



ENTRUST

HPE Alletra 9000 Storage Array

KeyControl[®] Integration Guide

2024-02-16

Table of Contents

1. Introduction	1
1.1. Product configurations	1
1.2. Requirements	1
2. Deploy and configure Entrust KeyControl	2
2.1. Deploy a Entrust KeyControl cluster	2
2.2. Additional Entrust KeyControl cluster configuration	3
2.3. Authentication	3
2.4. Create DNS record for Entrust KeyControl cluster	3
2.5. Create a KMIP Vault in the Entrust KeyControl	3
2.6. View the KMIP Vault details	8
2.7. Edit the KMIP Vault	9
2.8. Add KMIP Vault Administrators	10
3. Integrate Entrust KeyControl with HPE Alletra 9000	13
3.1. Create the HPE Alletra certificate request	13
3.2. Create the client certificate bundle	15
3.3. Import client certificate into Alletra	17
3.4. Register the Entrust KeyControl KMS	20
4. Test Integration	22
5. Integrating with an HSM	23
6. Additional resources and related products	24
6.1. KeyControl	24
6.2. Entrust products	24
6.3. nShield product documentation	24

Chapter 1. Introduction

This document describes the integration of the Hewlett Packard Enterprise (HPE) Alletra 9000 Storage Array (referred to as Alletra in this guide) with the Entrust KeyControl (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 9000 in the following configurations:

System	Version
Entrust KeyControl	10.2

1.2. Requirements

Before starting the integration process, familiarize yourself with:

- The documentation and set-up process for the HPE Alletra family of products in the [HPE Alletra online documentation](#).
- The documentation and set-up process for Entrust KeyControl, see the [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](#)

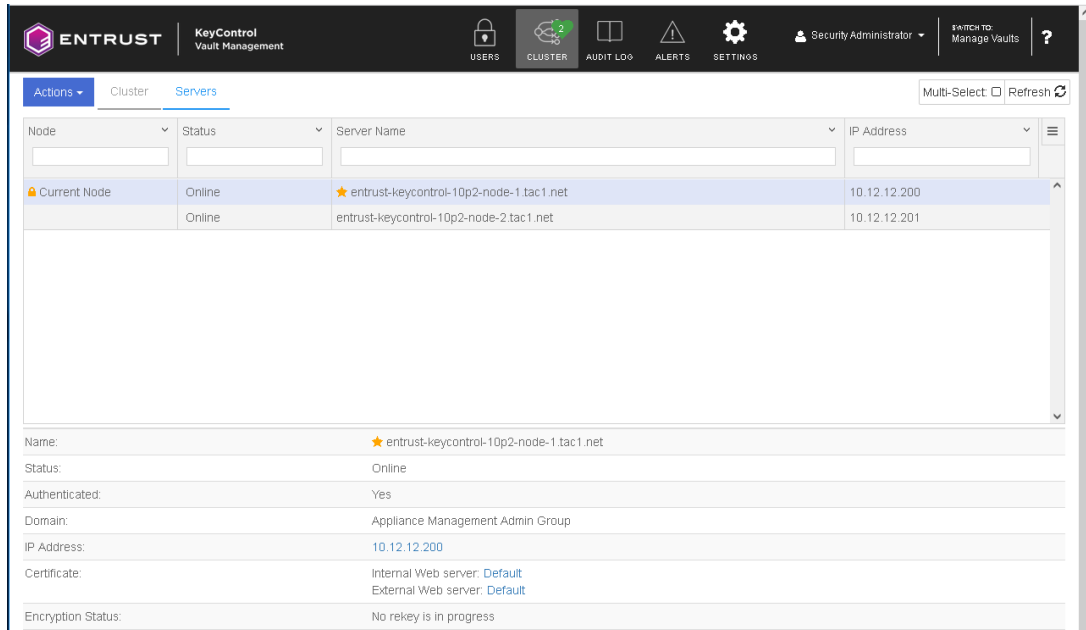
2.1. Deploy a Entrust KeyControl cluster

