HPE Alletra 6000 Storage Array

KeyControl® Integration Guide

21 Apr 2023

Contents

1. Introduction

This document describes the integration of the Hewlett Packard Enterprise (HPE) Alletra 6000 Storage Array (referred to as Alletra in this guide) with the Entrust KeyControl 10.0 (formerly HyTrust KeyControl) key management solution using the open standard KMIP protocol. Entrust KeyControl (referred to as KeyControl in this guide) serves as a key manager for encryption keys by using various protocols, including KMIP.

1.1. Product configurations

Entrust has successfully tested the integration of KeyControl with HPE Alletra 6000 in the following configurations:

System	Version
HPE Alletra 6000	6.1.2.0-1022277
Entrust KeyControl	10.0

1.2. Requirements

Before starting the integration process, familiarize yourself with:

- HPE general support page.
- HPE GUI administration guide for the Alletra 6000 version 6.1.2.x.
- The documentation and set-up process for Entrust KeyControl, see Entrust KeyControl Product Documentation.
- Also see Entrust KeyControl 10.0 Online Documentation Set.

Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

2. Procedures

Follow these steps to install and configure KeyControl.

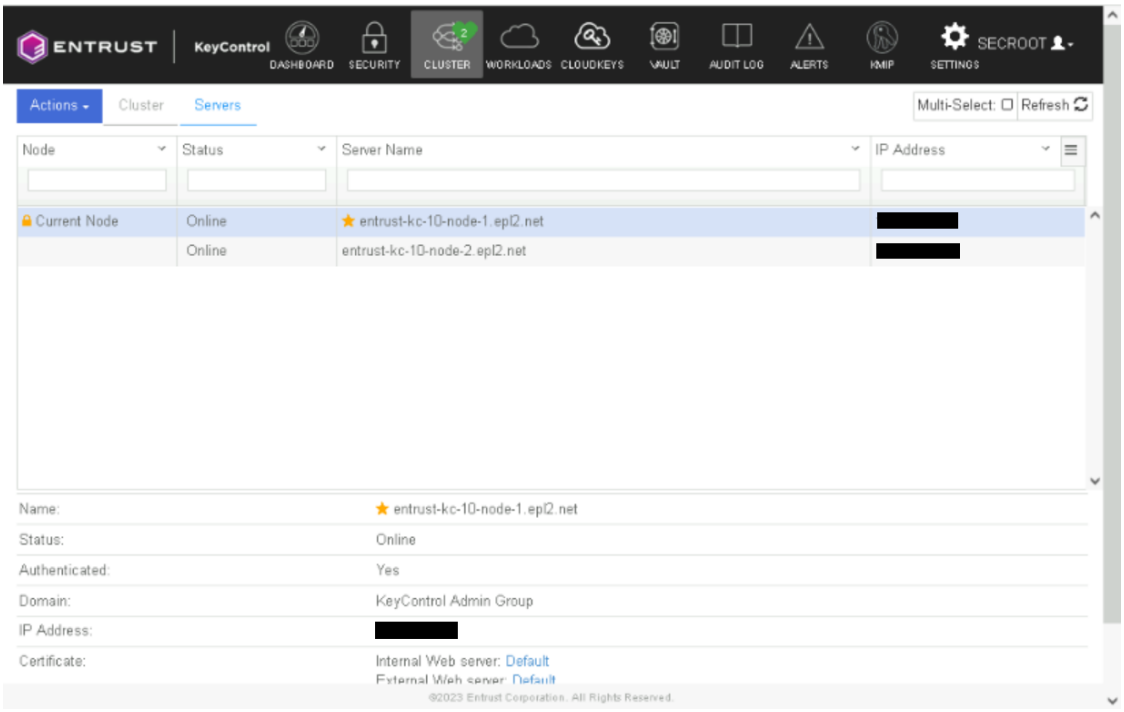
1. Deploy a KeyControl cluster.
2. Additional KeyControl cluster configuration.
3. Authentication.
4. Create DNS record for KeyControl cluster.
5. Enable KMIP.
6. Create tenant.
7. Create the HPE Alletra certificate request.
8. Create the tenant client certificate bundle.
9. Import tenant client certificate into Alletra.
10. Register the Entrust KeyControl KMS.
11. Execute tests.

2.1. Deploy a KeyControl cluster

This deployment has a KeyControl cluster with two nodes. To deploy a KeyControl cluster with two nodes:

1. Download the KeyControl software from https://my.hytrust.com/s/software-downloads. This software is available both as an OVA or ISO image. The OVA installation method in VMware is used in this guide for simplicity.
2. Install KeyControl as described in KeyControl OVA Installation.
3. Configure the first KeyControl node as described in Configuring the First KeyControl Node (OVA Install).
4. Add second KeyControl node to cluster as described in Adding a New KeyControl Node to an Existing Cluster (OVA Install).

