HPE Alletra 5000 Storage Array

KeyControl® Integration Guide

2024-03-05

Table of Contents

Chapter 1. Introduction

This document describes the integration of the Hewlett Packard Enterprise (HPE) Alletra 5000 Storage Array (referred to as Alletra in this guide) with the Entrust KeyControl key management solution using the open standard KMIP protocol. KeyControl 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 5000 in the following configurations:

System	Version
Entrust KeyControl	10.2

1.2. Requirements

Before starting the integration process, familiarize yourself with:

- HPE Alletra online documentation
- External Key Manager Support.
- Entrust KeyControl Online Documentation Set.

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

Chapter 2. Deploy and configure Entrust KeyControl

The following steps summarize the deployment of the Entrust KeyControl:

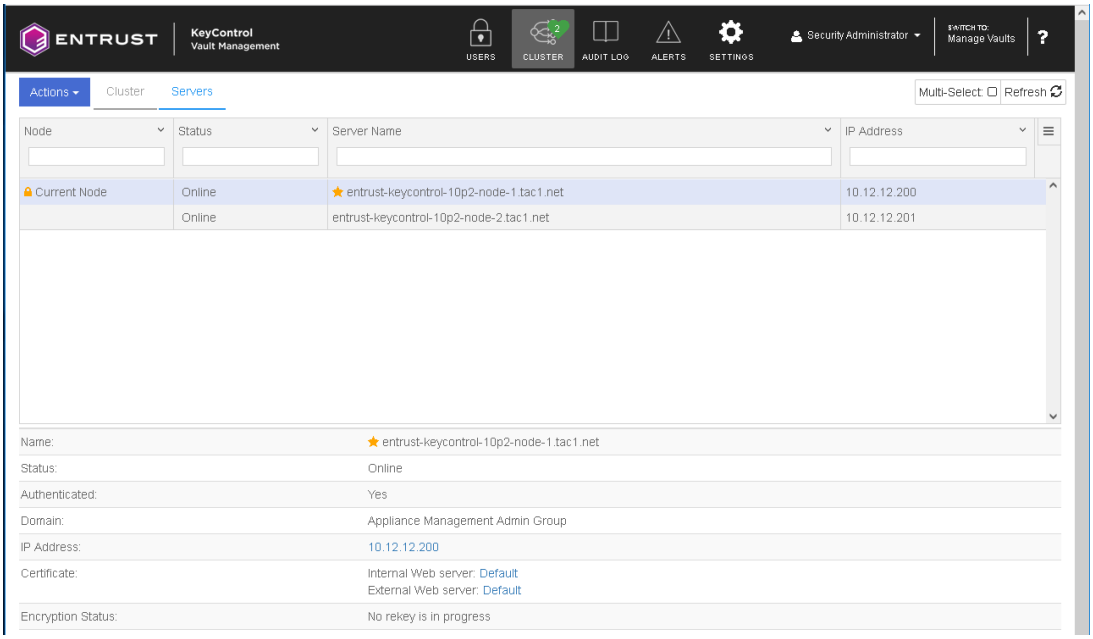
1. Deploy a Entrust KeyControl cluster
2. Additional Entrust KeyControl cluster configuration
3. Authentication
4. Create DNS record for Entrust KeyControl cluster
5. Create a KMIP Vault in the Entrust KeyControl
6. View the KMIP Vault details
7. Edit the KMIP Vault
8. Add KMIP Vault Administrators

2.1. Deploy a Entrust KeyControl cluster

This deployment consists of two nodes.

1. Download the Entrust KeyControl software from Entrust TrustedCare. 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 Entrust KeyControl as described in Entrust KeyControl OVA Installation.
3. Configure the first Entrust KeyControl node as described in Configuring the First Entrust KeyControl Node (OVA Install).
4. Add second Entrust KeyControl node to cluster as described in Adding a New Entrust KeyControl Node to an Existing Cluster (OVA Install).

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



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

2.2. Additional Entrust KeyControl cluster configuration

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

2.3. Authentication

For simplicity, 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 Entrust KeyControl cluster

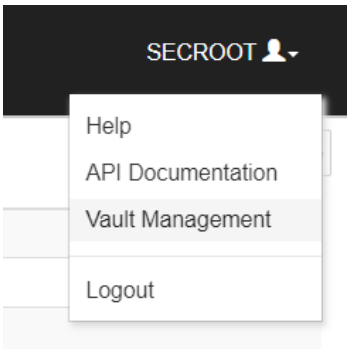
1. Create a DNS VIP record in the domain for the **Entrust KeyControl** cluster.
2. Associate all KeyControl Cluster node IPs to the DNS VIP, two in this integration..

2.5. Create a KMIP Vault in the Entrust KeyControl

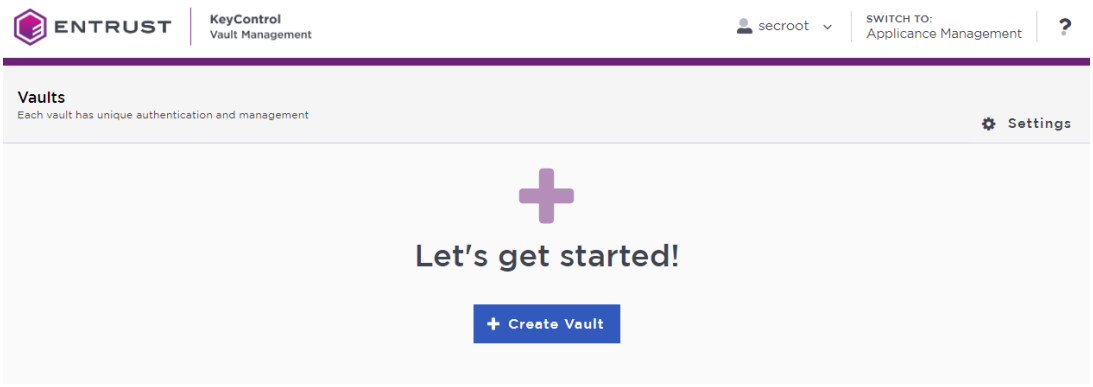
The Entrust KeyControl Vault appliance supports different type of vaults that can be used by all type of applications. This section describes how to create a KMIP Vault in the Entrust KeyControl Vault Server.

Refer to the Creating a Vault section of the admin guide for more details about it.

1. Sign in to the Entrust KeyControl Vault Server web user interface:
   a. Use your browser to access the IP address of the server.
   b. Sign in using the **secroot** credentials.
2. From the user's dropdown menu, select **Vault Management**.