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. Log in 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

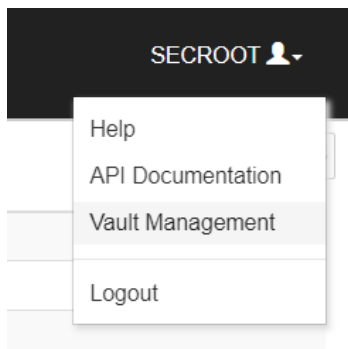
1. Create a single DNS record named **EntrustKeyControl** in the domain.
2. Assign this record as many IPs as nodes in the cluster created above, two in this integration.

2.5. Create a KMIP Vault in the Entrust KeyControl

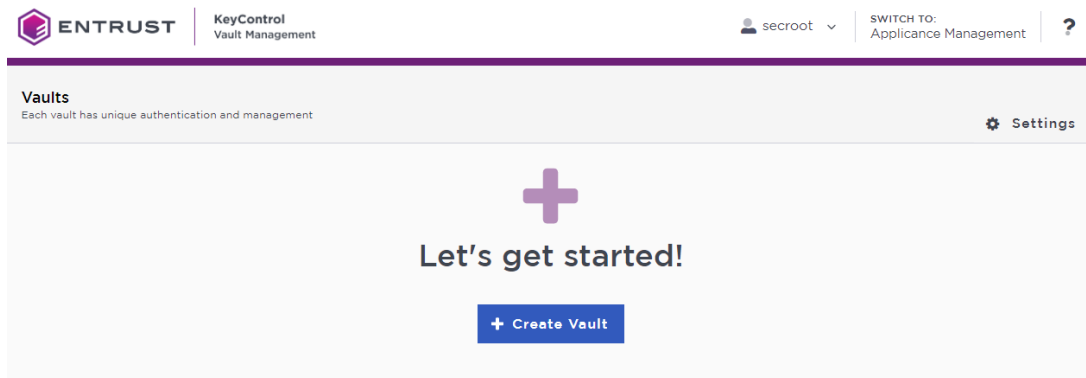
The Entrust KeyControl Vault appliance supports different type of vaults that can be used by all type of applications. This section describes how to create a KMIP Vault in the Entrust KeyControl Vault Server.

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. Select the user's dropdown menu and 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:

Create Vault

A vault will have unique authentication and management.

Type
Choose the type of vault to create

KMIP

Name*

HPE-Alletra-9000

Description

HPE Alletra 9000 integration with Entrust KeyControl

Max. 300 characters

Administration
Invite an individual to have complete access and control over this vault. They will be responsible for inviting additional members.

Admin Name*

Administrator

Admin Email*

Administrator@hpe.com

Create Vault **Cancel**

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

Vault Successfully Created

You will need to send the following information to the Vault Admin so they can log into their vault

Vault URL

<https://10.12.12.201/kmip/b7b4d2f7-1bd9-4563-8c5b-3859c8f3cc35/HPE-Alletra-9000/>

 Copy

User Name

Administrator@hpe.com

 Copy

Temporary Password

wzirIn-Eafume-mynvg8

 Copy

Close



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

Example email:

Administrator, you have been invited to become an administrator of the KMIP vault, CommVault.

To sign in, use the following:

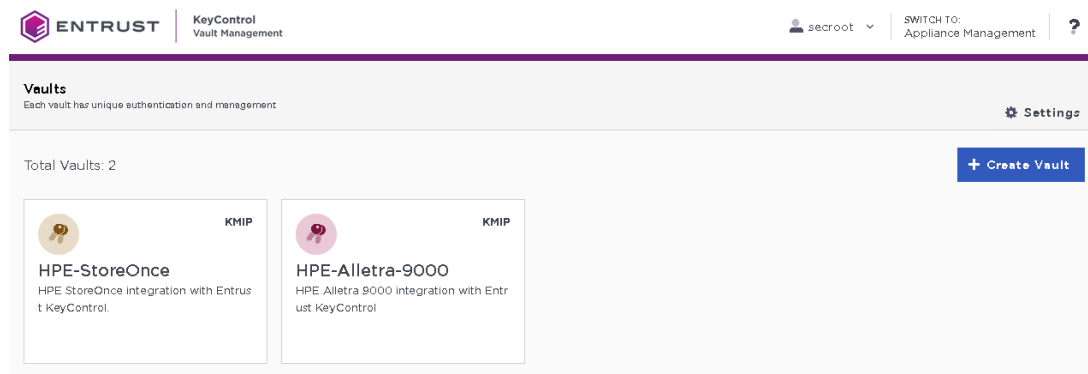
URL: 
User Name: 
Password: 