Both nodes require access to an NTP server, otherwise the above operation will fail. Log in the console to change the default NTP server if required.



5. Install the KeyControl license as described in Managing the KeyControl License.

2.2. Additional KeyControl cluster configuration

After the Entrust KeyControl cluster is deployed, additional system configuration can be done as described in KeyControl System Configuration.

2.3. Authentication

Local account authentication is used in this integration. For AD-managed Security groups, configure the LDAP/AD Authentication Server as described in Specifying an LDAP/AD Authentication Server.

2.4. Create DNS record for KeyControl cluster

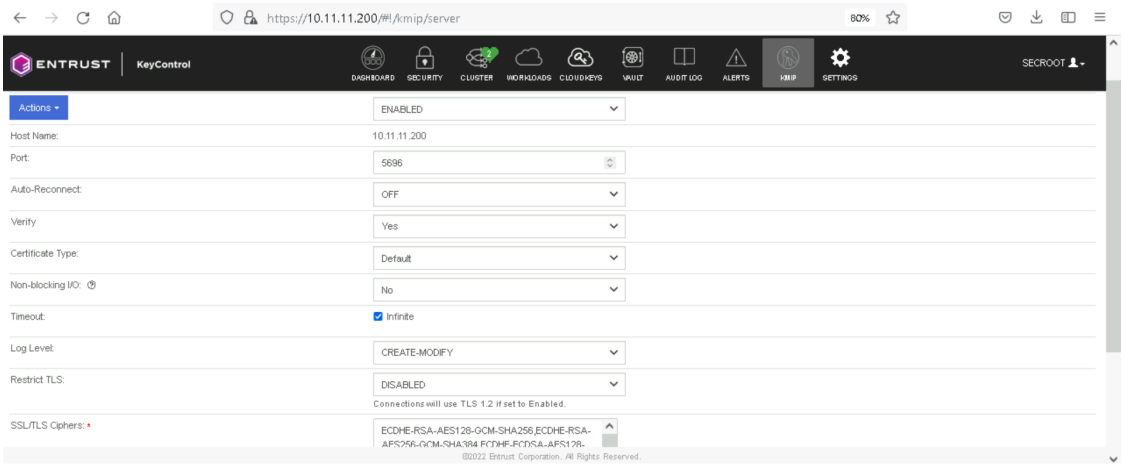
To create DNS record for KeyControl cluster:

1. Create a single DNS record named **EntrustKeyControl** in the domain.
2. Assign this record as many IPs as nodes in the cluster created above, two in this integration.

2.5. Enable KMIP

To enable KMIP:

1. Log into the KeyControl webGUI using an account with Security Admin privileges.
2. Select **KMIP** in the menu bar in the KeyControl webGUI. Then select the **Settings** tab.
3. For **State**, select **Enable**. Take the default for all other parameters. Then select **Apply**.



4. In the **Overwrite all existing KMIP Server settings?** dialog, select **Proceed**.

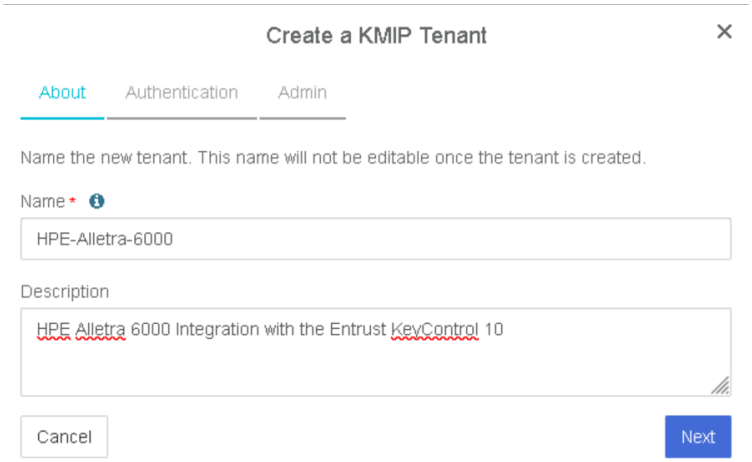
2.6. Create tenant

Entrust KeyControl 10.0 supports multi-tenancy. Therefore, a tenant must be created before setting up any KMIP services.

