



VMware vSphere and Entrust KeyControl KMIP Vault

Integration Guide

2024-04-23

Table of Contents

1. Introduction	1
1.1. Documents to read first	1
1.2. Product configuration	1
1.3. Requirements	1
2. Procedures	2
2.1. Prerequisites	2
2.2. Create a KMIP Vault in the KeyControl Vault Server	2
2.3. Establishing trust between the KeyControl KMIP Vault and the VMware vCenter	7
2.4. Create the KMS cluster in vCenter	8
2.5. Establish a trusted connection between the KMS cluster and the KeyControl KMIP Vault	10
2.6. Enable Encryption for virtual machines	12
2.7. Enable Data-At-Rest encryption on an existing vSAN cluster	14
3. Additional resources and related products	15
3.1. nShield Connect	15
3.2. nShield as a Service	15
3.3. KeyControl	15
3.4. KeyControl as a Service	15
3.5. Entrust products	15
3.6. nShield product documentation	15

Chapter 1. Introduction

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

1.1. Documents to read first

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

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

- *Entrust KeyControl Vault nShield HSM Integration Guide*. You can access it from the [Entrust Document Library](#) and from the [nShield Product Documentation website](#).
- [KeyControl Vault 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	8.0
KeyControl Vault	10.4.3

1.3. Requirements

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

Chapter 2. Procedures

2.1. Prerequisites

Before you integrate the KeyControl KMIP Vault KMS with VMware encryption solutions, complete the following tasks:

- KeyControl KMIP Vault is deployed and configured.
- VMware vSphere is deployed and configured using vCenter.
- You have administrator rights to manage the KMS configuration in vCenter.

2.2. Create a KMIP Vault in the KeyControl Vault Server

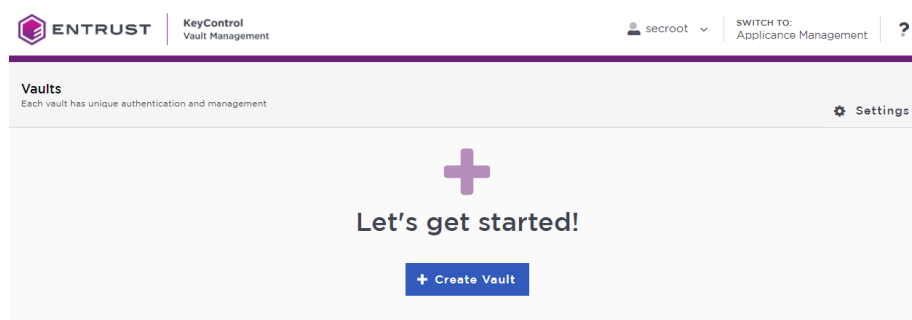
The KeyControl Vault appliance supports different type of vaults that can be used by all type of applications. This section describes how to create a KMIP Vault in the KeyControl Vault Server.

Refer to the [Creating a Vault](#) section of the admin guide for more details about it.

1. Log into the 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. If not in the Vault Management interface, select **SWITCH TO: Manage Vaults** in the Menu Header.

This action will take you to the KeyControl Vault Management interface.

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



4. In the **Create Vault** page, create a **KMIP** Vault:
 - For **Type**, select **KMIP**.

- For **Name**, enter the name of the Vault.
- For **Description**, enter the description of the Vault.
- For **Admin Name**, enter the name of the administrator of the Vault.
- For **Admin Email**, enter a valid email for the administrator.

Create Vault
A vault will have unique authentication and management.

Type
Choose the type of vault to create
KMIP

Name *
VMware-vCenter

Description
Vault to control vCenter Encryption
Max. 300 characters

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

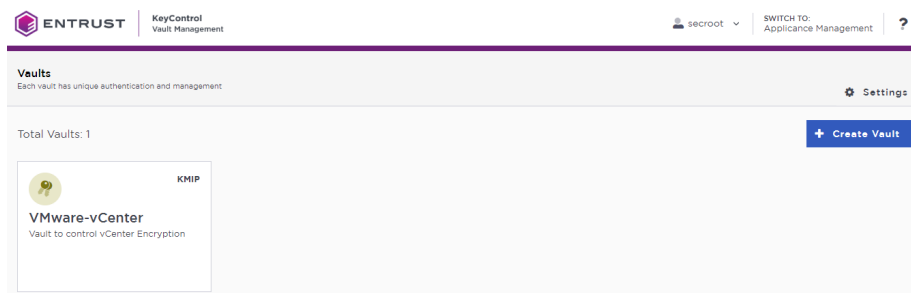
Admin Name *
Administrator

Admin Email *
[Redacted]