3. In the Entrust KeyControl Vault Management interface, select **Create Vault**.



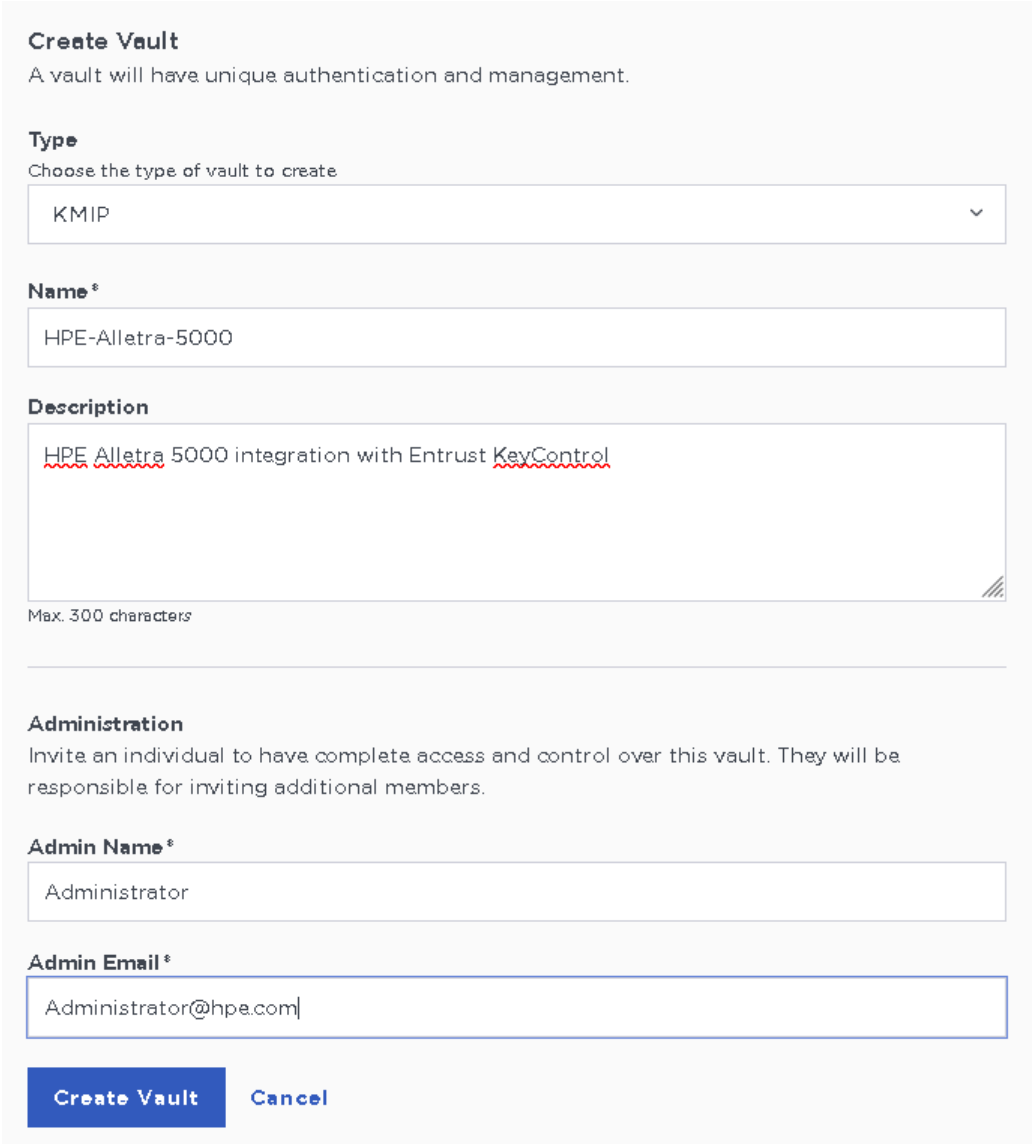
   Entrust KeyControl Vault supports the following types of vaults:

   - **Cloud Key Management** - Vault for cloud keys such as BYOK and HYOK.
   - **KMIP** - Vault for KMIP Objects.
   - **PASM** - Vault for objects such as passwords, files, SSH keys, and so on.
   - **Database** - Vault for database keys.
   - **Tokenization** - Vault for tokenization policies.
   - **VM Encryption** - Vault for encrypting VMs.

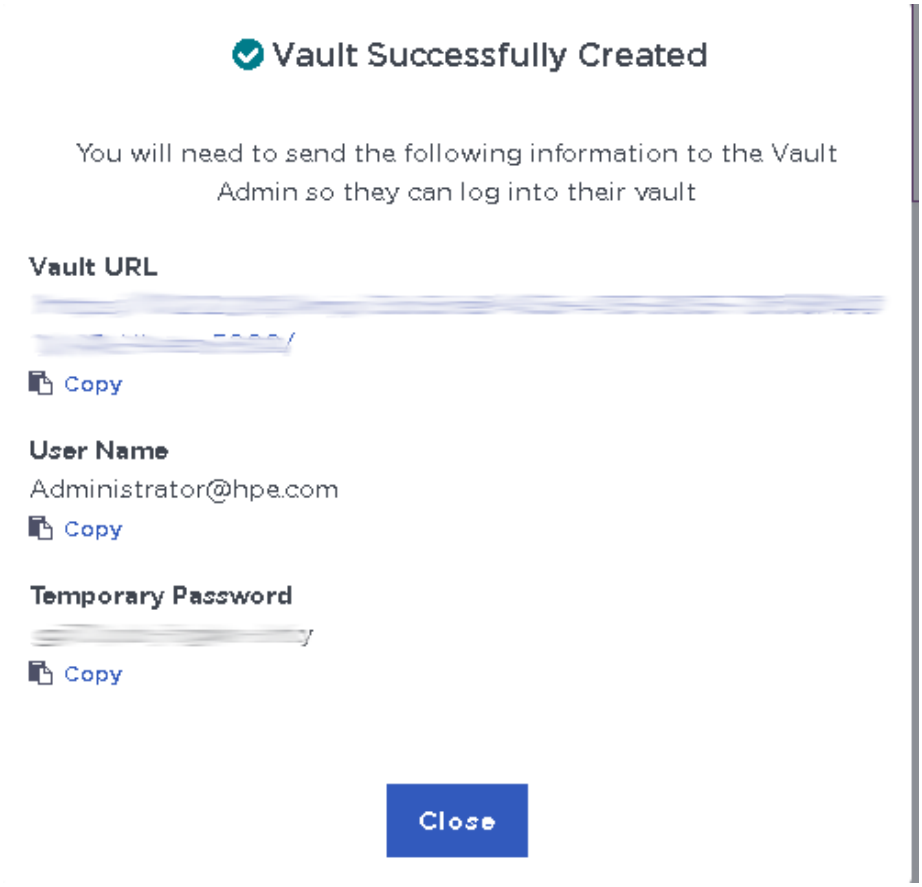
4. In the **Create Vault** page, create a **KMIP** Vault:

Field	Value
Type	**KMIP**
Name	Vault name
Description	Vault description
Admin Name	Vault administrator username
Admin Email	Vault administrator email

For example:

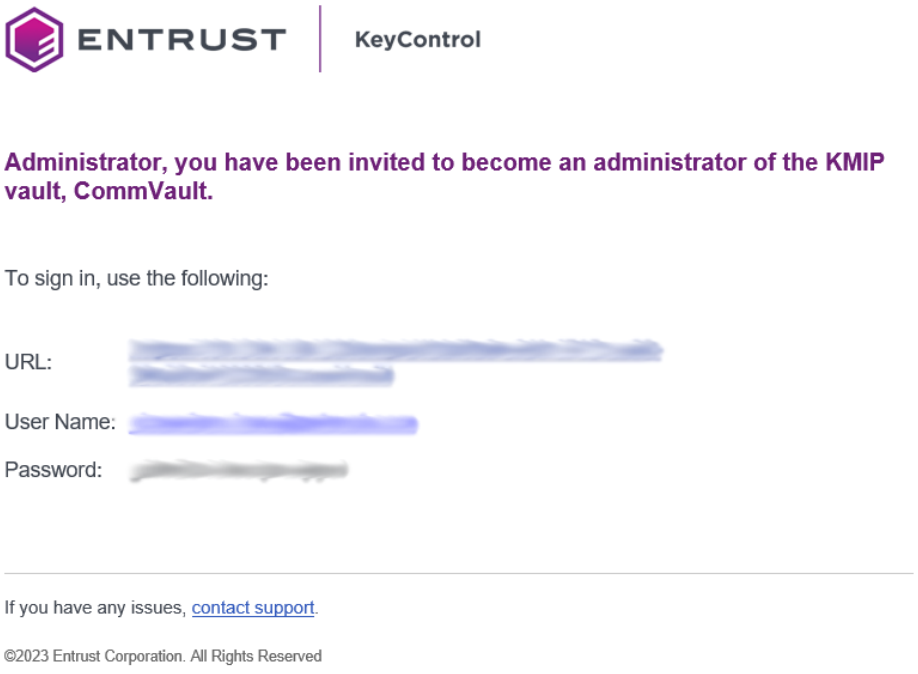


5. Select **Create Vault**. Then select **Close**.



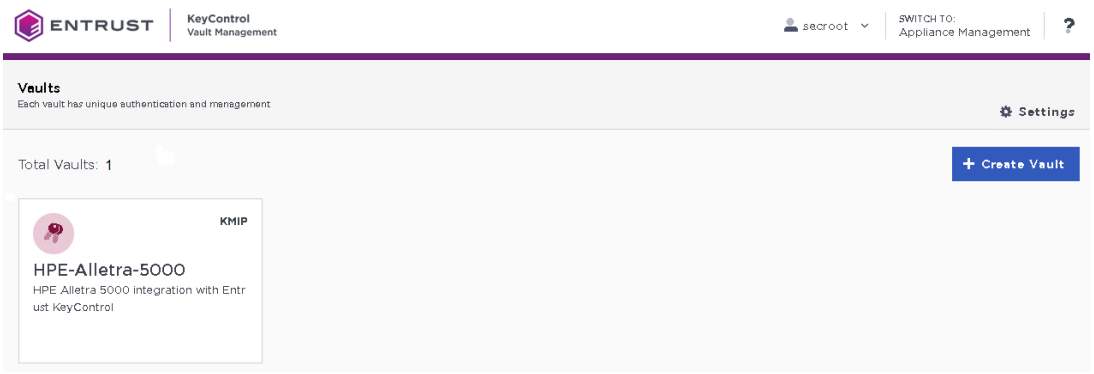
The new vault's URL and sign-in credentials will be emailed to the administrator's email address entered above. In closed gap environments where email is not available, the URL and sign-in credentials are displayed at this time.

Example email:



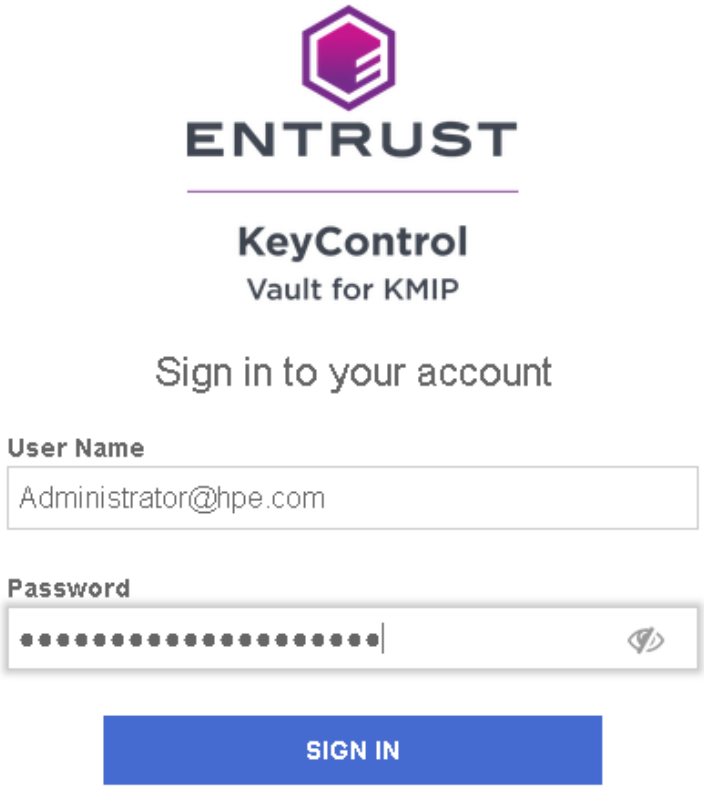
6. Bookmark the URL.
7. The newly created Vault is added to the **Vault Management** dashboard.

   For example:



8. Sign in to the URL provided above with the temporary password. Change the initial password when prompted. Sign in again to verify.