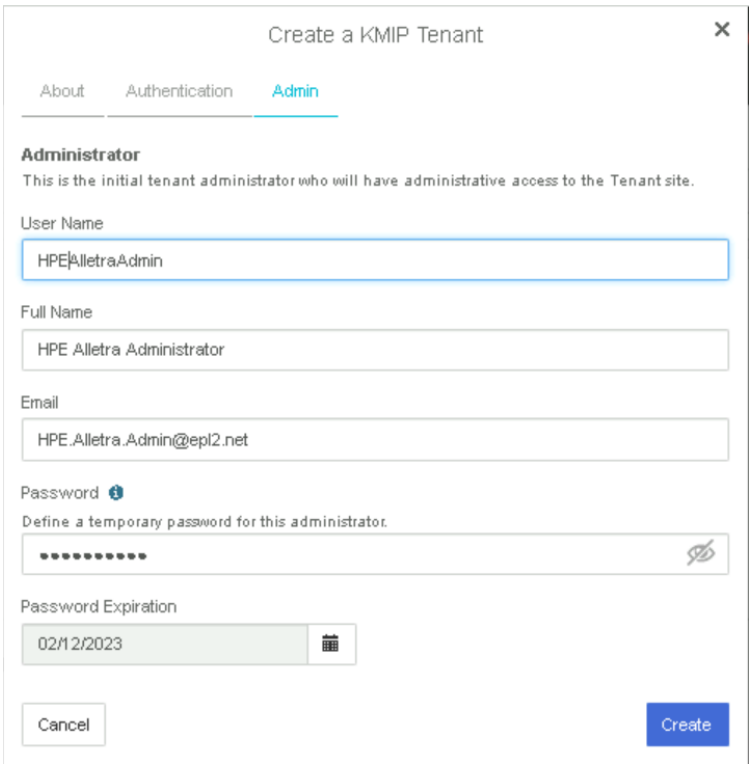
To create a tenant:

1. Log into the KeyControl webGUI using an account with Security Admin privileges.
2. Select **KMIP** in the menu bar in the KeyControl webGUI. Then select the **Tenants** tab.
3. Select **Actions > Create a KMIP Tenant**. The **Create a KMIP Tenant** dialog appears
4. On the **About** tab, enter the name and description. Then select **Next**.

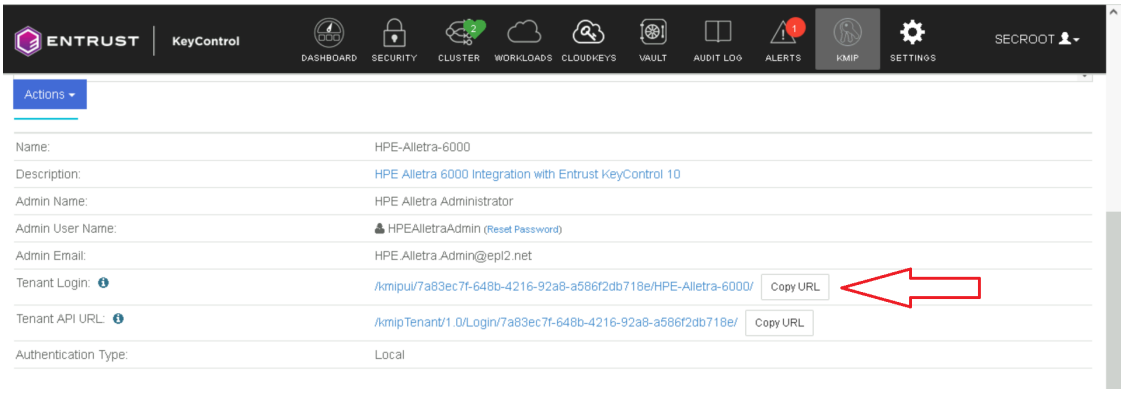
The tenant name cannot be changed after the tenant is created.



5. On the **Authentication** tab, select **Local User Authentication**, see Authentication. Then select **Next**.
6. On the **Admin** tab, enter the **Administrator** information. Then select **Create**.



7. Select the newly-created tenant and scroll down to see the tenant information. To test the tenant, select the **Tenant Login** URL and log in with the credentials above.