If you have any issues, [contact support](#).

©2023 Entrust Corporation. All Rights Reserved

6. Bookmark the URL and save the credentials. Then select **Close** if the URL and login credentials are displayed.
7. The newly created Vault is added to the **Vault Management** dashboard.

For example:



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

For example:



KeyControl Vault for KMIP

Sign in to your account

User Name

Password

SIGN IN

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:

Vault Details



HPE-Alletra-9000

HPE Alletra 9000 integration with Entrust KeyControl

Type

KMIP

Created

Feb 08, 2024 07:32:58 AM

Vault URL

<https://10.12.12.201/kmip/b7b4d2f7-1bd9-4563-8c5b-3859c8f3cc35/HPE-Alletra-9000/>

 Copy

API URL

<https://10.12.12.201/kmipTenant/1.0/Login/b7b4d2f7-1bd9-4563-8c5b-3859c8f3cc35/>

 Copy

Administrator

Admin Name

Administrator

User Name

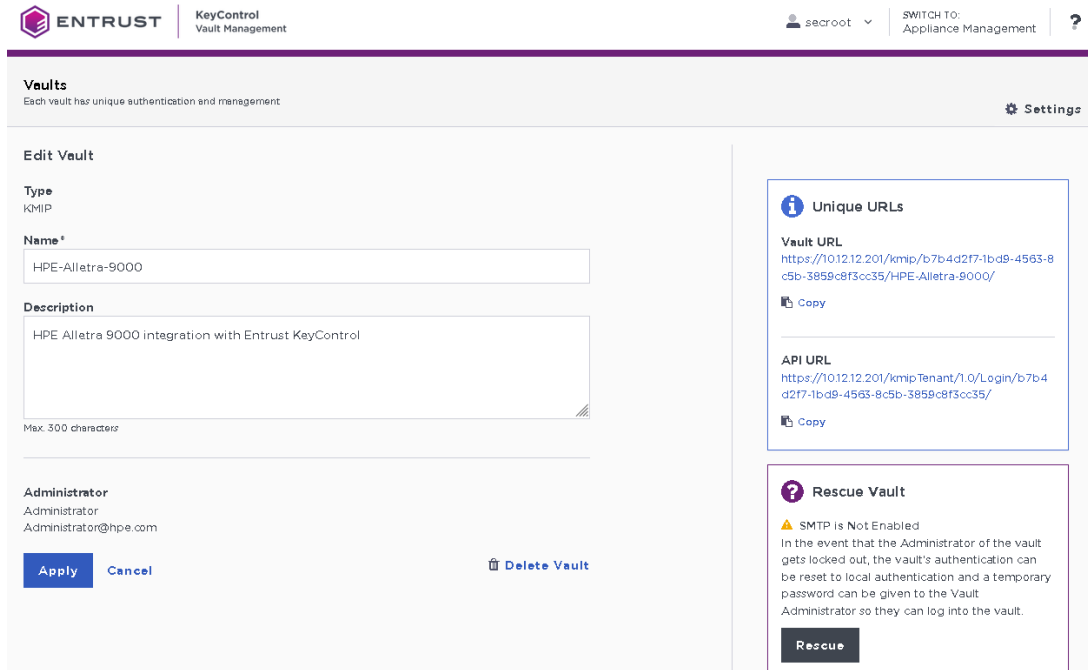
Administrator@hpe.com

2. Select **Close** when done.

2.7. Edit the KMIP Vault

1. Select **Edit** when you hover over the Vault.

For example:

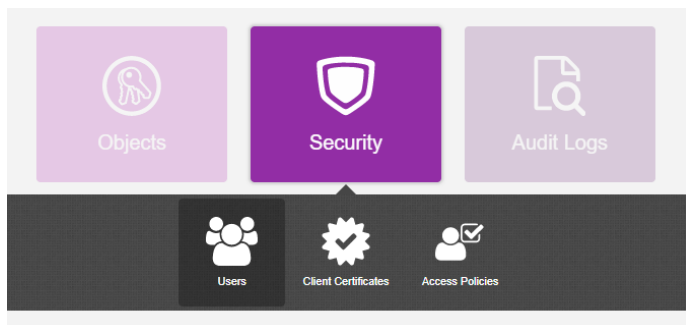


2. Select **Apply** when done.

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. Add the user by providing the information requested in the **Add User** dialog.

For example:

Add User ✕

Status ENABLED

User Name * i

Full Name *

Email *

Password * i

Password Expiration *

Cancel Add

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**.

✔ New User Successfully Added ✕

A new user has been successfully added.

Before the user can login, you will need to add the user to either a new or existing access policy. This will determine whether the user is an Admin or User.

Not Now
Add to Existing Policy
Create New 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
<input checked="" type="checkbox"/> 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 Alletra 9000

Follow these steps to register Entrust KeyControl as a KMS in HPE Alletra 9000.

1. [Create the HPE Alletra certificate request](#)
2. [Create the client certificate bundle](#)
3. [Import client certificate into Alletra](#)
4. [Register the Entrust KeyControl KMS](#)

3.1. Create the HPE Alletra certificate request

1. Sign in to the Alletra 9060 webGUI using an account with Security Admin privileges.
2. Select **Settings** in the toolbar. Then select **Array certificates**.
3. Select the **+** icon to add a certificate.
4. Select **Create a certificate signing request** for the **Certificate type**.
5. Select **ekm-client** for Array service and enter the **Common name** and other information. Then confirm the checkbox to proceed and select **Add**.

Add array certificate



Certificate type

You can create a self signed certificate from here, or you can create a certificate request that you will provide to your certificate management personnel to be signed.

Type
<input type="radio"/> Create a self signed certificate
<input checked="" type="radio"/> Create a certificate signing request

Array service

ekm-client	▼
------------	---

Certificate signing request

Key Length	▼
2048	
Common name	
HPEAlletra9060User	
Subject Alternative Name	
Example - DNS:myhost, DNS:myhostexample.com, IP:1.2.3.4	
IP:10.12.12.20	

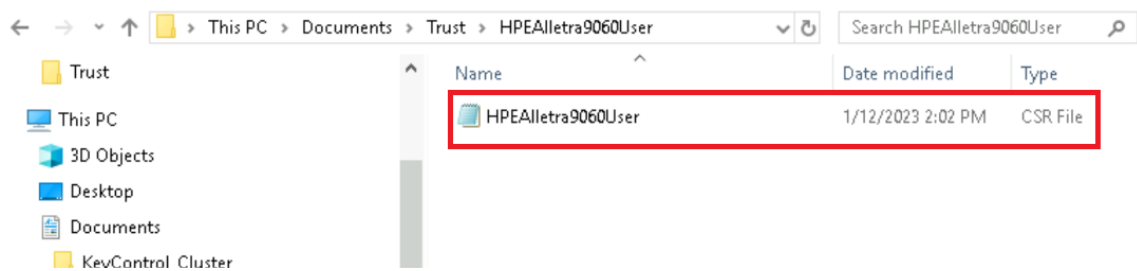
6. Select the certificate created.
7. Copy the **PEM** in the newly created certificate window.