   For example:



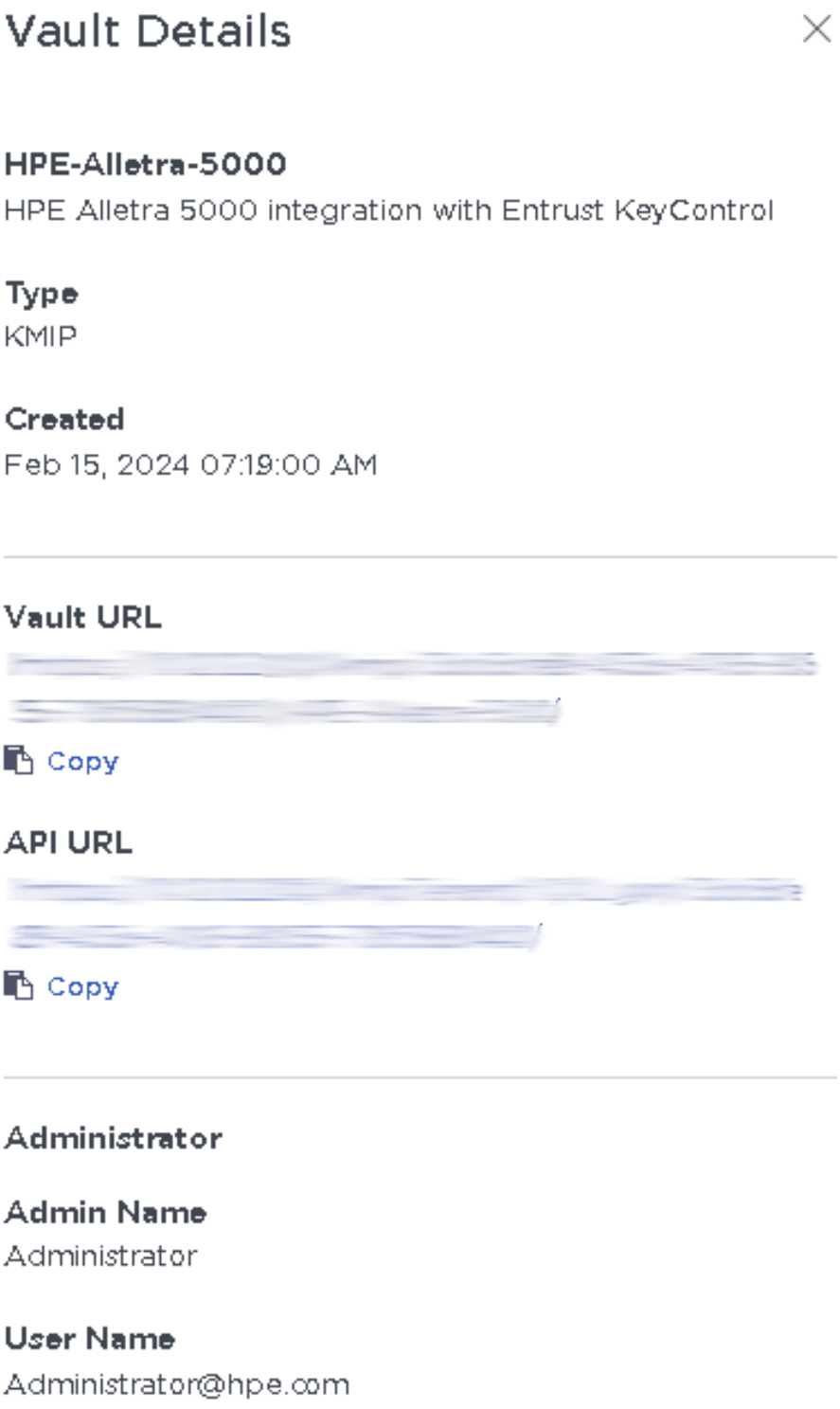
9. Notice the new vault.

   For example:

2.6. View the KMIP Vault details

1. Hover over the Vault and select **View Details**.

   For example:

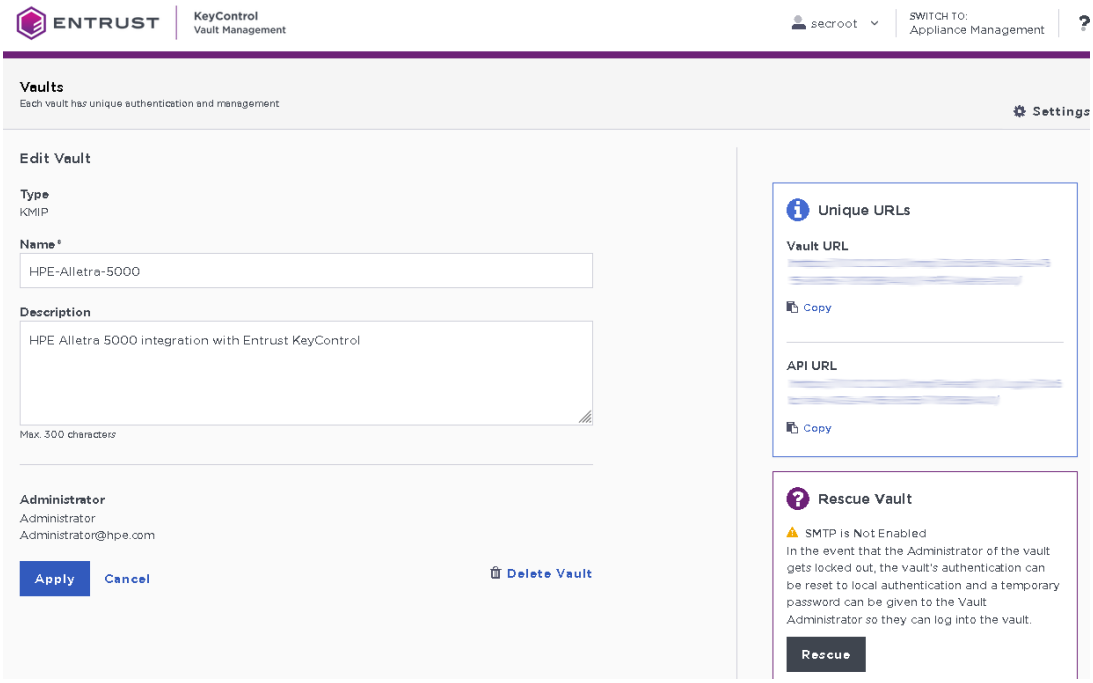


2. Select **Close** when done.

2.7. Edit the KMIP Vault

1. Hover over the vault and select **Edit**.

For example:



2. Select **Apply** when done.

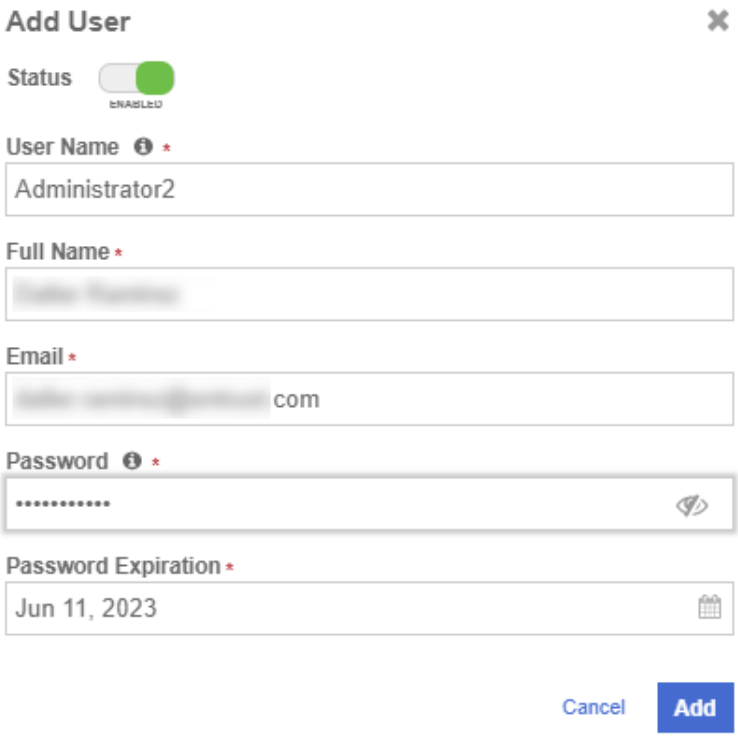
2.8. Add KMIP Vault Administrators

It is important to have other administrators set up on the Vault for recovery purposes. Add one or more admins to the Vault.

1. Select **Security > Users**.

2. In the **Manage Users** dashboard:
   a. Select the **+** icon to add one or more users.
   b. Enter the user details in the **Add User** dialog.

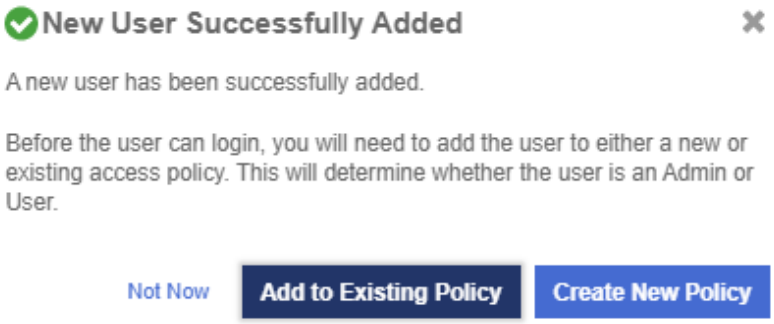
      For example:



c. Select **Add**.

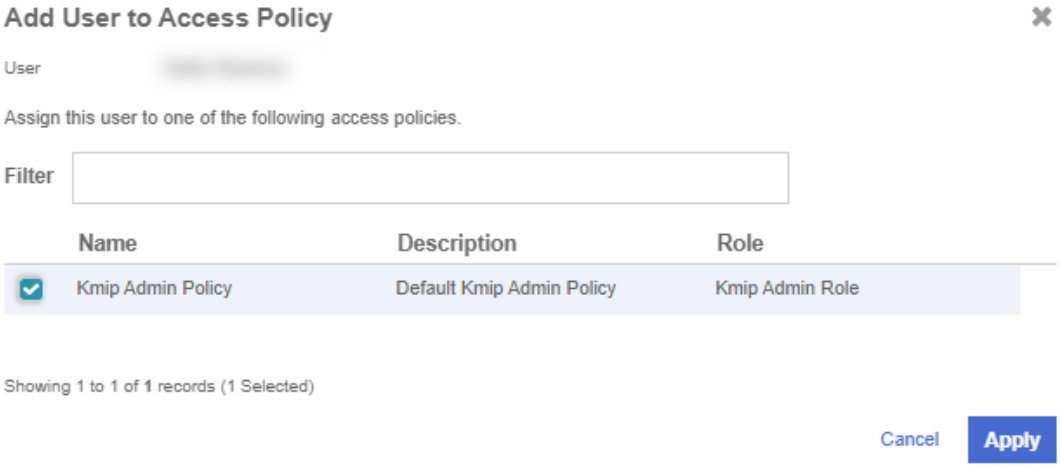
After the user is added, a window appears which requests selection of the policy to be used by this user.

3. Select **Add to Existing Policy**.



4. On the **Add User to Access Policy** dialog, select the **KMIP Admin Policy** and select **Apply**. The new user is added as an administrator to the Vault.

For example:


Add User to Access Policy
User
Assign this user to one of the following access policies.
Filter
Name
Description
Role
Kmip Admin Policy
Default Kmip Admin Policy
Kmip Admin Role
Showing 1 to 1 of 1 records (1 Selected)
Cancel
Apply

Chapter 3. Integrate Entrust KeyControl with HPE StoreOnce

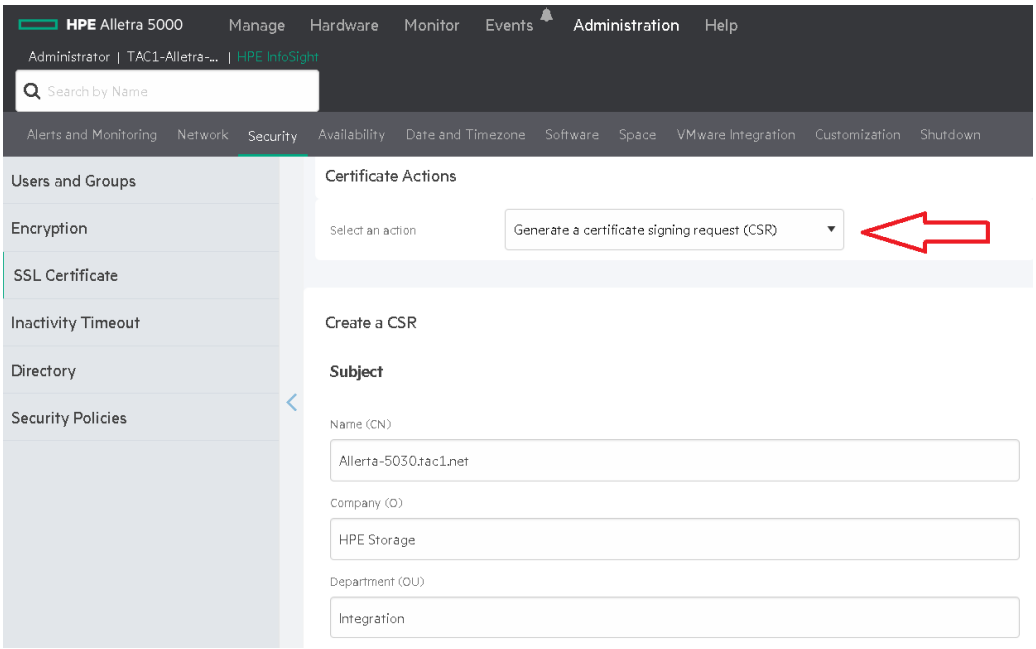
Follow these steps to register Entrust KeyControl as a KMS in HPE Alletra 5000.

