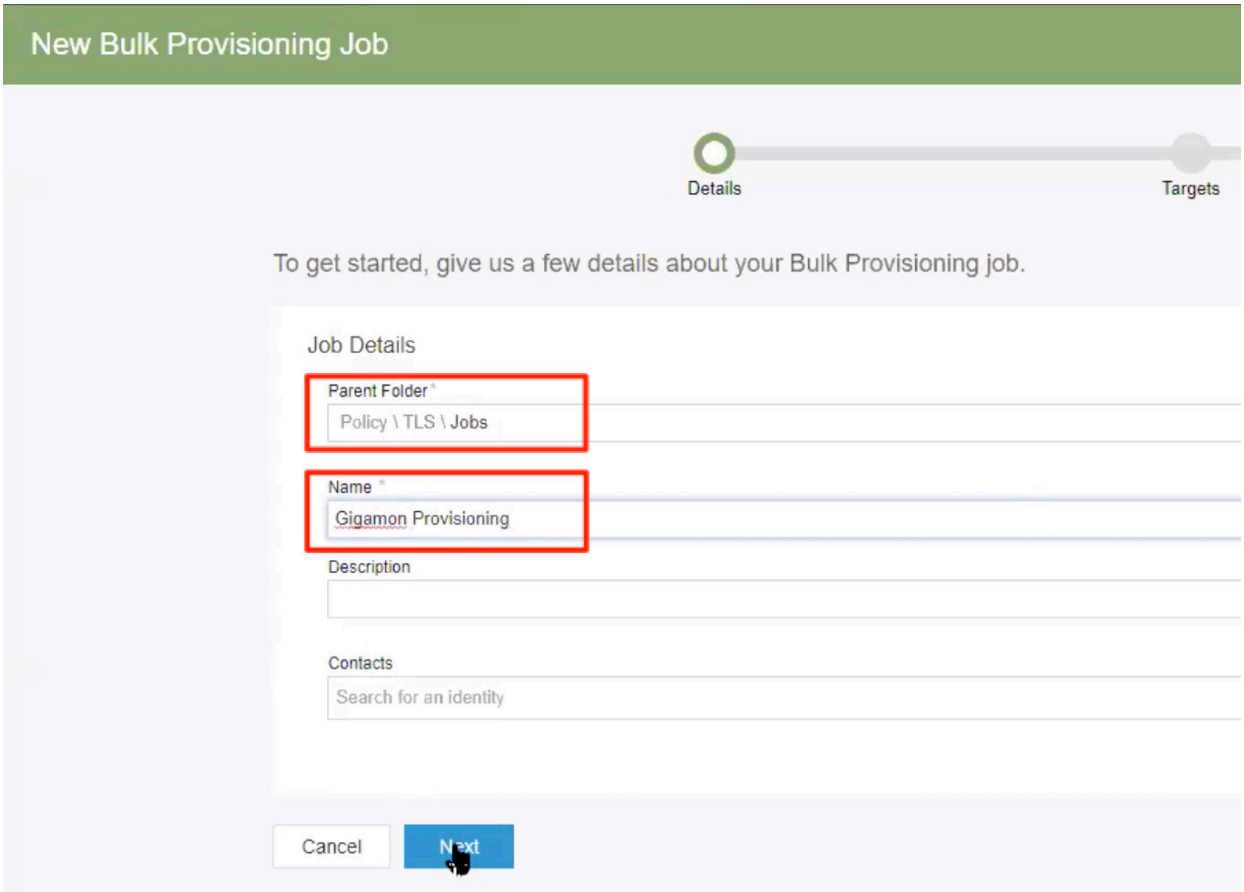
3. Click **Create New Job** on the top right.