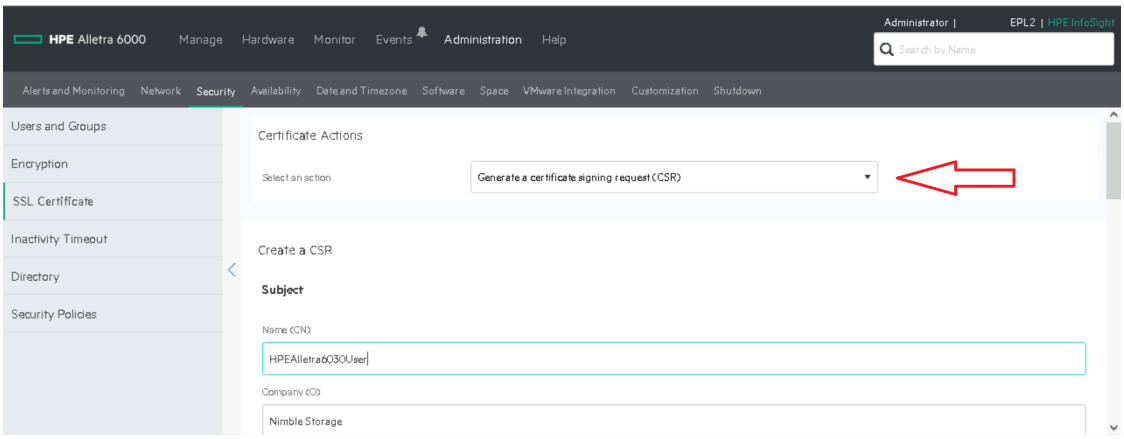
The **Tenant Login** URL is used later.

See the following link for additional information Creating a KMIP Tenant.

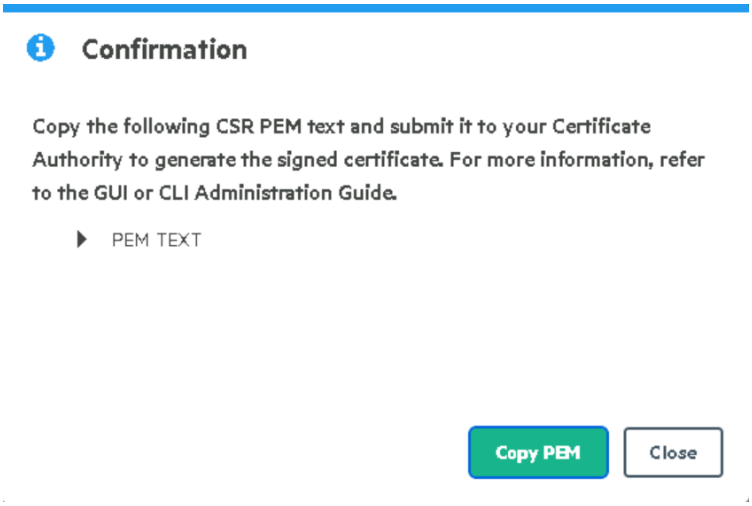
2.7. Create the HPE Alletra certificate request

1. Log into the Alletra 6030 webGUI using an account with Security Admin privileges.
2. Select **Administration** in the toolbar. Then select **Security > SSL Certificates**.

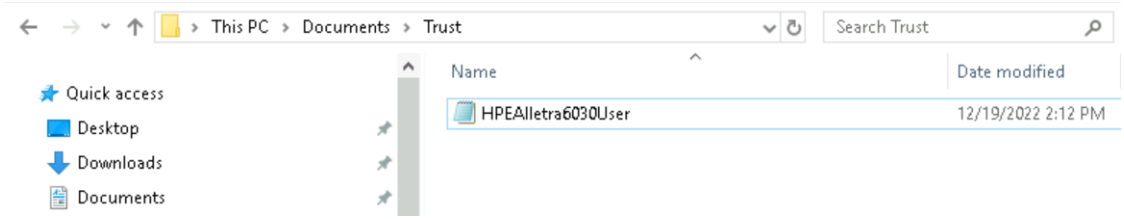
3. Select the **+** icon to add a certificate.
4. Select **Generate a certificate signing request (CSR)** in the **Select and action** drop-down text box.
5. Enter the **Name** and other required information. All defaults were selected in this integration. Then select **GENERATE**.



