



VMware vSphere and Entrust Cryptographic Security Platform Key Management Vault

Integration Guide

2026-10-15

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 Key Management Vault server	2
2.3. Establish trust between the Key Management 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 Key Management 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. Integrating with an HSM	15
4. Additional resources and related products	16
4.1. nShield HSMs	16
4.2. nShield as a Service	16
4.3. Entrust CSP Key Manager	16
4.4. Entrust products	16
4.5. nShield product documentation	16

Chapter 1. Introduction

This guide describes how to integrate the Entrust Cryptographic Security Platform Key Management Vault with VMware encryption solutions for vSAN and VM encryption. Entrust Cryptographic Security Platform Key Management Vault, configured with an open-standard KMIP Vault, can serve as a KMS in vCenter.

1.1. Documents to read first

- *Entrust Cryptographic Security Platform Key Management Vault nShield HSM Integration Guide*. You can access it from the [Entrust Document Library](#) and from the [nShield Product Documentation website](#).
- [Cryptographic Security Platform Key Management 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

Vendor	Product	Version
VMware	vSphere	8.0, 9.0
Entrust	Cryptographic Security Platform	1.4, 1.6
Entrust	Key Management Vault	10.5.3, 10.6.1

1.3. Requirements

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

Chapter 2. Procedures

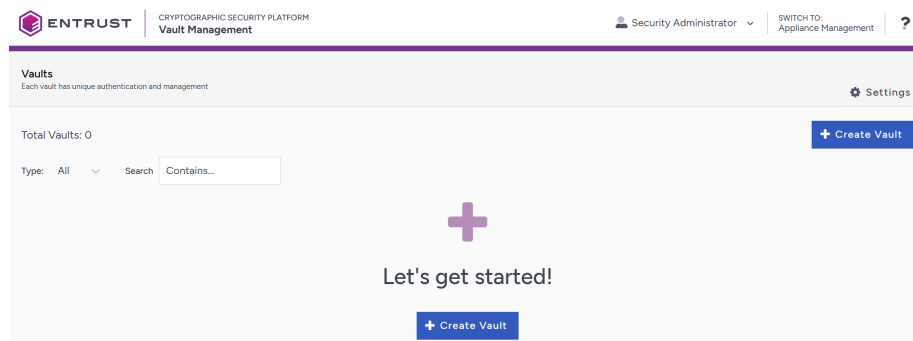
2.1. Prerequisites

Before you perform the integration, complete the following tasks:

- Key Management 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 Key Management Vault server

1. In your web browser, go to the Key Management Vault server's IP address and sign in with the **secroot** credentials.
2. If you are not in the vault Management interface, select **SWITCH TO: Manage Vaults** in the Menu Header
3. Select **Create Vault**.



4. 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.

Vaults
Each vault has unique authentication and management

Create Vault
A vault will have unique authentication and management.

Type
Choose the type of vault to create
KMIP

Name *
vcenter

Description
Optionally add a short description to help identify this vault.
Test vCenter
Max. 300 characters

Email Notifications
⚠ SMTP needs to be configured to turn on email notifications
Use email to communicate with Vault Administrators, including their temporary passwords. Turning off email notifications means you will see and need to give temporary passwords to Vault Admins. OFF

Administrator
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 *
xxxxxxxxx@yourcompany.com

Create Vault Cancel

A temporary password is emailed to the administrator. The user uses this password to sign in to the KMIP Vaults space in Key Management Vault for the first time. In a closed-gap environment where email is unavailable, the password is displayed when you create the vault. Copy it and send it to the user.

5. Select **Create Vault**.
6. Select **Close** when the vault creation completes.
7. The new vault is added to the vault dashboard.

ENTRUST CRYPTOGRAPHIC SECURITY PLATFORM
Vault Management

Security Administrator SWITCH TO: Appliance Management ?

Vaults
Each vault has unique authentication and management Settings

Total Vaults: 1 + Create Vault

Type: All Search: Contains...

KMIP
vcenter
Test vCenter

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 configured at the Key Management Vault appliance level and apply to all KMIP Vaults on the appliance. After a KMIP Vault is created, they are automatically set to **ENABLED**.

To use external key management and configure the Key Management Vault KMIP settings, refer to [Configuring a KMIP Server for vSphere KMS](#).

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

1. Select the **Settings** icon at the top right to view or change the KMIP settings.

The default settings are appropriate for most applications. Change them as needed.

The screenshot shows the 'Settings' dialog for KMIP Vault Settings. The dialog is titled 'KMIP Vault Settings' and includes an 'Actions' dropdown menu. The settings are as follows:

- ENABLED** (toggle switch)
- Port ***: 5696
- Verify**: ☒ Yes ☐ No
- Log Level ***: CREATE-MODIFY
- TLS**: ☐ TLS 1.3 ☒ TLS 1.2, TLS 1.3
- Timeout**: ☐ Yes ☒ No
- KMIP Locate Operation: Maximum Items Default**: ☒ The default value (1000 items). ☐ The value set to the maximum items value from the KMIP client.
- SSL/TLS Ciphers**: ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-AES256-GCM-SHA384,ECDHE-ECDSA-AES256-CCM,ECDHE-ECDSA-AES128-GCM-SHA256,ECDHE-RSA-AES128-GCM-SHA256,ECDHE-ECDSA-AES128-CCM,DHE-RSA-AES256-GCM-SHA384,DHE-RSA-AES256-CCM,DHE-RSA-AES128-GCM-SHA256,DHE-RSA-AES128-CCM,PSK-AES256-GCM-SHA384,PSK-AES256-CCM,PSK-AES128-GCM-SHA256,PSK-AES128-CCM,DHE-RSA-AES256-GCM-SHA384,DHE-RSA-AES256-CCM,DHE-RSA-AES128-GCM-SHA256,PSK-AES256-GCM-SHA384,PSK-AES256-CCM,PSK-AES128-GCM-SHA256,PSK-AES128-CCM
- Certificate Types**: ☒ Default ☐ Custom