4. Select “Bulk Provisioning” and click **Start**.



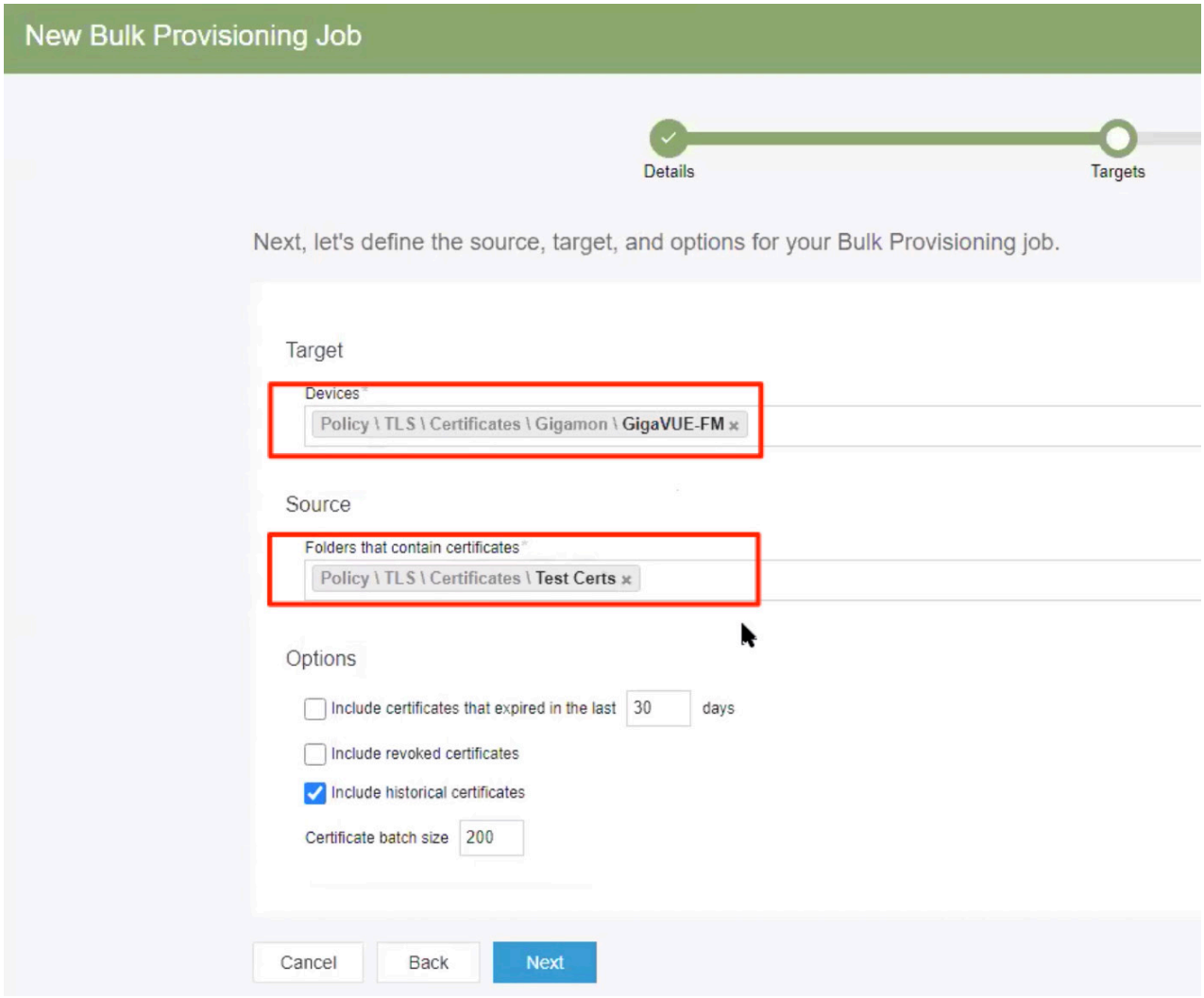
5. Select the jobs policy created earlier or use an existing one. Click **Next**.