6. Select the certificate created. Then select **View**.
7. Select **Copy PEM** in the **Confirmation** dialog.



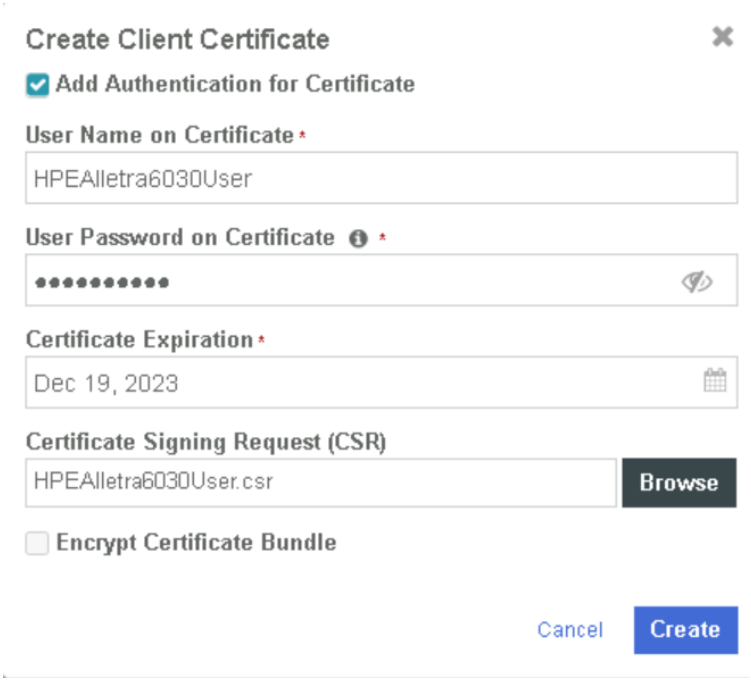
8. Create a `.csr` file type with a text editor containing the copied certificate request. If you use the **Notepad** text editor, you may need to rename the file using the Windows CLI to get the correct file type extension.



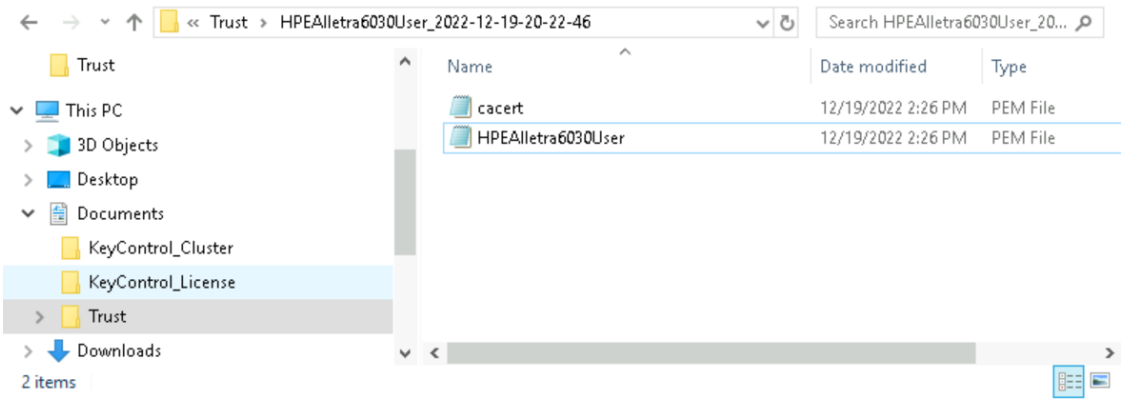
2.8. Create the tenant client certificate bundle

To create the tenant client certificate bundle:

1. Log into the KeyControl webGUI using an account with Security Admin privileges.
2. Select **KMIP** in the menu bar in the KeyControl webGUI. Then select the **Tenants** tab.
3. Highlight the required tenant. Scroll down and select the link on **Tenant Login**. A new tab opens in the browser.
4. Log in with the tenant credentials.
5. Select **Security > Client Certificates**.
6. Select the **+** icon on right top corner to create new client certificate.
7. Check **Add Authentication for Certificate** in the **Create Client Certificate** dialog.
8. Enter the authentication credentials and **Certificate Expiration** date. Upload the `.csr` file created in Create the HPE Alletra certificate request. Then select **Create**.



9. Select the certificate bundle created and select **Download**.
10. Extract the two files from the zip bundle.

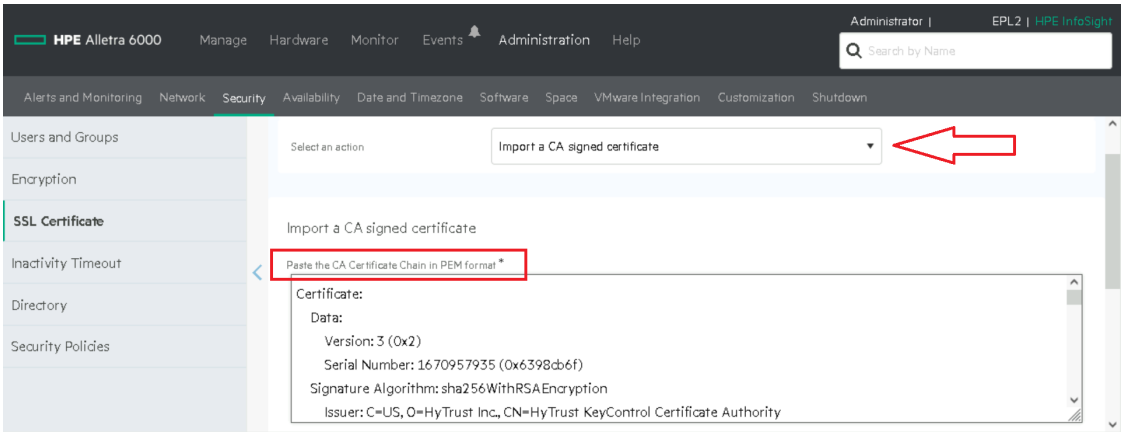


See the following link for additional information KMIP Tenant Client Certificates.