Create Vault **Cancel**

A temporary password will be emailed to the administrator's email address. This is the password that will be used to sign in for the first time to the KMIP Vaults space in KeyControl. In a closed gap environment where email is not available, the password for the user is displayed when you first create the vault. That can be copied and sent to the user.

5. Select **Create Vault**.
6. Select **Close** when the Vault creation completes.
7. The newly-created Vault is added to the Vault dashboard.



8. After the Vault has been created, the KMIP server settings on the appliance are **enabled**.

2.2.1. KMIP server settings

The KMIP server settings are set at the KeyControl appliance level and apply to all the KMIP Vaults in the appliance. After a KMIP Vault is created, they are automatically set to **ENABLED**.

To use external key management and configure the KeyControl Vault KMIP settings, refer to the [KeyControl Vault for KMIP](#) section of the admin guide.

When you are using external key management, as is the case in this solution, the KeyControl server is the KMIP server and the VMware vCenter server is the KMIP client.

1. Select the **Settings** icon on the top right to view/change the KMIP settings.

The defaults settings are appropriate for most applications. Make any changes necessary.

The screenshot shows the 'Settings' page for 'KMIP Vault Settings'. The page title is 'Settings' and the subtitle is 'KMIP Vault Settings'. Below the subtitle is the instruction 'Define the default setting for all KMIP vaults'. The 'ENABLED' toggle switch is turned on. The 'Port' field is set to '5696'. The 'Auto Reconnect' section has 'Off' selected. The 'Verify' section has 'Yes' selected. The 'Non-blocking I/O' section has 'No' selected. The 'Log Level' dropdown is set to 'CREATE-MODIFY'. The 'Restrict TLS' section has 'No' selected. The 'Timeout' section has 'No' selected. The 'SSL/TLS Ciphers' section has a text area containing a list of cipher names: 'ECDHE-RSA-AES128-GCM-SHA256,ECDHE-RSA-AES256-GCM-SHA384,ECDHE-ECDSA-AES128-GCM-SHA256,ECDHE-ECDSA-AES256-GCM-SHA384,DHE-RSA-AES128-GCM-SHA256,DHE-RSA-AES256-GCM-SHA384,DHE-ECDSA-AES128-GCM-SHA256,DHE-ECDSA-AES256-GCM-SHA384,AES128-GCM-SHA256,AES256-GCM-SHA384'. The 'Certificate Types' section has 'Default' selected. At the bottom are 'Apply' and 'Cancel' buttons.

Settings

KMIP Vault Settings

Define the default setting for all KMIP vaults

☒ **ENABLED**

Port *

5696

Auto Reconnect

☐ On ☒ Off

Verify

☒ Yes ☐ No

Non-blocking I/O

If set to yes, the client requires non-blocking I/O

☐ Yes ☒ No

Log Level *

CREATE-MODIFY

Restrict TLS

If set to yes, connection will use TLS 1.2

☐ Yes ☒ No

Timeout

☐ Yes ☒ No

SSL/TLS Ciphers

Enter comma separated cipher names

ECDHE-RSA-AES128-GCM-SHA256,ECDHE-RSA-AES256-GCM-SHA384,ECDHE-ECDSA-AES128-GCM-SHA256,ECDHE-ECDSA-AES256-GCM-SHA384,DHE-RSA-AES128-GCM-SHA256,DHE-RSA-AES256-GCM-SHA384,DHE-ECDSA-AES128-GCM-SHA256,DHE-ECDSA-AES256-GCM-SHA384,AES128-GCM-SHA256,AES256-GCM-SHA384

Certificate Types

☒ Default ☐ Custom

Apply Cancel

2. Select **Apply**.

2.2.2. View details for the Vault



To view the details on the Vault, select **View Details** when you hover over the Vault.