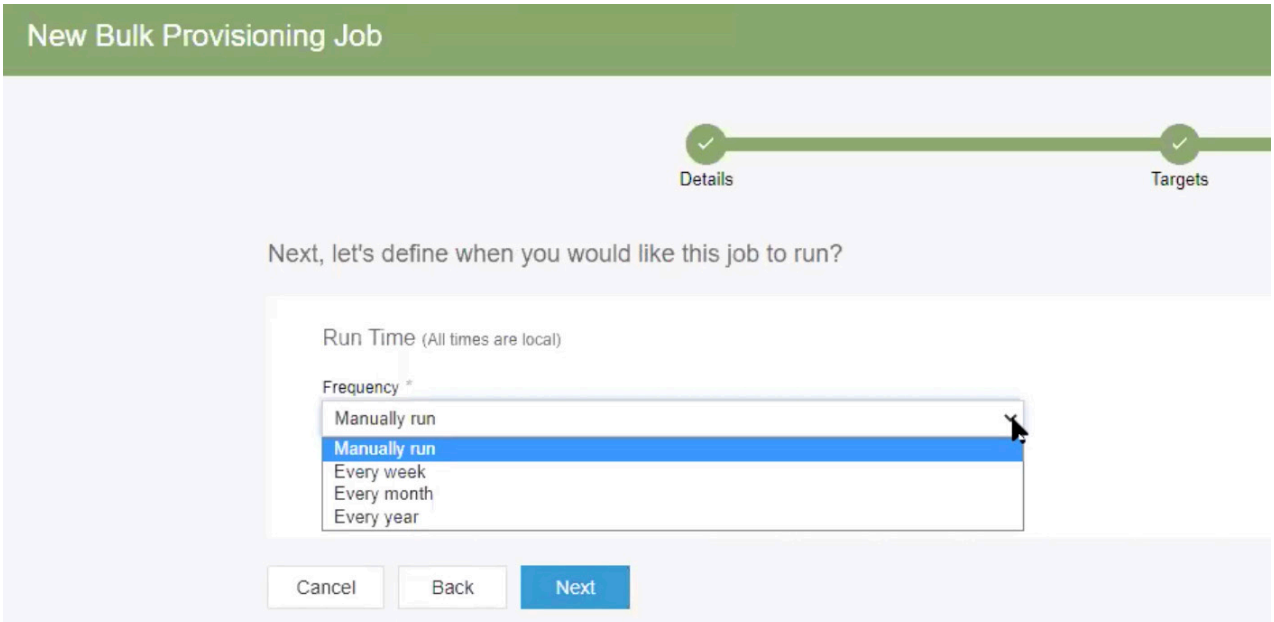
6. Under Job Details, specify
   - **Target**: set the GigaVUE-FM Device (GigaVUE-FM in this example) as the target
   - **Source**: specify the policy folder that contains the certificates to be provisioned to the GigaVUE-FM Device

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.

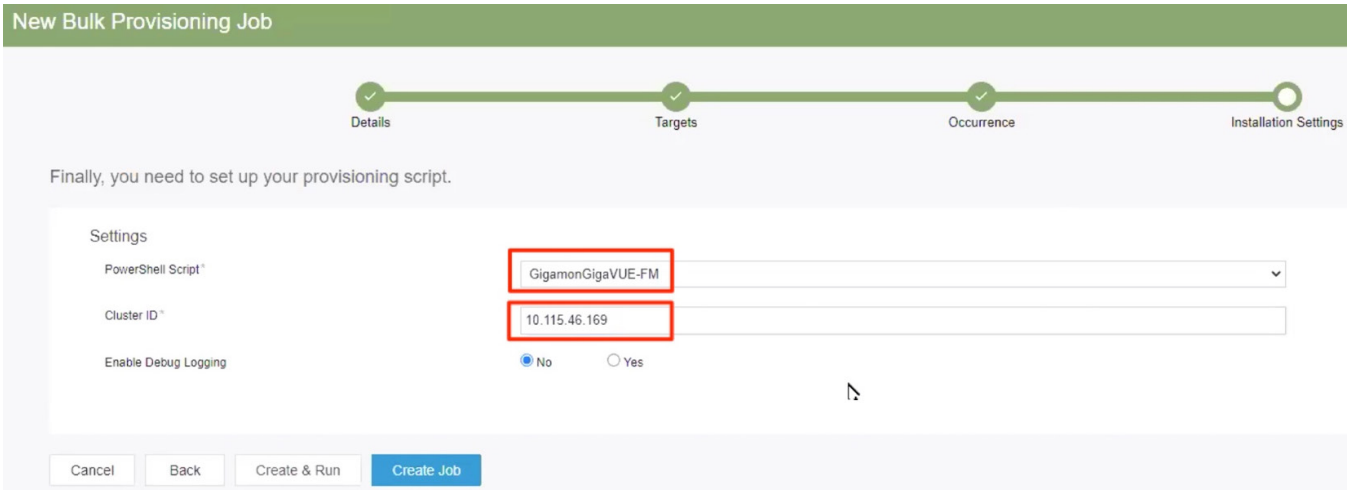
NOTE: These certificates will be provisioned to a specific Gigamon node, which is specified in the Cluster ID parameter later in this section. You will need to create and run a separate job for each Gigamon node.



