



# VMware vSphere and Entrust KeyControl

## Integration Guide

21 Oct 2022

# Contents

1. Introduction	3
1.1. Documents to read first	3
1.2. Product configuration	3
2. Procedures	4
2.1. Prerequisites	4
2.2. Create the KMS cluster in vCenter	4
2.3. Establish a trusted connection between the KMS cluster and the Entrust KeyControl server	6
2.4. Enable Encryption for target servers	8
2.5. Enable Data-At-Rest encryption on an existing vSAN cluster	10

# 1. Introduction

This guide describes the integration of the Entrust KeyControl Key Management Solution (KMS) with VMware encryption 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 [Entrust KeyControl nShield HSM Integration Guide](#). You can access this in the Entrust Document Library.

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	8.0
KeyControl	5.5.1

## 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 [Creating the KMS Cluster in vSphere](#).

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:
  - 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. 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 Standard Key Provider ×

Name	KeyControl	
<b>KMS</b>	<b>Address</b>	<b>Port</b>
Keycontrol 1	10.194. [REDACTED]	5696 <span>⊗</span>
Keycontrol 2	10.194. [REDACTED]	5696 <span>⊗</span>
<input type="button" value="ADD KMS"/>		
<div style="border: 1px solid #ccc; padding: 5px;"><p>&gt; Proxy configuration (optional)</p><p>&gt; Password protection (optional)</p></div>		
<input type="button" value="CANCEL"/> <input type="button" value="ADD KEY PROVIDER"/>		

- 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:

### Make vCenter Trust Key Provider ×

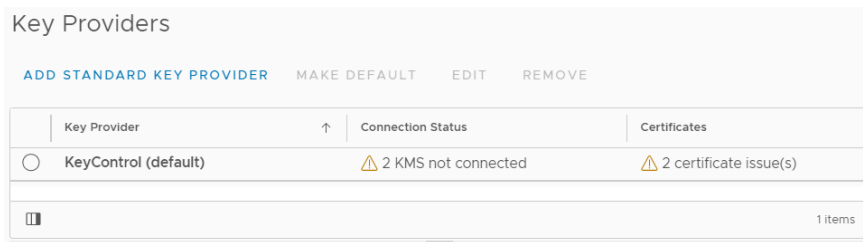
Keycontrol 1

Serial number	0x7E9E56
> Subject	keycontrol-551-1. [REDACTED].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	F7:B0:42:02:69:2F:56:81:D0:F8:FE:8A:5A :5F: [REDACTED]
> Certificate	Expand to view details

Keycontrol 2

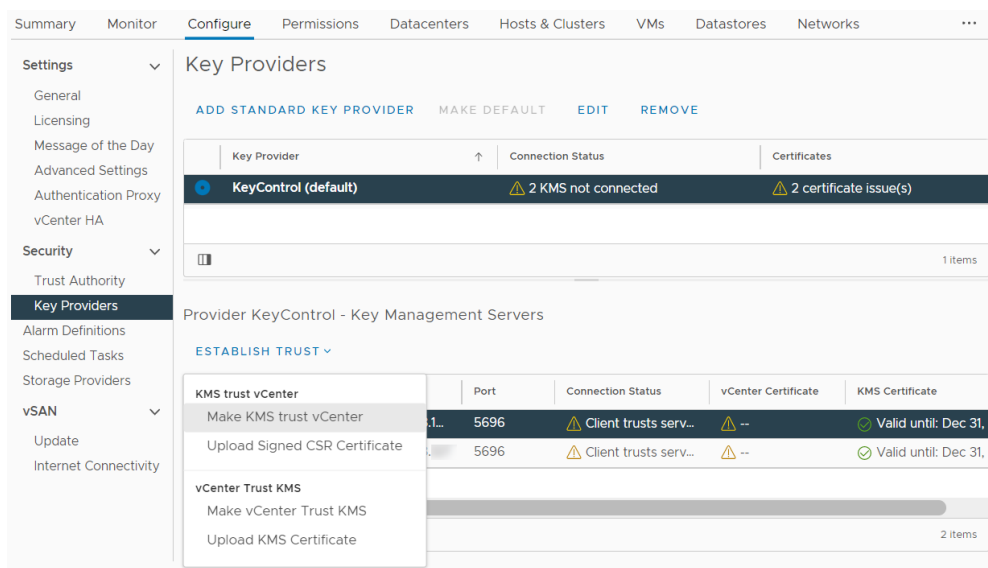
Serial number	0x7F9E5E
> Subject	keycontrol-551-2. [REDACTED].com