Vault Details ×

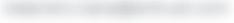
VMware-vCenter
Vault to control vCenter Encryption

Type
KMIP

Created
Apr 13, 2023 02:15:02 PM

Vault URL

 [Copy](#)

API URL

 [Copy](#)

Administrator
Administrator


Close

2.2.3. Edit a vault

To edit the details of the Vault, select **Edit** when you hover over the Vault.

Vaults
Each vault has unique authentication and management

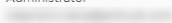
Edit Vault


Type
KMIP

Name
VMware-vCenter

Description

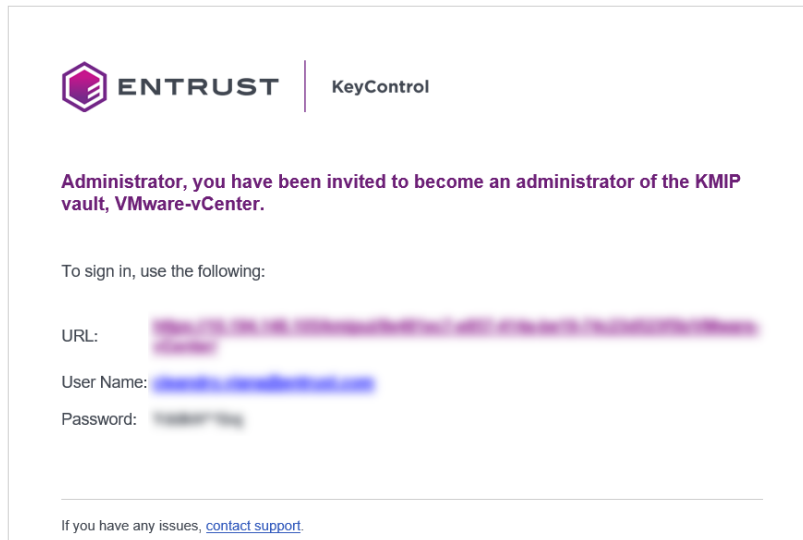
Max. 300 characters

Administrator
Administrator


Apply **Cancel**  **Delete Vault**

2.2.4. Managing the Vault

After the Vault has been created, look for the email that was sent with the Vault's URL and the login information for the Vault. For example:



Go to the URL and sign in with the credentials given. When you sign in for the first time, the system will ask the user to change the password.

In a closed gap environment where email is not available, the password for the user is displayed when you first create the vault. That can be copied and sent to the user.

2.2.5. Setup other 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.

-
- c. Select **Add**.

2.3. Establishing trust between the KeyControl KMIP Vault and the VMware vCenter

Certificates are required to facilitate the KMIP communications from the KeyControl KMIP Vault and the vCenter application and conversely. The built-in capabilities in the KeyControl KMIP Vault are used to create and publish the certificates.

For more information on how to create a certificate bundle, refer to [Establishing a Trusted Connection with a KeyControl Vault-Generated CSR](#).

The process below will show how to integrate VMware vSphere encryption or VSAN encryption with KeyControl KMIP Vault.

1. Sign in to the KMIP Vault created earlier. Use the login URL and credentials provided to the administrator of the Vault.
2. Select **Security**, then **Client Certificates**.



3. In the **Manage Client Certificate** page, select the **+** icon on the right to create a new certificate.

There is the option of creating two types of certificates that can be used by vCenter:

- A certificate with no authentication.
 - A certificate with authentication.
4. Create the certificate that best fits your environment needs.
 5. In the **Create Client Certificate** dialog box:
 - Enter a name in the **Certificate Name** field.
 - Set the date on which you want the certificate to expire in the **Certificate Expiration** field.

If you are creating a certificate with authentication:

- Select **Add Authentication for Certificate**.
- Enter the User Name
- Enter the Password

These settings will be used later when the certificates are used in vCenter if authentication is used.

6. Select **Create**.

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

7. Select the certificate and select the **Download** icon to download the certificate.

The webGUI downloads `certname_datetimestamp.zip`, which contains a user certification/key file called `certname.pem` and a server certification file called `cacert.pem`.

