



# VMware vSphere and Entrust KeyControl

#### **Integration Guide**

2024-04-19

 $\ensuremath{\mathbb{C}}$  2024 Entrust Corporation. All rights reserved.

### Table of Contents

1. Introduction
1.1. Documents to read first
1.2. Product configuration
1.3. Requirements
2. Procedures
2.1. Prerequisites
2.2. Create the KMS cluster in vCenter
2.3. Establish a trusted connection between the KMS cluster and the
Entrust KeyControl server
2.4. Enable Encryption for virtual machines
2.5. Enable Data-At-Rest encryption on an existing vSAN cluster
3. Additional resources and related products
3.1. Video
3.2. nShield Connect
3.3. nShield as a Service
3.4. KeyControl
3.5. Entrust digital security solutions
3.6. nShield product documentation

### **Chapter 1. Introduction**

This guide describes the integration of the Entrust KeyControl Key Management Solution (KMS) with VMware encryptions solutions, vSAN, and VM encryption. Entrust KeyControl can serve as a KMS in vCenter using the open standard Key Management Interoperability Protocol (KMIP).

#### 1.1. Documents to read first

This guide describes how to configure the Entrust KeyControl server as a KMS in vCenter.

To install and configure the Entrust KeyControl server as a KMIP server, see the following documents:

- *Entrust KeyControl nShield HSM Integration Guide*. You can access it from the Entrust Document Library and from the nShield Product Documentation website.
- KeyControl with VSAN and VMware vSphere VM Encryption.

Also refer to the following documents in the VMware online documentation:

- Using Encryption in a vSAN Cluster.
- Virtual Machine Encryption.

#### 1.2. Product configuration

Product	Version
VMware vSphere	7.0, 8.0
KeyControl	10.0

#### 1.3. Requirements

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

### Chapter 2. Procedures

#### 2.1. Prerequisites

- Entrust KeyControl has been deployed and configured.
- VMware vSphere has been deployed and configured using vCenter.
- You have administrator rights to manage the KMS configuration in vCenter.

#### 2.2. Create the KMS cluster in vCenter

For more detail on how to do this, see Adding a KMS Cluster in vSphere in the Entrust online documentation.

- 1. Launch the vSphere Web Client and log into the vCenter server that you want to add to Entrust KeyControl.
- 2. Select the required vCenter Server in the **Global Inventory Lists**.
- 3. Select the **Configure** tab.
- 4. In the left-hand pane, select **Security > Key Providers**.
- 5. Select Add Standard Key Provider.
- 6. In the **Add Standard Key Provider** dialog, set the following configuration options:
  - $\circ~$  For Name, enter the name of the cluster.
  - For each node in the KeyControl cluster, enter the KMS (node name), IP
     Address and Port. The default port is 5696.



Make sure that the KMIP server resides on a device that is not encrypted using the KeyControl cluster. The KMIP server must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.

To add an extra node line, select Add KMS.

Add Star	ıdard Key F	Provider			×
Name	KeyControl				
KMS		Address	P	ort	
Keycontrol 1		10.194.	5	5696	$\otimes$
Keycontrol 2		10.194.	Ę	5696	$\otimes$
ADD KMS					
> Proxy con	figuration (optional)				
> Password	protection (optional)	)			
		CANCEL	ADD KE		DER

- Open and set **Proxy Configuration** if you are using a proxy.
- **Password protection** is optional.
- 7. Select Add Key Provider.
- 8. In the **Make vCenter Trust Key Provider** dialog, confirm the details for each node and then select **Trust**. For example:

lode 1	
Serial number	OXAO8E6
> Subject	keycontrol-10-1. com
> Issuer	HyTrust KeyControl Certificate Authority
Valid from	05/31/2011, 8:00:00 PM
Valid to	12/31/2049, 6:59:59 PM
Fingerprint	A8:1D:CD:5F:4D:F4:9A:FC:E1:A8:9D:D1:2D:E D:3C
> Certificate	Expand to view details
Serial number	0xD090
> Subject	keycontrol-10-2com
> Issuer	HyTrust KeyControl Certificate Authority
Valid from	05/31/2011, 8:00:00 PM
Valid to	12/31/2049, 6:59:59 PM
Fingerprint	E5:53:8F:DD:65:06:17:10:4C:

This adds the KMS cluster to vCenter but the connection status will be **KMS not connected** with **Certificate issues**. For example:

Key Providers		
ADD STANDARD KEY PROVIDER	MAKE DEFAULT EDIT REMOVE	
Key Provider	↑ Connection Status	Certificates
C KeyControl (default)	⚠ 2 KMS not connected	⚠ 2 certificate issue(s)
		1 items