General

Name HPEAlletra9060User
Issuer ---
Start time ---
End time ---
Subject C=US,ST=FL,L=Sunrise,O= Testing,OU=Integration,CN=HPEAlletra9060User
Subject IP Address:10.12.12.20
Alternative Name
PEM

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIC2DCCAcaACAQAwwcTELMakGA1UEBhmCvVMxCzAJBgNVBAGMAkZMMRAwDgYDVQQH  
DAdTdW5yaXNIMRAwDgYDVQQKDAUZXN0aW5nMRQwEgYDVQQLDAtJbnRlZ3JhdGlv  
bjEibGkGA1UEAwwSSSFBFQWxsZXRYytKWNBVc2VYMIIBJjANBgkqhkiG9w0BAQEFA  
AAOCAQ8AMIIBCgKCAQEAA2WEXf1+8hQRenCYNH1ng5dxrxUrdfxPULhsOoBtCx  
Oj1B6dfSiC9uTxRIPYQHQuvSTCU6BQLRrhHjfpb4iXSh8UBENvx7L5rn0tRpph3  
gS0mdMi3mBEtFUN+PzcKplbYl8vm75DQOId+wl3qQ/7reaYQSQh0JwQZV9n3dpJ  
9jdPLjN0ybe1KAlAehqwhxho9u+o+eJrGPPIZG30roKsQu1rJZgK2xtvSszil0q  
2ms8FPnJOILRqUlfvGlu6uTbvYkm4dZJORLZKa4DuEUHJlCs1SU+hzRhThGPMt  
F4O+6U1EfeDDyImytTnaDKkDWNvVrLdGxWKixdYMKQIDAQABoClwIAYJKoZIhvdn  
AQkOMRMwETAPBgNVHREECDAGhwQKDAwUMAOGCSqGSiB3DQEBCwUAA4IBAQAWitX.1  
71hYaOpTb2TRgWXMdTzwSRyMZbTKyKUALG/O67WLUkM1Wa9k8S9hLrCZDR5erTSu  
dRz1NtXIZZ5tuOKd3DpavkZozqPpeRf1Mf5gqDJb918S2Vz5tkUyvwgpgWY9WUPs  
2uWzkGna3A4XyYyOX9WOv9EVpW00yWvb7UfBILpDj74OpTHrv1Gg/2Cj1DqP9  
ZHRMotply9v22BJrGzLen5EGey2FzKVxMrQNywNYItgYRgRpGSam2XRlnKQvrfLB  
vx125ML28KDtL0ZojH47m5QplQtHBAW/kAdmBhtHXWnBWSyWV9PtDuE6e3C1hjzn  
tNr2dX7ugdli5M9X  
-----END CERTIFICATE REQUEST-----
```

8. Create a `csr` file type with a text editor containing the copied certificate request. May need to rename the file using the Windows CLI to get the correct file type extension if using Notepad text editor.



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 the 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.

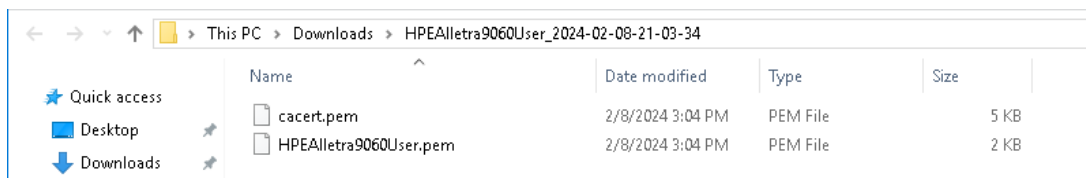


5. Select the certificate and select the **Download** icon to download the certificate.
6. Unzip the downloaded file. It contains the following:
 - A **certname.pem** file that includes both the client certificate and private key. In this example, this file is called **HPEAlletra9060User.pem**.

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 client certificate into Alletra

1. Sign in to the Alletra 9060 webGUI using an account with Security Admin privileges.
2. Select **Settings** in the toolbar. Then select **Array certificates**.
3. Select the certificate that was created in [Create the HPE Alletra certificate request](#). Then select **Import Signed CSR** in the **Actions** tab.

← Array certificate HPEAlletra9060User



Actions

Import Signed CSR

Delete

General