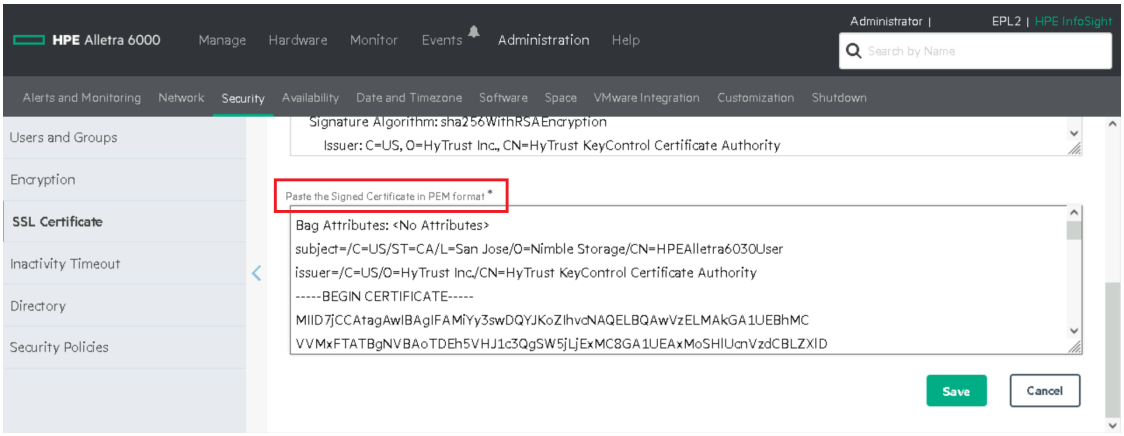
2.9. Import tenant client certificate into Alletra

To import tenant client certificate into Alletra:

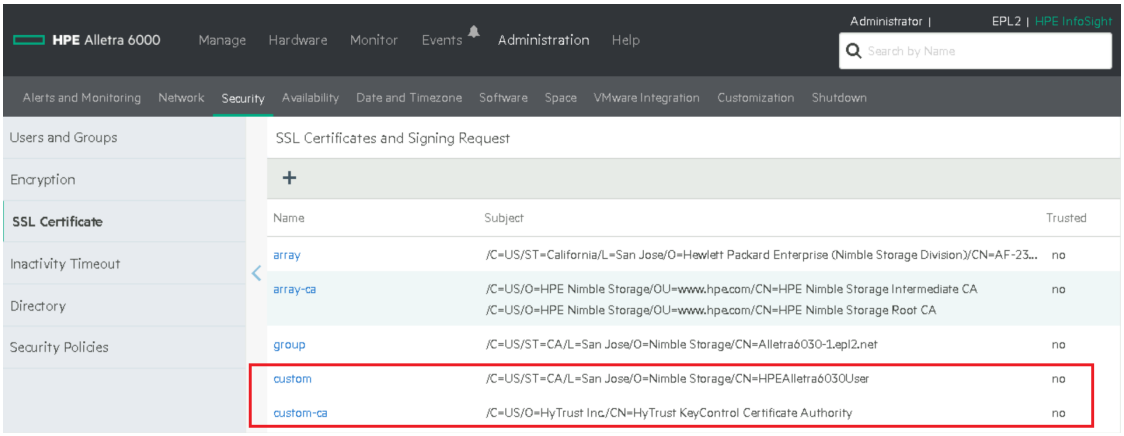
1. Log into the Alletra 6030 webGUI using an account with Security Admin privileges.
2. Select **Administration** in the toolbar. Then select **Security > SSL Certificates**.
3. Select **Input a CA signed certificate** in the **Select and action** drop-down text box.
4. Paste the content of the extracted `cacert.pem` file from Create the tenant client certificate bundle in the **Paste the CA Certificate Chain in PEM format** text box.



5. Paste the content of the extracted `HPEAlletra6030User.pem` file from Create the tenant client certificate bundle in the **Paste the Signed Certificate in PEM format** text box. Then select **Save**.