## 2.3. Establish a trusted connection between the KMS cluster and the Entrust KeyControl server

To establish a trusted connection between the KMS cluster and the Entrust KeyControl server:

- 1. Continuing from the previous section, select the KeyControl KMS cluster in the list, then scroll down to where the nodes are displayed.
- Select one of the nodes, then select on Establish Trust > Make KMS trust vCenter. For example:

Summary Monitor	Configure Permissions Data	acenters Hosts	s & Clusters VMs	Datastores	Networks	
Settings V	Key Providers					
Licensing	ADD STANDARD KEY PROVIDER	MAKE DEFAU	LT EDIT REMO	VE		
Message of the Day	Key Provider	↑ Con	nection Status	c	ertificates	
Authentication Proxy	• KeyControl (default)	:	2 KMS not connected	4	2 certificate issue(s	)
vCenter HA						
Security 🗸						1 items
Trust Authority						
Key Providers	Provider KeyControl - Key Man	agement Serve	rs			
Scheduled Tasks	ESTABLISH TRUST Y					
Storage Providers	KMS trust vCenter	Port	Connection Status	vCenter Ce	rtificate KMS Certi	ficate
vSAN V	Make KMS trust vCenter	.1 5696	🗥 Client trusts ser	/ 🛆	🔗 Valid	until: Dec 31,
Update Internet Connectivity	Upload Signed CSR Certificate	. 5696	\land Client trusts serv	/ 🛆	⊘ Valid	until: Dec 31,
	vCenter Trust KMS					
	Make vCenter Trust KMS					
	Upload KMS Certificate					2 items

 In the Choose method pane of the Make KMS Trust vCenter dialog, select KMS certificate and private key.

Make KMS trust vCenter	Choose a method Choose a method to make the KMS trust the vCenter based on the KMS vendor's	×
1 Choose a method	requirements. Once the trust is established, all replicas in the same KMS cluster will also trust the vCenter.	
2 Establish Trust		
	🔿 vCenter Root CA Certificate	
	Download the vCenter root certificate and upload it to the KMS. All	
	certificates signed by this root certificate will be trusted by the KMS.	
	🔿 vCenter Certificate	
	Download the vCenter certificate and upload it to the KMS.	
	<ul> <li>KMS certificate and private key</li> </ul>	
	Upload the KMS certificate and private key to vCenter.	
	O New Certificate Signing Request (CSR)	
	Submit the vCenter-generated CSR to the KMS then upload the new KMS-	
	signed certificate to vCenter.	
	CANCEL NEXT	

- 4. Select Next.
- 5. In the **Upload KMS Credentials** pane of the **Make KMS Trust vCenter** dialog, you need to upload the certname.pem file created during the certificate creation process described in the Entrust KeyControl nShield Integration guide. This file needs to be uploaded for the KMS certificate, and then uploaded again for the private key. To do this:
  - For KMS certificate, select Upload file. Then select the certname.pem file and select Open.
  - For Private key, select Upload file. Then select the certname.pem file again and select Open.
  - Select Establish Trust.

KMS Certificate Bag Attributes localKeyID: 69 28 D7 B7 D0 1C 03 E8 4E 36 F5 65 71 4A E1	UPLOAD A FILE
(MS Private Key Bag Attributes Jocaliwardh: 69 28 D7 B7 D0 10 03 58 45 36 55 45 71 46 51	UPLOAD A FILE
E	MS Certificate  3ag Attributes IocalKeyID: 69 28 D7 B7 D0 1C 03 E8 4E 36 F5 65 71 4A E1  MS Private Key  Bag Attributes IocalKeyID: 69 28 D7 B7 D0 1C 03 E8 4E 36 F5 65 71 4A E1  CANCEL BACK E

6. Wait until vCenter reports that the connection status for the KMS cluster has changed to **Connected**. For example:

Key	Pr	oviders						
ADD	STA	NDARD KEY PROVIDE	R MAKE DEFAULT	EDIT	REMOVE			
	Key	Provider	Ť	Connectio	on Status		Certificates	
•	Key	/Control (default)		🔗 Conr	nected		🔗 Valid	
								1 items
Provider KeyControl - Key Management Servers								
		KMS $\uparrow$ Add	Iress Port		Connection Status	vCenter Certificate		KMS Certificate
0	>	Keycontrol 1 10	.194. 569	5	⊘ Connected	⊘ Valid until: Jun 7,	2023	⊘ Valid until: Dec 31, 2049
0	>	Keycontrol 2 10	).194 569	6	⊘ Connected	⊘ Valid until: Jun 7,	2023	⊘ Valid until: Dec 31, 2049

#### 2.4. Enable Encryption for virtual machines

Enable encryption using VMware Storage Policies.

