



# HPE Alletra 6000 Storage Array

**KeyControl® Integration Guide** 

21 Apr 2023

 $\ensuremath{\textcircled{\sc c}}$  2023 Entrust Corporation. All rights reserved.

## Contents

1. Introduction
1.1. Product configurations
1.2. Requirements
2. Procedures
2.1. Deploy a KeyControl cluster
2.2. Additional KeyControl cluster configuration
2.3. Authentication
2.4. Create DNS record for KeyControl cluster
2.5. Enable KMIP
2.6. Create tenant
2.7. Create the HPE Alletra certificate request
2.8. Create the tenant client certificate bundle
2.9. Import tenant client certificate into Alletra
2.10. Register the Entrust KeyControl KMS 11
2.11. Execute tests
3. Integrating with an HSM

## 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/softwaredownloads. 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.

<b>(</b> entrust	KeyControl		WORKLOADS CLOUDKEYS	VANULT AUDIT LOG		KMIP SETTINGS	ECROOT 👤 -
Actions - Cluster	Servers					Multi-Select	t: 🗆 Refresh 🕽
Node 🗸	Status ~	Server Name			`	P Address	~ =
Current Node	Online	★ entrust-kc-10-node	e-1.epl2.net				^
	Online	entrust-kc-10-node-2	.epl2.net				
							v
Name:		🚖 entrust-kc-10	)-node-1.epl2.net				
Status:		Online					
Authenticated:		Yes					
Domain:		KeyControl Adr	nin Group				
IP Address:							
Certificate:		Internal Web se External Web s 92023 E	erver: Default erver: Default intrust Corporation, All Rights Re	eserved.			

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**.

$\leftarrow$ $\rightarrow$ C $\textcircled{a}$	○ 🔒 https://10.11.11.200/#I/kmip/server		80% 🟠	$\bigtriangledown$ $\checkmark$ $\blacksquare$ $\equiv$
	COS CONSTRUCTION CLUSTER WORKLOARDS CLUBIO			SECROOT &+
Actions -	ENABLED	~		
Host Name:	10.11.11.200			
Port:	5696	0		
Auto-Reconnect:	OFF	~		
Verify	Yes	~		
Certificate Type:	Default	~		
Non-blocking I/O: (9)	No	~		
Timeout:	Infinite			
Log Level	CREATE-MODIFY	~		
Restrict TLS:	DISABLED	~		
	Connections will use TLS 1.2 if set to Enabled.			
SSL/TLS Ciphers: •	ECDHE-RSA-AES128-GCM-SHA258,ECDHE-RSA AFS258-GCM-SHA398 +CDHF-FCDSA-AES128- 80227 EParto Convertion of Bit	hts Reserved		

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.

		Create a KMIP Tenant	×
About	Authentication	Admin	
Name the r Name * 🚯	new tenant. This na	me will not be editable once the tenant is created.	
HPE-Alle	tra-6000		
Description	1		
HPE Alle	tra 6000 Integratior	n with the Entrust <u>KeyControl</u> 10	//.
Cancel			Next

- 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.

		Create a KMIP Tenant	×
About	Authentication	Admin	
Administr	ator		
User Name	nitiai tenant admini	strator who will have administrative access to the lenant si	te.
HPE Alletr	aAdmin		
Full Name			
HPE Allet	ra Administrator		
Email			
HPE.Allet	ra.Admin@epl2.net		
Password	0		
Define a tei	mporary password fo	r this administrator.	
•••••	••••		9D
Password	Expiration		
02/12/20	23	前	
Cancel			reate

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.

	DASHBOARD		CLUSTER		CLOUDKEYS	() VAULT	AUDIT LOG	ALERTS	() KMIP	SETTINOS	SECROOT 👤 -
Actions -											
Name:		HPE-Alletr	a-6000								
Description:		HPE Alletr	a 6000 Int	egration with	Entrust Key	Control 10					
Admin Name:		HPE Alletr	a Administ	rator							
Admin User Name:		& HPEAIle	etraAdmin (	Reset Passwor	£)						
Admin Email:		HPE.Alletr	a.Admin@	epl2.net						_	
Tenant Login: 🕚		/kmipui/7a	83ec7f-64	8b-4216-92	a8-a586f2db	718e/HPE-	Alletra-6000/	Copy URI	<		
Tenant API URL: ()		/kmipTena	int/1.0/Log	in/7a83ec7f-	648b-4216-9	2a8-a586	f2db718e/	Copy URL			
Authentication Type:		Local									

B

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** dropdown text box.
- 5. Enter the **Name** and other required information. All defaults were selected in this integration. Then select **GENERATE**.

HPE Alletra 6000 Manage	Hardware Monitor Events <sup>🌲</sup> Adm	inistration Help	Administrator   Q Search by Name	EPL2   HPE InfoSight
Alerts and Monitoring Network Security				
Users and Groups	Certificate Actions			^
Encryption	Select an action	Generate a certificate signing request (CSR)		- I
SSL Certificate				-
Inactivity Timeout	Create a CSR			
Directory	Subject			
Security Policies	Name (CN)			
	HPEAIletra6030User			
	Company (O)			
	Nimble Storage			~

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

#### Confirmation

Copy the following CSR PEM text and submit it to your Certificate Authority to generate the signed certificate. For more information, refer to the GUI or CLI Administration Guide.