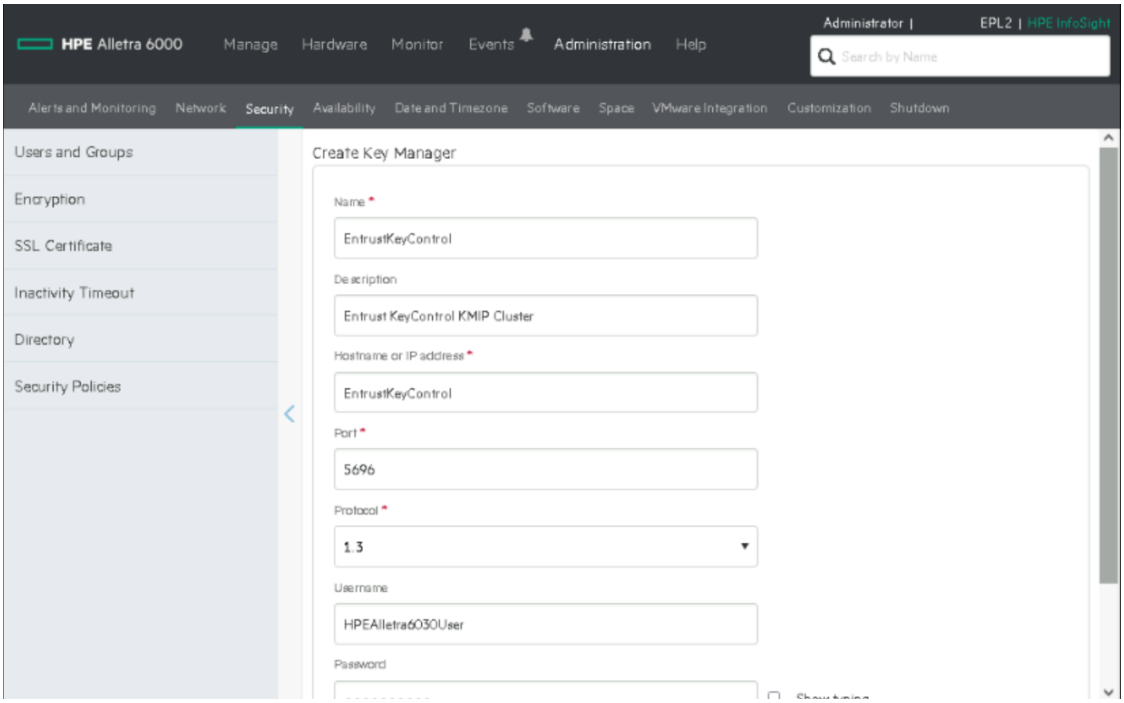
The **custom** and **custom-ca** certificates are added.



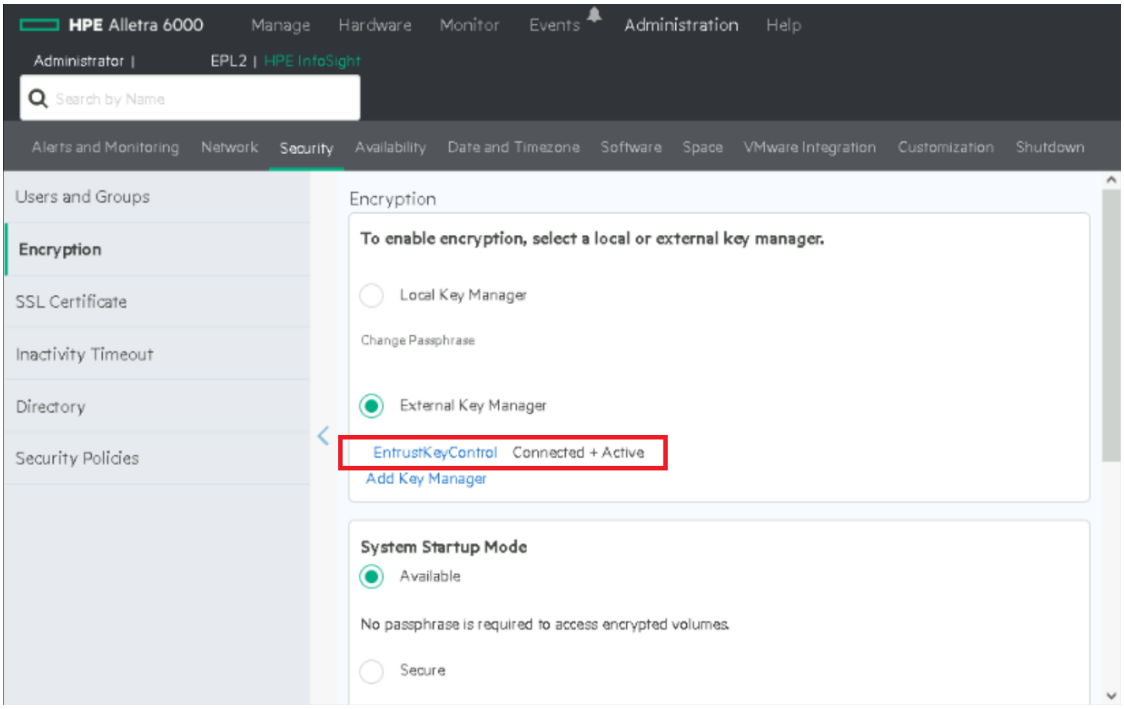
2.10. Register the Entrust KeyControl KMS