- 1. Launch the vSphere Web Client and log into the vCenter server.
- 2. Locate a VM that you would like to encrypt.
- 3. Make sure the **Power** state of the VM is **Powered Off**.
- Right-click the VM for which you would like to enable encryption, and select VM Policies > Edit VM Storage Policies.
- 5. Select the storage policy VM Encryption Policy and select OK.

This will trigger a reconfiguration of the VM.

Recent Tasks Alarms						
Task Name	∽ Target	Status	✓ Details			
Reconfigure virtual	🗗 testpxe-server	27%	Reconfiguring Virtual Machine on destination host			

After the reconfiguration is complete, the disks are encrypted and the keys are managed by the configured KMS (KeyControl).

#### 2.4.1. Check encryption at the VM level

- 1. Launch the vSphere Web Client and log into the vCenter server.
- 2. Locate a VM, and select it.
- 3. In VM View, select the Summary tab.
- 4. Under VM Hardware > Encryption, the status should be:

```
VM configuration files are encrypted.
Hard disk is encrypted.
```

### 2.4.2. Check encryption by looking for the Keys in the Entrust KeyControl KMS

- 1. Log into the KeyControl web user interface using the **Tenant Login** URL.
- Select the **Objects** tab to view a list of **KMIP Objects**. This will include the newly created keys. For example:

ENTRUST Keyc	ontrol ×				•	2 4 ?
KMIP Objects						Actions -
UUID	Initial Date	Last Change Date	Object Type	Archived	State	
dc2bef6e-8f97-4dc5-93f1-0d	Jun 7, 2022, 3:15:18 PM	Jun 7, 2022, 3:15:18 PM	SymmetricKey		Active	

3. Select one of the keys to display its details. For example:

KMIP Object Details		×
UUID	dc2bef6e-8f97-4dc5-93f1-	
Cryptographic Usage Mask	Encrypt,Decrypt	
Key Format Type	Raw	
Cryptographic Algorithm	AES	
Cryptographic Length	256	
Encrypted With KEK	✓ Yes	

4. In the main screen, select the **Audit Logs** tab to view the log records related to the key creation process. For example:

Close

ENTRUST KeyControl				> 4	?
👫 KMIP 🔀 Audit Logs	×				
Audit Logs					
Filter				난 Down	nload
Time	Туре	User	Message		
Jun 7, 2022, 3:17:58 PM	Information	vCenterKMS	KMIP Response - Operation: AddAttribute, Object: None, UUID: dc2bef6e-8f97-4dc5-93f1-	, Re.	•
Jun 7, 2022, 3:15:22 PM	Information	vCenterKMS	KMIP Response - Operation: Activate, Object: None, UUID: dc2bef6e-8f97-4dc5-93f1-	, Result	
Jun 7, 2022, 3:15:22 PM	Information	vCenterKMS	KMIP Response - Operation: AddAttribute, Object: None, UUID: dc2bef6e-8f97-4dc5-93f1-	, Re.	
Jun 7, 2022, 3:15:21 PM	Information	vCenterKMS	KMIP Response - Operation: AddAttribute, Object: None, UUID: dc2bef6e-8f97-4dc5-93f1-	, Re.	
Jun 7, 2022, 3:15:21 PM	Information	vCenterKMS	KMIP Response - Operation: AddAttribute, Object: None, UUID: dc2bef6e-8f97-4dc5-93f1-	, Re.	
Jun 7, 2022, 3:15:19 PM	Information	vCenterKMS	KMIP Response - Operation: Create, Object: SymmetricKey, UUID: dc2bef6e-8f97-4dc5-93f1-	,	
Jun 7, 2022, 11:37:46 AM	Information	administrator	administrator enabled KMIP KEK wrapping		
Jun 7, 2022, 11:34:43 AM	Information	administrator	User 'administrator' logged in successfully.		
Jun 7, 2022, 10:42:04 AM	Information	administrator	KMIP Client Certificate VCenterKMS' created		
Jun 7, 2022, 10:36:42 AM	Information	administrator	User 'administrator' logged in successfully.		
Jun 6, 2022, 5:20:53 PM	Information	administrator	User 'administrator' logged in successfully.		•
Showing 4 to 14 of 14 records @2022 Entrust Corporation. All Rights Reserved.					

For more information on this topic, refer to Virtual Machine Encryption on the VMware documentation site.

# 2.5. Enable Data-At-Rest encryption on an existing vSAN cluster

To enable Data-At-Rest encryption on an existing vSAN cluster, refer to Using Encryption in a vSAN Cluster on the VMware documentation site.

# Chapter 3. Additional resources and related products

- 3.1. Video
- 3.2. nShield Connect
- 3.3. nShield as a Service
- 3.4. KeyControl
- 3.5. Entrust digital security solutions
- 3.6. nShield product documentation