Follow these steps to install and configure KeyControl.

1. Create the HPE Alletra certificate request.
2. Create the client certificate bundle.
3. Import tenant client certificate into Alletra.
4. Register the Entrust KeyControl KMS.

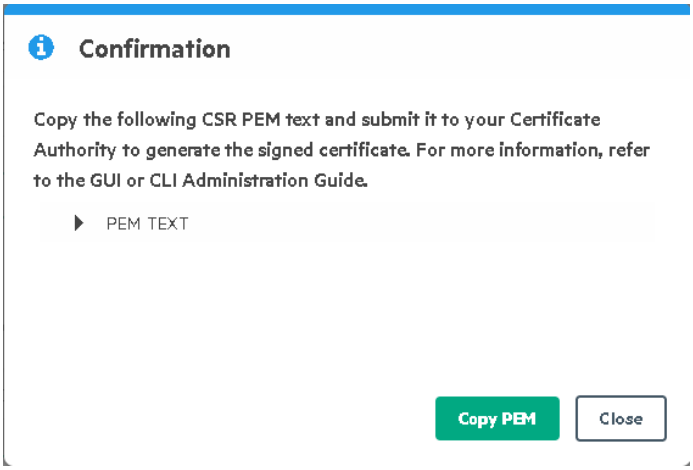
3.1. Create the HPE Alletra certificate request

1. Log into the Alletra 5030 webGUI using an account with Security Admin privileges.
2. Select **Administration** in the toolbar.
3. Select the **Security** tab and then **SSL Certificates** from he left-hand menu.
4. Select the **+** icon to add a certificate.
5. Select **Generate a certificate signing request (CSR)** from the **Select an action** drop-down list.

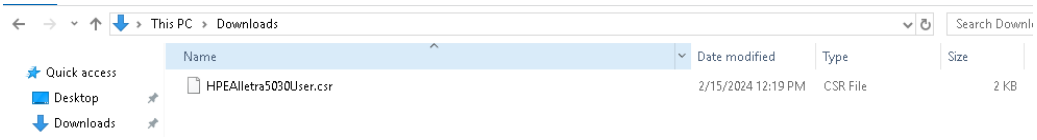


6. Enter the **Name** and other required information. You can leave all the other values as the defaults.

7. Select **GENERATE**.
8. Select **Copy PEM** in the **Confirmation** dialog.



9. Create a `.csr` file type with a text editor containing the copied certificate request. If you are using Notepad as your text editor, you might need to rename the file using the Windows CLI to get the correct file type extension.



3.2. Create the client certificate bundle

1. Sign in to the KMIP Vault with the URL and credentials from Create a KMIP Vault in teh Entrust KeyControl.
2. Select **Security**, then **Client Certificates**.

3. In the **Manage Client Certificate** page, select the **+** icon on the right to create a new certificate. The **Create Client Certificate** dialog box appears.
4. In the **Create Client Certificate** dialog box:
    a. Check **Add Authentication for Certificate**.
    b. Enter the **User Name on Certificate**.

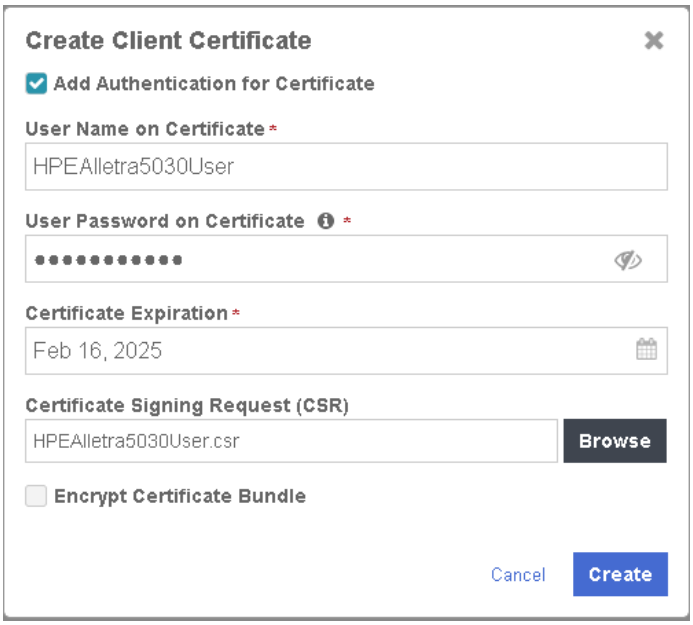
c. Enter the **User Password on Certificate**.

d. Enter the **Certificate Expiration**.

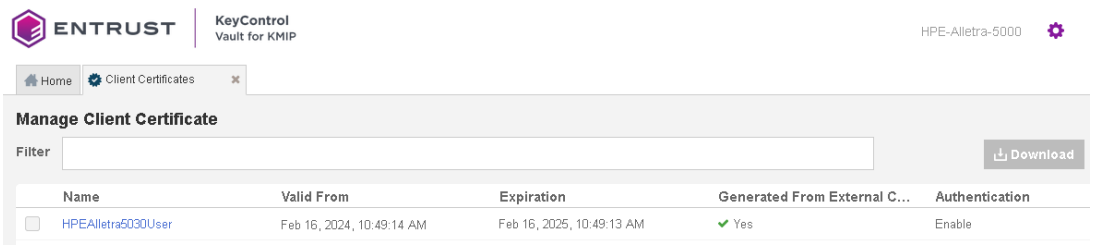
e. Upload the certificate request created in Create the HPE Alletra certificate request.

f. Select **Create**.

For example:



The new certificates are added to the **Manage Client Certificate** pane.



5. Select the certificate and select the **Download** icon to download the certificate.
6. Unzip the downloaded file. It contains the following:

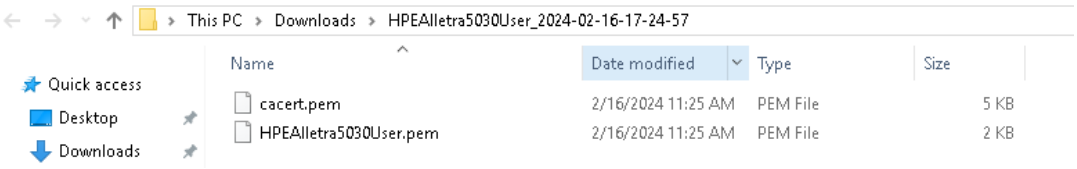
   - A `certname.pem` file that includes both the client certificate and private key. In this example, this file is called `HPEAlletra5030User.pem`.