8. Unzip the file so that you have the `certname.pem` file available to upload.

9. The download zip file contains the following:

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

These files will be used in the vCenter KMS cluster configuration later.

2.4. 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 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 using the KeyControl Vault server 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 Standard Key Provider

×

Name

keycontrol

KMS	Address	Port	
kms1	10.10.10.10	5696	⊗
kms2	10.10.10.10	5696	⊗

ADD KMS

> Proxy configuration (optional)

> Password protection (optional)

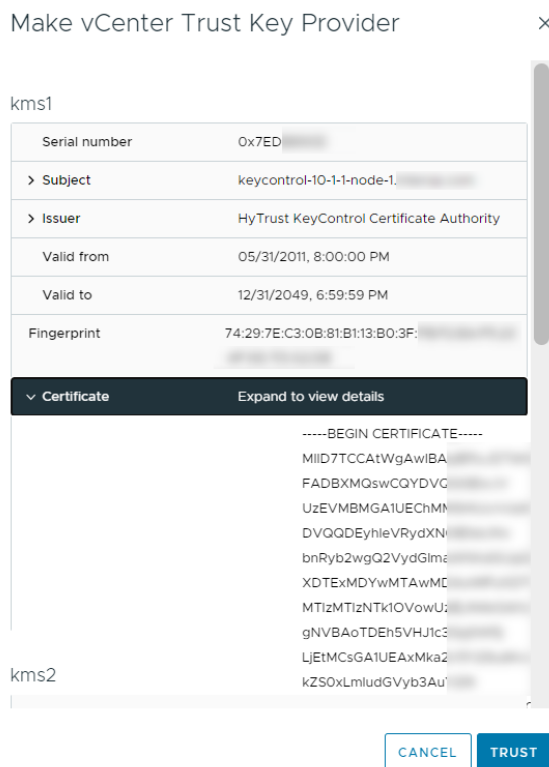
CANCEL

ADD KEY PROVIDER

7. Open and set **Proxy Configuration** if you are using a proxy.

Password protection is optional.

8. Provide the information if the certificate created in the KeyControl KMIP Vault was created with authentication.
9. Select **Add Key Provider**.
10. In the **Make vCenter Trust Key Provider** dialog, confirm the details for each node and then select **Trust**. For example:



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

Key Provider	Type	Status	Certificates
<input type="radio"/> keycontrol (default)	Standard	⚠ 2 KMS not connected	⚠ 2 certificate issue(s)

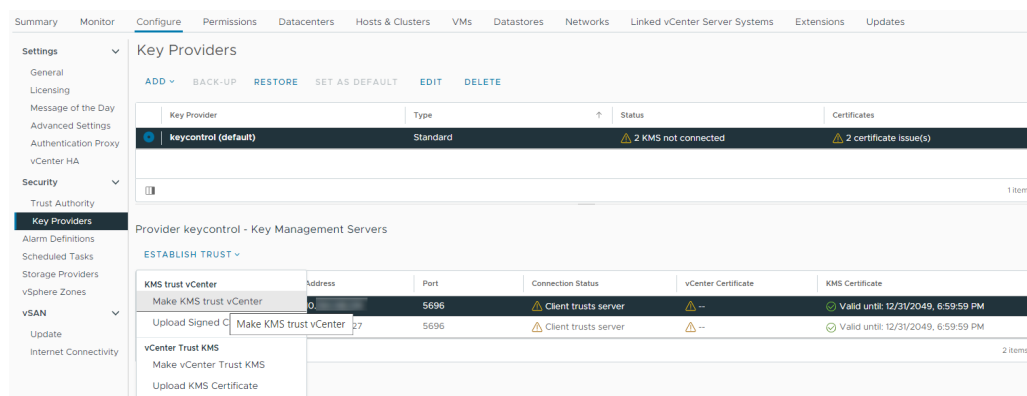
If you get a message stating that it **"Cannot retrieve the requested certificate"**, it may be related to the **TLS Configuration** in the KeyControl Appliances. This issue is related to using earlier versions of vCenter where **TLS Extended Master Secret** is not supported. Suggested fixes are upgrading to the latest version of vCenter or change KeyControl to **NOT** enforce EMS in the **TLS configuration**. Please refer to [TLS Configuration](#) settings in the KeyControl Administration Guide.