PEM TEXT

Сору РВМ	Close

 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**.

Create Client Certificate		×
🗹 Add Authentication for Certificate		
User Name on Certificate *		
HPEAlletra6030User		
User Password on Certificate 👩 *		
*******		S)
Certificate Expiration *		
Dec 19, 2023		<u></u>
Certificate Signing Request (CSR)		
HPEAlletra6030User.csr		Browse
Encrypt Certificate Bundle		
	Cancel	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.

HPE Alletra 6000 Manage	Hardware Monitor Events <sup>A</sup> Administration Help	Administrator   EPL2   HPE Info Q Search by Name	oSight
Alerts and Monitoring Network Security			
Users and Groups	Select an action Import a CA signed certificate	•	^
Encryption			
SSL Certificate	Import a CA signed certificate		
Inactivity Timeout	Paste the CA Certificate Chain in PEM format *		
Directory	Certificate: Data:	î	
Security Policies	Version: 3 (0x2)		
	Signature Algorithm: sha256WithRSAEncryption Issuer: C=US, O=HyTrust Inc., CN=HyTrust KeyControl Certificate Authority	<b>*</b>	~

 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.

HPE Alletra 6000 Manage	Hardware         Monitor         Events         Administration         Help         Q         Search by Name	EPL2   HPE InfoSight
Alerts and Monitoring Network Securi	ry Availability Date and Timezone Software Space VMware Integration Customization Shutdown	
Users and Groups	Signature Algorithm: sha256WithRSAEncryption Issuer: C=US, O=HyTrust Inc., CN=HyTrust KeyControl Certificate Authority	× ^
Encryption	Paste the Signed Certificate in PEM format *	
SSL Certificate	Bag Attributes: «No Attributes»	^
Inactivity Timeout	subject=/C=US/ST=CA/L=San Jose/O=Nimble Storage/CN=HPEAlletra6030User issuer=/C=US/O=HyTrust Inc/CN=HyTrust KeyControl Certificate Authority	
Directory		
Security Policies	VVMxFTATBgNVBAoTDEh5VHJ1c3QgSW5jLjExMC8GA1UEAxMoSHiUmVzdCBLZXID	× ///
	Sav	/e Cancel

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

HPE Alletra 6000 Managi				Administratic	<b>n</b> Help		Administrator   EPL2 Q Search by Name	HPE InfoSight
Alerts and Monitoring Network Sec	urity	Availability Date ar	id Timezone	Software Space	VMware Integration	Customization	Shutdown	
Users and Groups		SSL Certificates an	d Signing R	equest				
Encryption	<	+						
SSL Certificate		Name		Subject				Trusted
Inactivity Timeout		array		/C=US/ST=Califor	nia/L=San Jose/O=Hew	dett Packard Enterp	prise (Nimble Storage Division)/CN=AF-23	no
Directory		array-ca		/C=US/O=HPE Nimble Storage/OU=www.hpe.com/CN=HPE Nimble Storage Intermediate CA /C=US/O=HPE Nimble Storage/OU=www.hpe.com/CN=HPE Nimble Storage Root CA				no
Security Policies		group		/C=US/ST=CA/L=San Jose/O=Nimble Storage/CN=Alletra6030-1.epl2.net				no
	Γ	custom	stom /C=US/ST=CA/L=San Jose/O=Nimble Storage/CN=HPEAIletra6030User				no	
	L	custom-ca		/C=US/0=HyTrus	t Inc./CN=HyTrust KeyC	ontrol Certificate A	Authority	no

#### 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.
- Enter Name, Description, KeyControl cluster Hostname, and the credential for the certificate authentication in Create the tenant client certificate bundle. Then select Save.

HPE Alletra 6000 Manage	e ⊦	Hard	tware Monitor Events <sup>&amp;</sup> Administration Help	Administrator   Q Search by Name	EPL2   HPE InfoSight
Alerts and Monitoring Network Secu	irity	Ava	eilability Date and Timezone Software Space VMware Integration	n Customization Shutdown	
Users and Groups		Cr	eate Key Manager		î
Encryption	<		Name *		
SSL Certificate			EntrustKeyControl		
Inactivity Timeout			Description		
Directory			Entrust KeyControl KMIP Cluster		
Security Policies			EntrustKeyControl		
			Port*		
			5696		
			Protocol *		
			1.3 *		
			Uærname		
			HPEAlletra6030User		
			Password	Show trains	

The external key manager is added.



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

HPE Alletra 6000 Manage	Hardware Monitor Events 🌲 Administration Help	
Administrator   EPL2   HPE InfoSi	ght .	
Q Search by Name		
Alerts and Monitoring Network Seourity	Availability Date and Timezone Software Space VMware Integration Customization Shutdown	
Users and Groups	Encryption	î
Encryption	To enable encryption, select a local or external key manager.	
SSL Certificate	Local Key Manager	
Inactivity Timeout	Change Passphrase	
Directory	External Key Manager	
Security Policies	EntrustKeyControl Disconnected +	1
	Add Key Manager	
	System Startup Mode	
	Available	
	No passphrase is required to access encrypted volumes.	
	Secure	~

#### 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.