     The client certificate section of the `certname.pem` file includes the lines `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` and all text between them.

     The private key section of the `certname.pem` file includes the lines `-----BEGIN`

`PRIVATE KEY-----` and `-----END PRIVATE KEY-----` and all text in between them.

- A `cacert.pem` file which is the root certificate for the KMS cluster. It is always named `cacert.pem`.

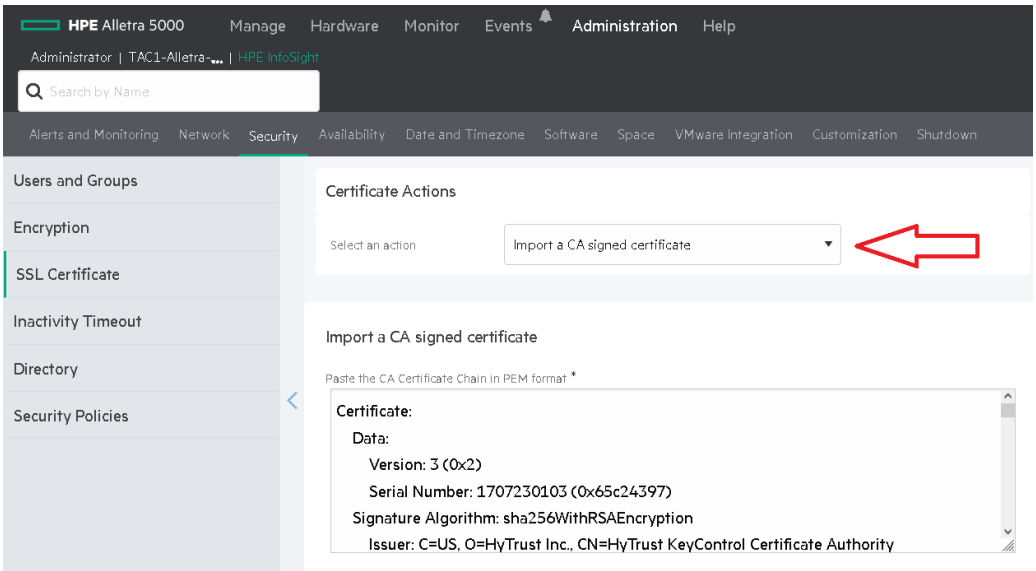


See the following link for additional information Managing KMIP Tenant Client Certificates.

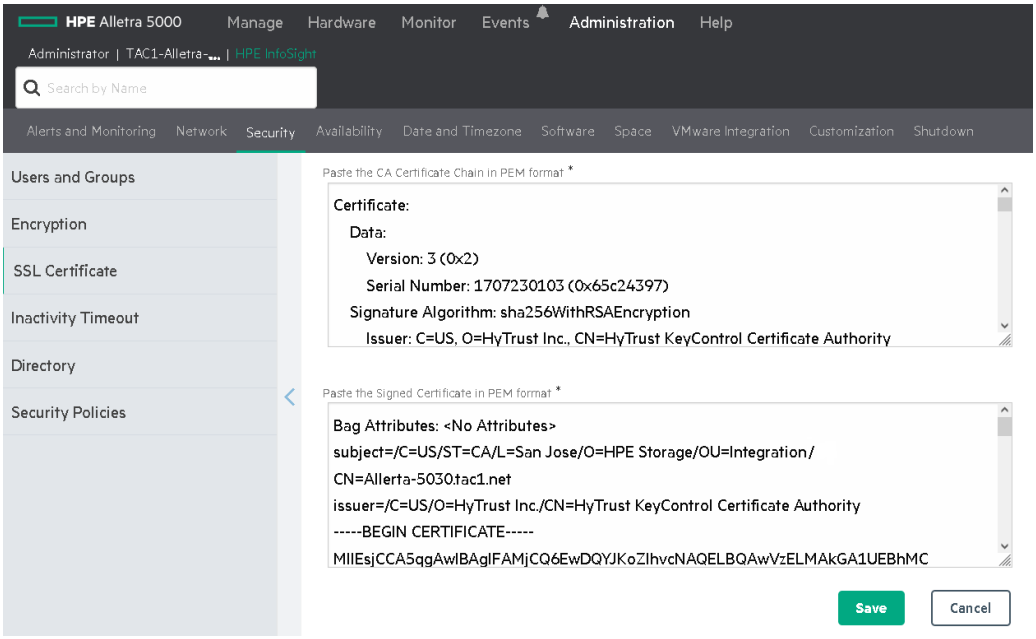
3.3. Import tenant client certificate into Alletra

To import tenant client certificate into Alletra:

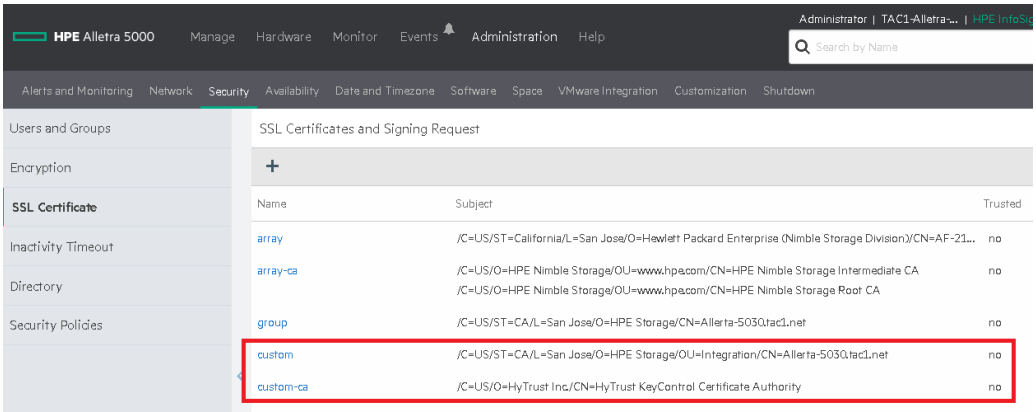
1. Log into the Alletra 5030 webGUI using an account with Security Admin privileges.
2. Select **Administration** in the toolbar. Then select **Security > SSL Certificates**.
3. Select the **+** icon to add a certificate.
4. Select **Input a CA signed certificate** in the **Select and action** drop-down text box.
5. Paste the content of the extracted `cacert.pem` file from Create the client certificate bundle in the **Paste the CA Certificate Chain in PEM format** text box.



6. Paste the content of the extracted `HPEAlletra5030User.pem` file from Create the 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.