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

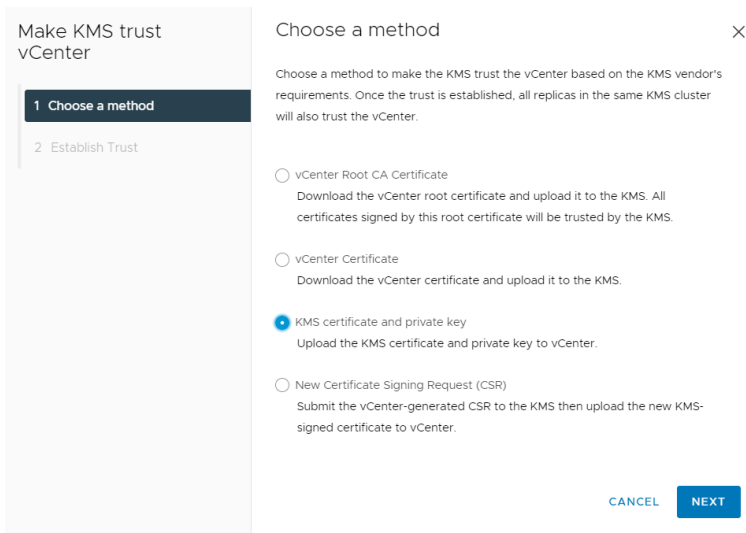


## 2.3. Establish a trusted connection between the KMS cluster and the Entrust KeyControl server

1. Launch the vCenter vSphere Web Client and log into the vCenter server to which you added the KeyControl KMS cluster.
2. Select the **Configure** tab for the server.
3. In the left-hand pane, select **Security > Key Providers**.
4. Select the KeyControl KMS cluster in the list, then scroll down to where the nodes are displayed.
5. Select one of the nodes, then select on **Establish Trust > Make KMS trust vCenter**.  
For example:



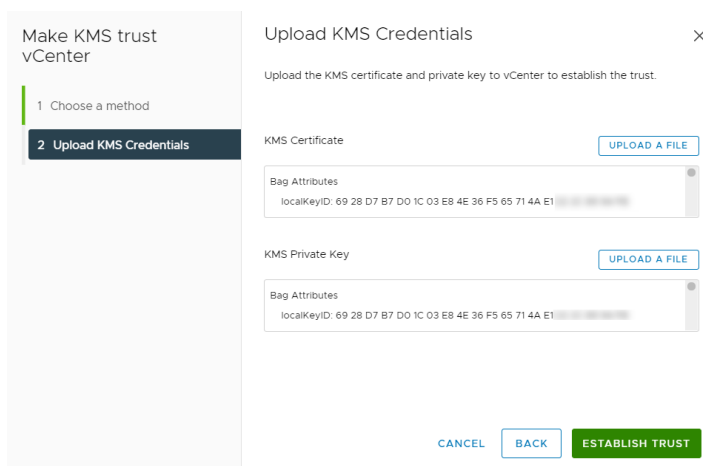
6. In the **Choose method** pane of the **Make KMS Trust vCenter** dialog, select **KMS certificate and private key**.



7. Select **Next**.

8. 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**.



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

Key Providers

ADD STANDARD KEY PROVIDER MAKE DEFAULT EDIT REMOVE

Key Provider	Connection Status	Certificates
KeyControl (default)	Connected	Valid

1 Items

Provider KeyControl - Key Management Servers

ESTABLISH TRUST

	KMS	Address	Port	Connection Status	vCenter Certificate	KMS Certificate
<input type="radio"/>	> Keycontrol 1	10.194. [REDACTED]	5696	Connected	Valid until: Jun 7, 2023	Valid until: Dec 31, 2049
<input type="radio"/>	> Keycontrol 2	10.194. [REDACTED]	5696	Connected	Valid until: Jun 7, 2023	Valid until: Dec 31, 2049

## 2.4. Enable Encryption for target servers

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**.
4. 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
Reconfigure virtual machine	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.
2. Select the **Objects** tab to view a list of **KMIP Objects**. This will include the newly created keys. For example:

UUID	Initial Date	Last Change Date	Object Type	Archived	State
dc2bef6e-8f97-4dc5-93f1-...	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

Close

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

Time	Type	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.

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.