```

Name HPEAlletra9060User
Issuer
Start time
End time
Subject C=US,ST=FL,L=Sunrise,O=Testing,OU=Integration,CN=HPEAlletra9060User
Subject Alternative Name IP Address:10.12.12.20
PEM -----BEGIN CERTIFICATE REQUEST-----
MIIC2DCCACAAQAwcTELMakGA1UEBhMCVVMx: CzAJBgNVBAGwMAKZMMRAwDgYDVQQH
DAAdTdw5yaXNIMRAwDgYDVQQKDAUZXNOaW5nMRQwEgYDVQLDA1JbnRIZ3JhdGlv
bjEbmBkGA1UEAwwSSFBFQWxsZXRyYTkwnJbVc2VyMlIiBjANBgkqhkiG9wOBAQE
AAOCAQ8AMIIBCgKCAQEAE2WEXtf1+8hQRenCYNH1ng5dxrxUrdfxPUlhzsOoBtC
Oi1B6dfSiC9uTxRIPYQHOUkvSTCU6BQLRrhHjfb4iXSh8UBENx7L5mOfRpph3
gSQmdMi5mBEtfUN+PzdK:CplbYl8vm75DQOid+wl3qO/7reaYQSQhQUwQZV9n3dpJ
9jdPLjNOybe1KAIAehqwhxho9u+o+eJrGPPIZG3OroK:sxQu1rJZgk2xtvSszilOq
2ms8FPhJOILRqUIFvGlu6uTbvYkm4dZJORLZKa4DuEUHJrIcs1SU+hzRhThGPMT
F40+6U1EfeDDylmyrTnaDKKdWNvVrLdgaWK:bdYMKQIDAQABoClwIAYJKoZIhvdN
AQkOMRMwETAPBgNVHREECDAGhwQKDAwLMAOGCSqGSIb3DQEBCwUAA4IBAQAWhX1
71hYaOpTb2TRgWXMdZzwSRyMZbTKyKUALG/O67WLUkM1Wa9k8S9hLrCZDR5erTSu
cRz1NTXiZZ5tuOKd3DpapvKZoaPpeRf1Mf5ggDjB918S2Vz5tKUYvwgpGWY9WUPs
2uWzkGna3A4XyYyOX9WObv9EVpWOOyWvb7UfBLLpJdJ74OpTHrv1Gg/2Cj1DqPz
ZHRMotpIY9v22BJrGzLen5EGey2FzKvXMrQNYwNYHtYRgRpGSan2XRlnKQvrfLB
vx125ML28KDrLOZojH47m5QplQIHBAW/kAdmBhHtXWnBWSyWV9PHDuE6e3C1jhzn
tNr2dX7ugdi5M9X
-----END CERTIFICATE REQUEST-----

```

- Paste the content of the extracted `cacert.pem` file from [Create the client certificate bundle](#) in the **Authority chain** text box. When pasting the content, only include the certificate section of the file starting from **-----BEGIN CERTIFICATE-----** and ending with **-----END CERTIFICATE-----**.
- Paste the content of the extracted `HPEAlletra9060User.pem` file from [Create the client certificate bundle](#) in the **Certificate** text box. Only paste the certificate section starting from **-----BEGIN CERTIFICATE-----** and ending with **-----END CERTIFICATE-----**. Then select **Add**.

Import Signed CSR

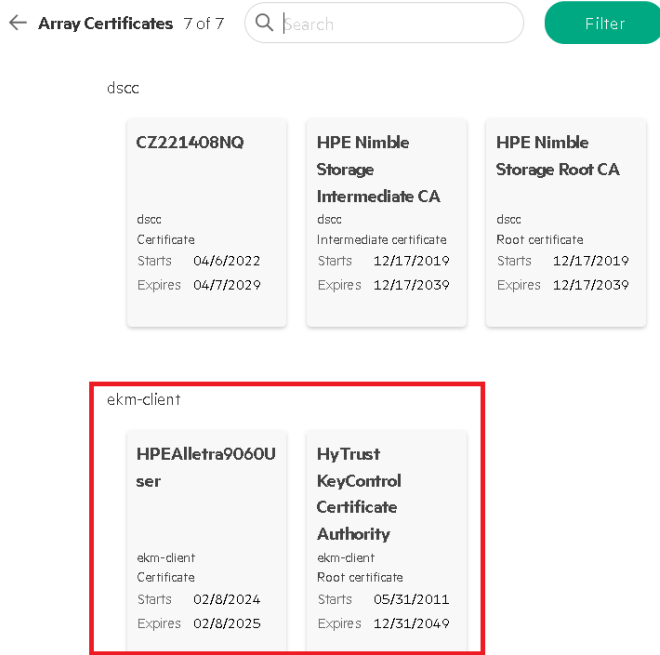