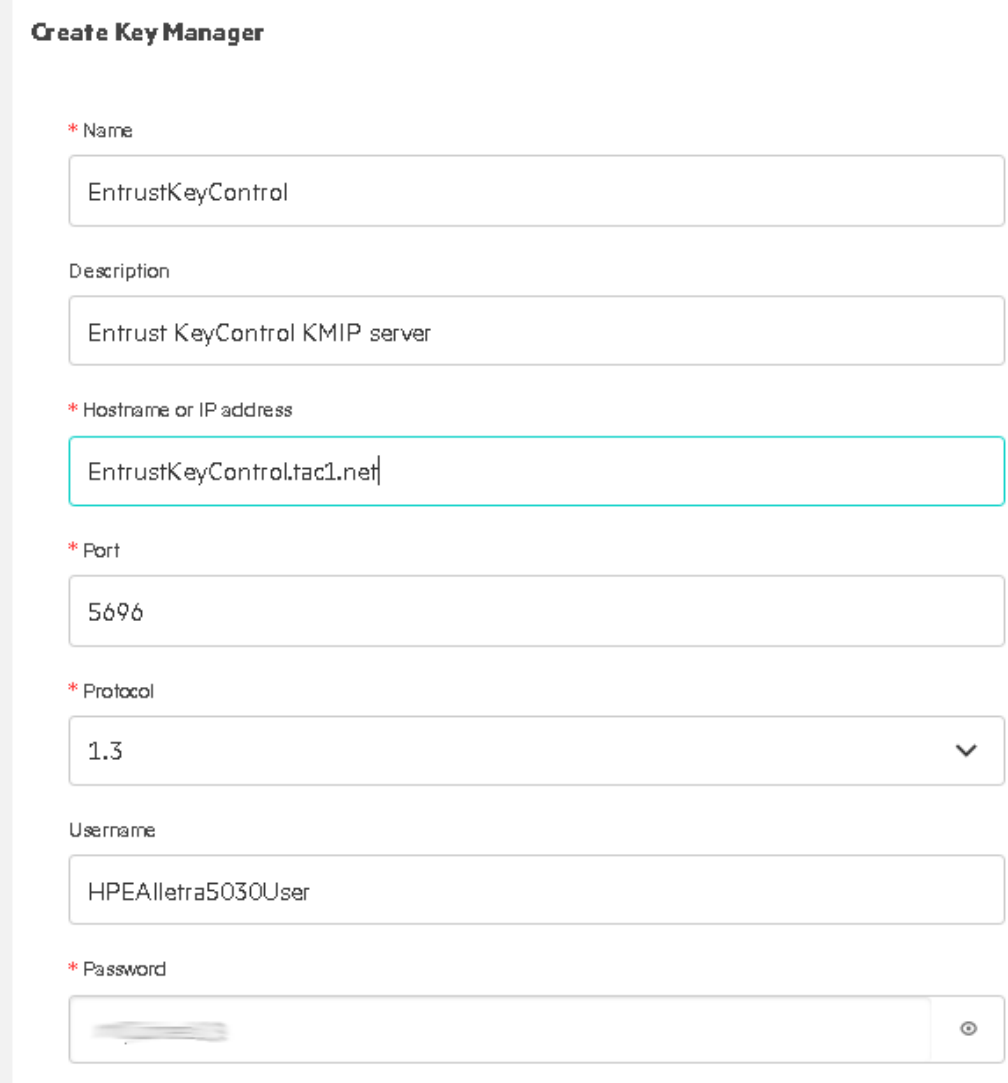
3.4. Register the Entrust KeyControl KMS

To register the Entrust KeyControl KMS:

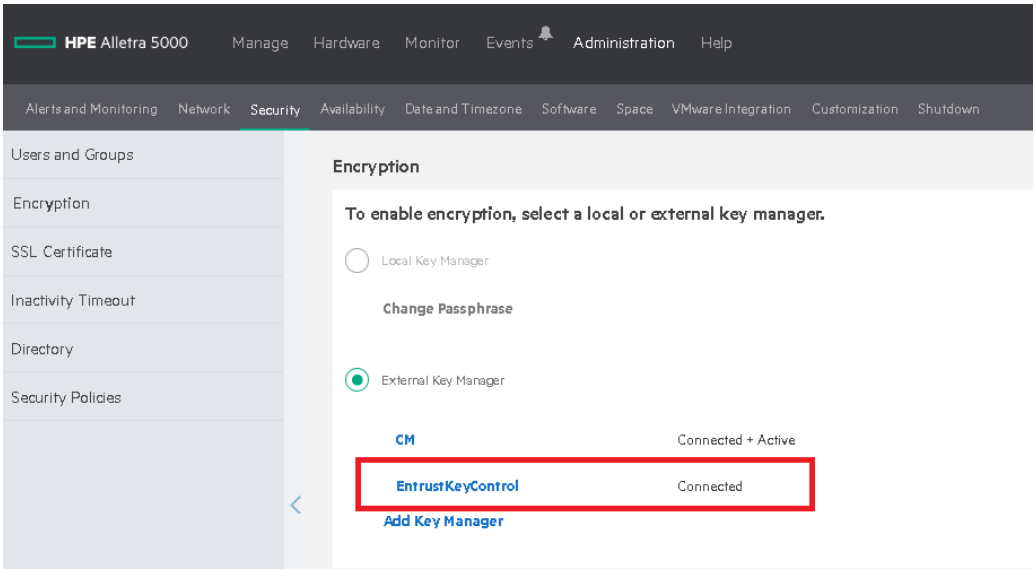
1. Log into the Alletra 5030 webGUI using an account with Security Admin privileges.
2. Select **Administration** in the toolbar. Then select **Security > Encryption**.
3. Select the **External Key Manager** radio button. Then select **Add Key Manager**.
4. Enter **Name**, **Description**, KeyControl cluster **Hostname**, and the credential for the certificate authentication in Create the client certificate bundle. Then

select **Save**.

Notice the DNS entry created in Create DNS record for Entrust KeyControl cluster in **Hostname of IP Address** text box.



The external key manager is added.


HPE Alletra 5000
Manage
Hardware
Monitor
Events
Administration
Help
Alerts and Monitoring
Network
Security
Availability
Date and Timezone
Software
Space
VMware Integration
Customization
Shutdown
Users and Groups
Encryption
SSL Certificate
Inactivity Timeout
Directory
Security Policies
Encryption
To enable encryption, select a local or external key manager.
Local Key Manager
Change Passphrase
External Key Manager
CM
Connected + Active
EntrustKeyControl
Connected
Add Key Manager

Chapter 4. Test Integration

Execute the test as described in the HPE internal documentation.

Chapter 5. 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.

Chapter 6. Additional resources and related products

6.1. Entrust products

6.2. nShield product documentation