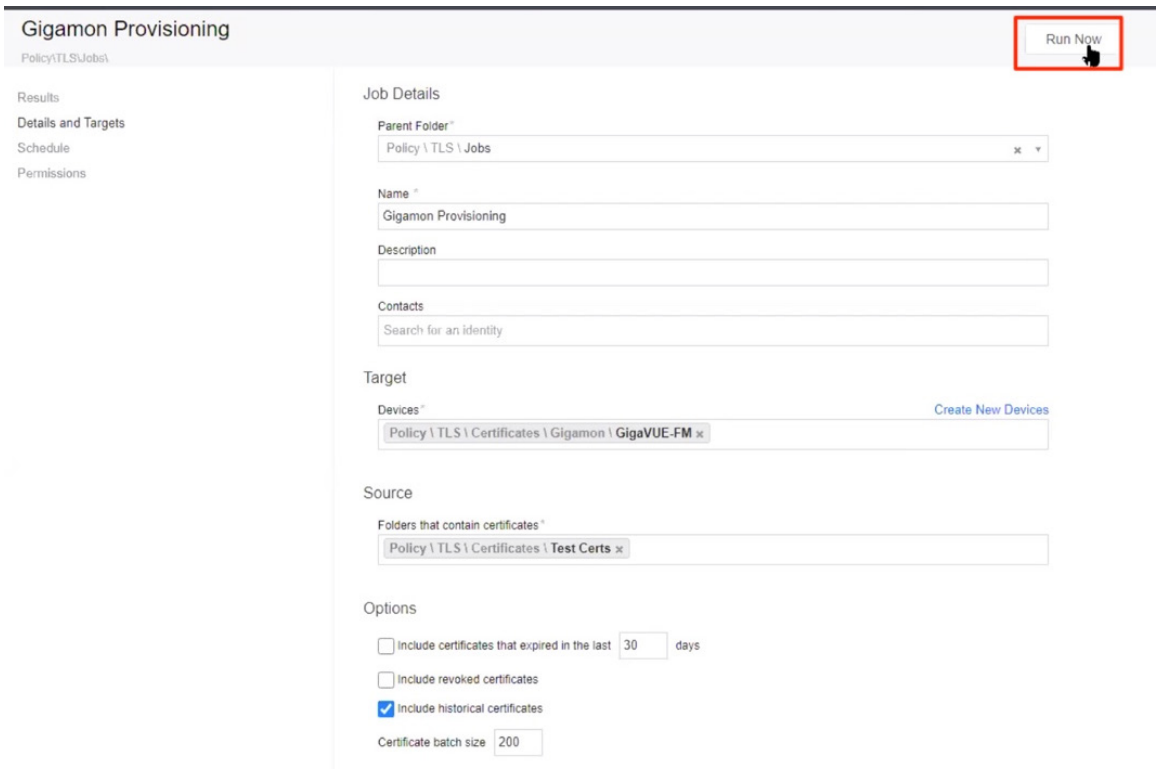
7. Select the appropriate options for your environment and click **Next**.
8. Select the appropriate frequency for the provisioning job to run and click **Next**.



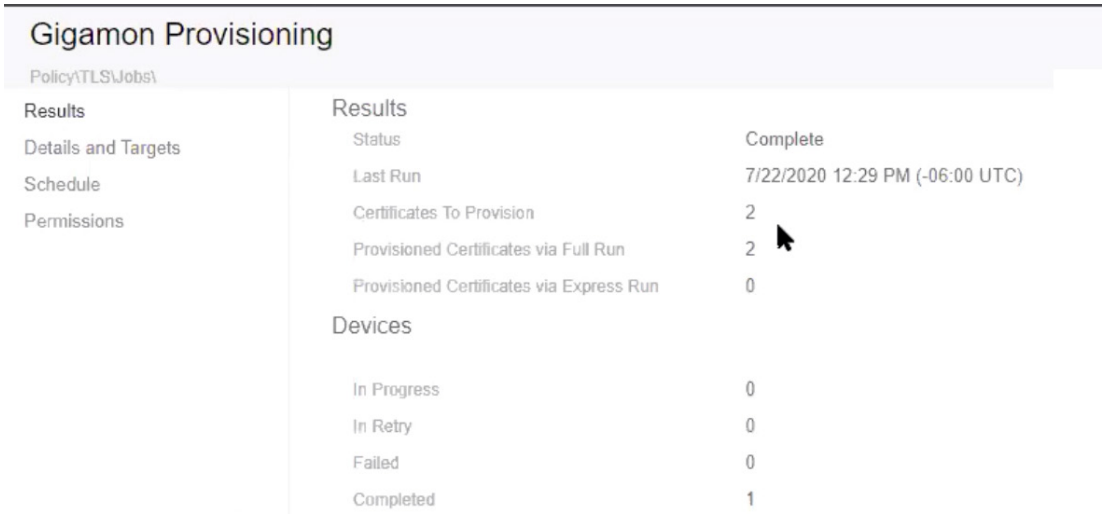
9. For **Powershell Script**, select the Gigamon GigaVUE-FM driver that was installed earlier.
10. For **Cluster ID**, enter the hostname or IP address of the Gigamon device that requires provisioned certificates, and then click **Next**.



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.



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



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.