2.5. Establish a trusted connection between the KMS cluster and the KeyControl KMIP Vault

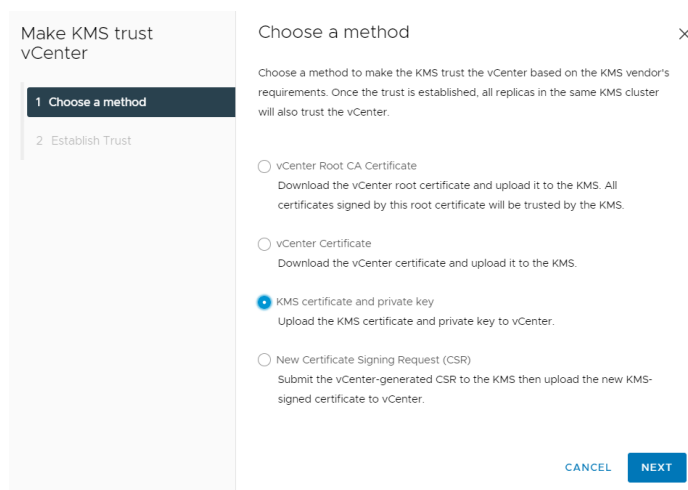
To establish a trusted connection between the KMS cluster and the KeyControl KMIP Vault:

1. Continuing from the previous section, select the KeyControl KMS cluster in the list, then scroll down to where the nodes are listed.

2. Select one of the nodes, then select on **Establish Trust > Make KMS trust vCenter**. For example:



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



4. Select **Next**.
5. In the **Upload KMS Credentials** pane of the **Make KMS Trust vCenter** dialog, you must upload the **certname.pem** file created during the certificate creation process earlier. This file must be uploaded for the KMS certificate and then uploaded again for the private key. To do this:
 - a. For **KMS certificate**, select **Upload file**. Then select the **certname.pem** file and select **Open**.
 - b. For **Private key**, select **Upload file**. Then select the **certname.pem** file again and select **Open**.
 - c. Select **Establish Trust**.

Make KMS trust vCenter

1 Choose a method
2 Upload KMS Credentials

Upload KMS Credentials

Upload the KMS certificate and private key to vCenter to establish the trust.

KMS Certificate

Upload A File

Bag Attributes

localKeyID: 69 28 D7 B7 D0 1C 03 E8 4E

KMS Private Key

Upload A File

Bag Attributes

localKeyID: 69 28 D7 B7 D0 1C 03 E8 4E

CANCEL

BACK

ESTABLISH TRUST

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

Key Providers

ADD

BACK-UP

RESTORE

SET AS DEFAULT

EDIT

DELETE

	Key Provider	Type	Status	Certificates
	keycontrol (default)	Standard	Healthy	Valid
1 item				

Provider keycontrol - Key Management Servers

ESTABLISH TRUST

		KMS	Address	Port	Connection Status	vCenter Certificate	KMS Certificate
		kms1	10.10.10.10	5696	Connected	Valid until: 8/15/2024, 11:59 PM	Valid until: 12/31/2049, 6:59:59 PM
		kms2	10.10.10.10	5696	Connected	Valid until: 8/15/2024, 11:59 PM	Valid until: 12/31/2049, 6:59:59 PM
2 items							

2.6. 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**.
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. For example:

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Reconfigure virtual mach...	test-encryption-vm	Completed	Reconfiguring Virtual Machi...	VSPHERE.LOCAL\Administrator	3 ms	04/17/2023, 2:32:30 ...	04/17/2023, 2:34:12 PM	10.194.148.11

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

2.6.1. Check encryption at the VM level

To 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 **Virtual Machine Details** > **Encryption**, the status should be:

Encrypted with standard key provider

2.6.2. Check encryption by looking for the Keys in the KeyControl KMIP Vault

To check encryption by looking for keys:

- 1. Log into the KMIP Vault using the login URL.
- 2. Select the **Objects** tab to view a list of **KMIP Objects**. This will include the newly-created keys. For example:

The screenshot shows the 'KMIP Objects' tab in the KeyControl interface. It features a table with columns: UUID, Description, Initial Date, Last Status Changed Date, Object T..., Archived, and State. Three rows of data are visible, each representing a symmetric key object. The first row has a highlighted UUID: 62d9e596-1376-42e1-ba24-ec5d862f9a6d.