```
Certificate
-----BEGIN CERTIFICATE-----
MIID1TCCAr2gAwIBAgIFAMjCQ5swDQYJKoZIhvcNAQELBQAwVzELMAkGA1UEBhMC
VVMxFTATBgNVBAoTDEh5VHJ1c3QgSW5jLjExMC8GA1UEAxMoSHIUCnVzdCBLZXID
b250cm9sENlcnRpmjYXRlIEF1dGhvcmlOeTAeFwOyNDYyMDgyMTAwMDNaFwOy
NTAyMDgyMTAwMDNaMHEXChZAJBgNVBAYTAiVTMQswCQYDVQQIDAJTDEQMA4GA1UE
BwwHU3VucmlzZTEQMA4GA1UECgwHVGVzdGluZzEUMBIGA1UECwwwLSW5OZWdyYXRp
b24xGzAZBgNVBAMMEkhQRUFsbGVOcmE5MDYwVXNlcjCCASlwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBANiHF7X9fvIUExpwDR9Z4OXca8cVK3X8T1JYc7DqAbQ
sTofQenXOogvbk8USD2EBOFJLOkwI0GUCC0a4R436W+IIOofFARDb8ey+a59LUaaY
d4E1JnTH5gRLX1Dfj83CgqZW2JfL5u+QODpXfsCN6jv+63mmEEkldCCEGVfZ93a
SfY3Ty4zdMm3ISgCAHoaslcYaPbvqPniaxjzyGRt9K6CrMULtayWYCTsbBOrM4pd
KtprPBT5yTpSOalJRbxburk272JJuHWSTkS2SmuA7hFBYsa5QrNUIPocOYU4Rjz
```

```
Authority chain
-----BEGIN CERTIFICATE-----
MIID9TCCAIt2gAwIBAgIEZcJlZANBgkqhkiG9w0BAQsFADBxMQswCQYDVQQGEwJV
UzEVMBMGA1UECHMmSHIUCnVzdCBLZXJmMTUwYVZlYVZlYVZlYVZlYVZlYVZlYVZl
bnRyb2wgQ2Y2YVZlYVZlYVZlYVZlYVZlYVZlYVZlYVZlYVZlYVZlYVZlYVZlYVZl
MTIzMTIzNTk1OVoVzELMAkGA1UEBhMCVVMxFTATBgNVBAoTDEh5VHJ1c3QgSW5j
LjExMC8GA1UEAxMoSHIUCnVzdCBLZXIDb250cm9sENlcnRpmjYXRlIEF1dGhvc
cmI0eTAeFwOyNDYyMDgyMTAwMDNaFwOyNTAyMDgyMTAwMDNaMHEXChZAJBgNVBAYT
A1VTMQswCQYDVQQIDAJTDEQMA4GA1UECgwHVGVzdGluZzEUMBIGA1UECwwwLSW5O
ZWdyYXRpb24xGzAZBgNVBAMMEkhQRUFsbGVOcmE5MDYwVXNlcjCCASlwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBANcZrAHKfBw4oVUa
UVwU7EBvCtbTd2WDWSIMm5c4InQ/opDxeJIACTh7AetdKBDvE541N3Q+pkgYF7Y+
+uthaLQfy9xn652dORTVcWS6iEKqwxFQDIqYx1HwGSCAm3b/Njhj/EIK7xL5PsUv
rAZWesXznzCJHyvYOrms5ffb5cm00us9na63JVEUSMJJ0ooUkOnQLOA2qIDHDzzHs
SANDAy4XbhQyikt5laOGsBU7bnSHQ69l480FeatpmNily4e01GrNa6d3PyNNGNW6
m9cseUf4QRS/fPaMWbbuBF0cLbabIRkuMubI4LE6n4if4BlbAx05f2y5JX09BhNi
```

Add

6. Check **I have read and understand the implications**. Then select **Add**.
7. Notice the new status of the **Certificate** along with the **Root Certificate** now showing up beside our created certificate.



8. Launch the Alletra 9060 CLI using an account with Security Admin privileges.