To register the Entrust KeyControl KMS:

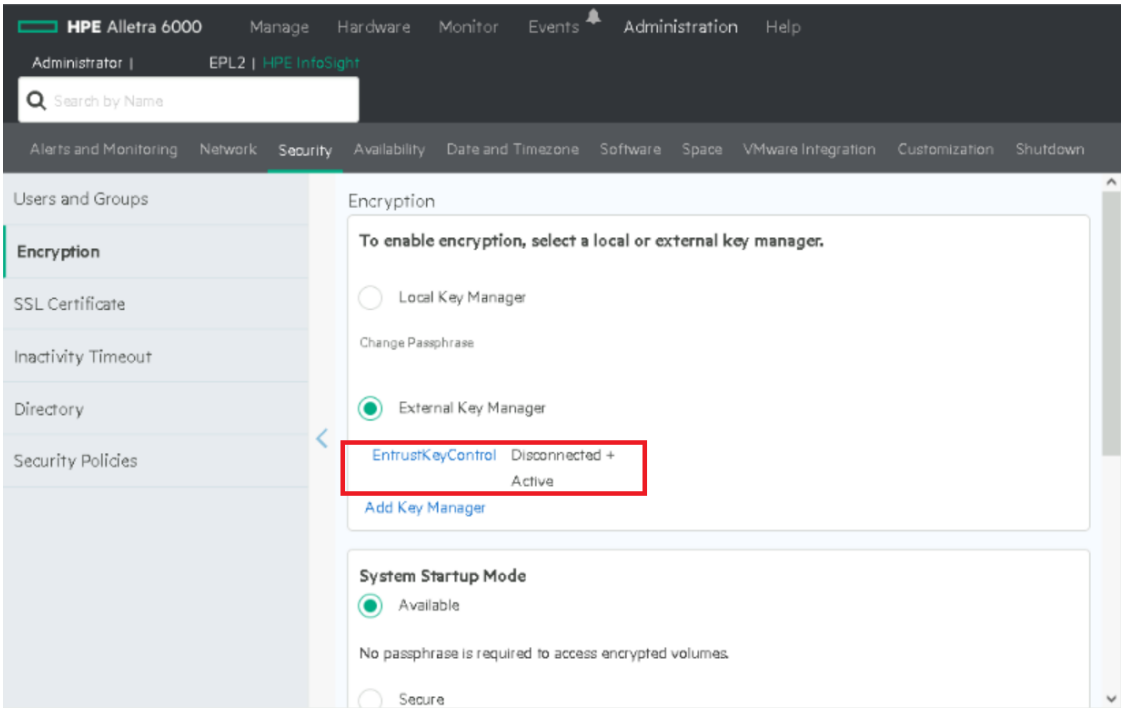
1. Log into the Alletra 6030 webGUI using an account with Security Admin privileges.
2. Select **Administration** in the toolbar. Then select **Security > Encryption**.
3. Select the **External Key Manager** radio button. Then select **Add Key Manager**.
4. Enter **Name**, **Description**, KeyControl cluster **Hostname**, and the credential for the certificate authentication in Create the tenant client certificate bundle. Then select **Save**.



The external key manager is added.



5. Power down the KeyControl nodes one at a time and verify the **External Key Manager** still shows **Connected + Active** as above.
6. Power down both KeyControl nodes and verify the **External Key Manager** shows **Disconnected + Active**.



2.11. Execute tests

Execute the test as described in the HPE Alletra internal documentation.

3. Integrating with an HSM

For guidance on integrating the Entrust KeyControl with a Hardware Security Module (HSM), consult with your HSM vendor. If you are using an Entrust nShield HSM, refer to the Entrust KeyControl nShield HSM Integration Guide available at Entrust documentation library.