UUID	Description	Initial Date	Last Status Changed Date	Object T...	Archived	State
62d9e596-1376-42e1-ba24-ec5d862f9a6d		Jul 31, 20...	Jul 31, 2024, 9:22:19 AM	Symmetric...		ACTIVE
62d9e596-1376-42e1-ba24-ec5d862f9a6d		Jul 31, 20...	Jul 31, 2024, 9:22:19 AM	Symmetric...		ACTIVE
f12f98a9-cd76-4208-835...		Jul 31, 20...	Jul 31, 2024, 9:53:21 AM	Symmetric...		ACTIVE

- 3. Select one of the keys to display its **KMIP Object Details**. For example:

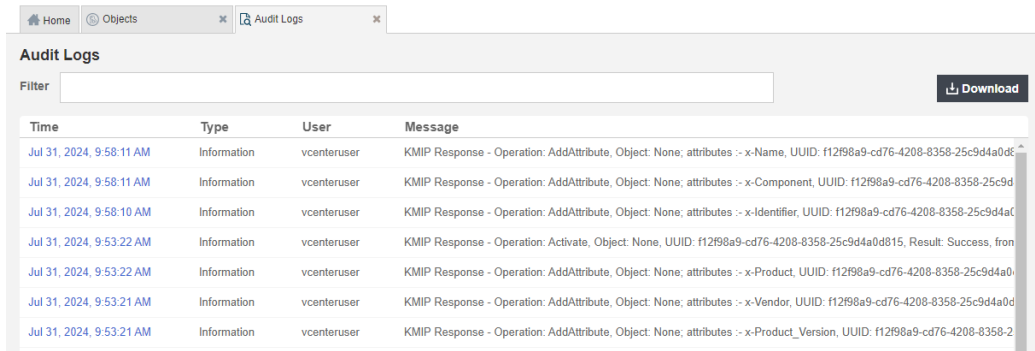
The screenshot shows the 'KMIP Object Details' dialog box for the key with UUID 62d9e596-1376-42e1-ba24-ec5d862f9a6d. The dialog has three tabs: 'KMIP Attributes', 'Custom Attributes', and 'KMIP Identifiers'. The 'KMIP Attributes' tab is selected, showing details such as Object Type (Symmetric Key), State (ACTIVE), Activation Date, Cryptographic Usage Mask (Encrypt, Decrypt), Key Format Type (Raw), Cryptographic Algorithm (AES), Cryptographic Length (256), Encrypted With KEK (No), Initial Date, and Last Status Changed Date.

KMIP Object Details	
	62d9e596-1376-42e1-ba24-ec5d862f9a6d
UUID	62d9e596-1376-42e1-ba24-ec5d862f9a6d
Object Type	Symmetric Key
State	ACTIVE
Activation Date	Jul 31, 2024, 9:22:19 AM
Cryptographic Usage Mask	Encrypt, Decrypt
Key Format Type	Raw
Cryptographic Algorithm	AES
Cryptographic Length	256
Encrypted With KEK	No
Initial Date	Jul 31, 2024, 9:22:19 AM
Last Status Changed Date	Jul 31, 2024, 9:27:30 AM

- 4. Select the **Custom Attributes** tab to make sure it is the key used by VMware vSphere.



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



For more information on this topic, refer to <https://docs.vmware.com/en/VMware-vSphere/8.0/com.vmware.vsphere.security.doc/GUID-E6C5CE29-CD1D-4555-859C-A0492E7CB45D.html> [Virtual Machine Encryption] on the VMware documentation site.

2.7. 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. nShield Connect

3.2. nShield as a Service

3.3. KeyControl

3.4. KeyControl as a Service

3.5. Entrust products

3.6. nShield product documentation