```
Microsoft Windows [Version 10.0.17763.5329]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ssh 3paradm@10.12.12.20
The authenticity of host '10.12.12.20 (10.12.12.20)' can't be established.
RSA key fingerprint is SHA256:e1K15j9xCCcQyuMTV4h0cCIW25boA9jypH1tJzAbB5I.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.12.12.20' (RSA) to the list of known hosts.
3paradm@10.12.12.20's password:
TAC1-Alletra-9060 cli%
```

9. Verify that the certificates were created with the `showcert` command.

```
TAC1-Alletra-9060 cli% showcert
Service      Commonname                                     Type  Enddate      Fingerprint
ekm-client   HPEAlletra9060User                            cert  Feb  8 21:00:03 2025 GMT
88b2042086346406396f6a347172aa1e52ba54ac
ekm-client*  HyTrust KeyControl Certificate Authority rootca Dec 31 23:59:59 2049 GMT
ed1e2e09efe0ef77c7546afa8b58adcba2575222
ekm-server*  HyTrust KeyControl Certificate Authority rootca Dec 31 23:59:59 2049 GMT
ed1e2e09efe0ef77c7546afa8b58adcba2575222
```

3.4. Register the Entrust KeyControl KMS

1. Launch the Alletra 9060 CLI using an account with Security Admin privileges.

```
Microsoft Windows [Version 10.0.17763.5329]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ssh 3paradm@10.12.12.20
The authenticity of host '10.12.12.20 (10.12.12.20)' can't be established.
```

```
RSA key fingerprint is SHA256:e1K15j9xCcCQyuMTV4h0cCIW25boA9jyph1tJzAbB5I.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '10.12.12.20' (RSA) to the list of known hosts.  
3paradm@10.12.12.20's password:  
TAC1-Alletra-9060 cli%
```

2. Create an **External Key Manager Server** with the `controlencryption setekm` command in the CLI.



Notice the IP of all the nodes in the Entrust KeyControl cluster.

```
TAC1-Alletra-9060 cli% controlencryption setekm -setserver 10.12.12.200,10.12.12.201 -port 5696 -ekmuser  
HPEAlletra9060User -kmipprotocols 1.3  
Password for EKM user:
```

3. Verify that the external key manager has been created with the `controlencryption status -d` command.

```
TAC1-Alletra-9060 cli% controlencryption status -d  
Licensed Enabled BackupSaved State SeqNum Keystore FIPS non-SEDS FailedDisks nodeNonSED  
yes no no normal 0 --- --- 0 0 0  
  
Number of EKM servers defined: 1  
EKM servers: EntrustKeyControl.tac1.net  
EKM server port: 5696  
EKM username: HPEAlletra9060User  
KMIP Protocols: 1.3
```

4. Verify communication with the newly created External Key Management server with the `controlencryption checkekm` command to show that **EKM settings are correct**.

```
TAC1-Alletra-9060 cli% controlencryption checkekm  
EKM settings are correct.
```

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. KeyControl

6.2. Entrust products

6.3. nShield product documentation