Buttons: Apply, Cancel

2. Select **Apply**.

2.2.2. View details for the vault

To view the vault's details, hover over it and select **View Details**.

Vault Details



VMware-vCenter

Vault to control vCenter encryption.

Type

KMIP

Created

Oct 24, 2024 01:35:28 PM

Vault URL

[Redacted URL]

Copy

API URL

[Redacted URL]

Copy

Administrator

Admin Name

Administrator

User Name

[Redacted Username]

Email Notifications

Off

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

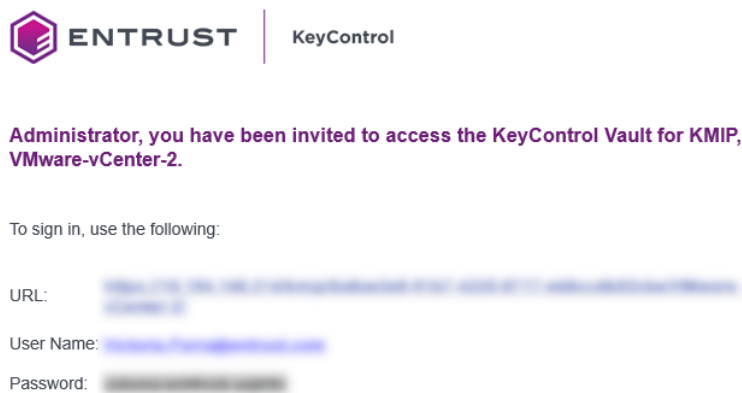
Description
Vault to control vCenter Encryption
Max: 300 characters

Administrator
Administrator

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

2.2.4. Manage the vault

After creating the vault, check for an email containing its URL and login information. For example:



Open the URL and sign in with the credentials provided. The first time you sign in, you need to change the password.

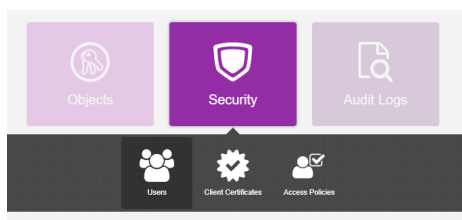


In a closed-gap environment where email is unavailable, the password is displayed when you create the vault. Copy it and send it to the user.

2.2.5. Set up other administrators

For recovery purposes, add one or more additional administrators 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. Establish trust between the Key Management KMIP Vault and the VMware vCenter

Certificates are required to support KMIP communication between the Key Management Vault KMIP Vault and the vCenter application. Use the built-in capabilities of the Key Management KMIP Vault to create and publish the certificates.

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

The following steps show how to integrate VMware vSphere or VSAN encryption with the Key Management 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.

You can create the following certificate types for vCenter:

- A certificate with no authentication.

- A certificate with authentication.
4. Create the certificate type that best fits your environment.
 5. In the **Create Client Certificate** dialog box:
 - Enter a name in the **Certificate Name** field.
 - Set the certificate's expiration date 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.

If you use certificate authentication, enter these credentials in vCenter later.

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 client certificate and key file named `certname.pem` and a server certificate file named `cacert.pem`.

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

9. The ZIP file contains the following files:

- 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`.

Use these files later when you configure the KMS cluster in vCenter.

2.4. Create the KMS cluster in vCenter

For more details, 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 Key Management Vault.
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 Key Management Vault 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 Key Management 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	CSP-Vault		
KMS	Address	Port	
kms1		5696	×
kms2		5696	×

> Proxy configuration (optional)

> Password protection (optional)

7. If you use a proxy, open and configure **Proxy Configuration**.

Password protection is optional.

8. If the certificate you created in the Key Management KMIP Vault uses authentication, enter the required credentials.

9. Select **Add Key Provider**.
10. In the **Make vCenter Trust Key Provider** dialog, review the details for each node, then select **Trust**.

This adds the KMS cluster to vCenter, but its status is **KMS not connected** because of **Certificate issues**. For example:

Key Providers				
ADD BACK-UP RESTORE SET AS DEFAULT EDIT DELETE				
Key Provider	Type	Status	Certificates	
☐ CSP-Vault (default)	Standard	⚠ 2 KMS not connected	⚠ 2 certificate issue(s)	

If you see the message "**Cannot retrieve the requested certificate**", the issue may be related to the **TLS Configuration** in the Key Management Vault appliances. This can occur with earlier versions of vCenter that do not support **TLS Extended Master Secret**. To resolve the issue, upgrade to the latest version of vCenter or change Key Management Vault so that it does **NOT** enforce EMS in the **TLS configuration**. See [Configuring TLS](#) in the Key Management Vault Administration Guide.

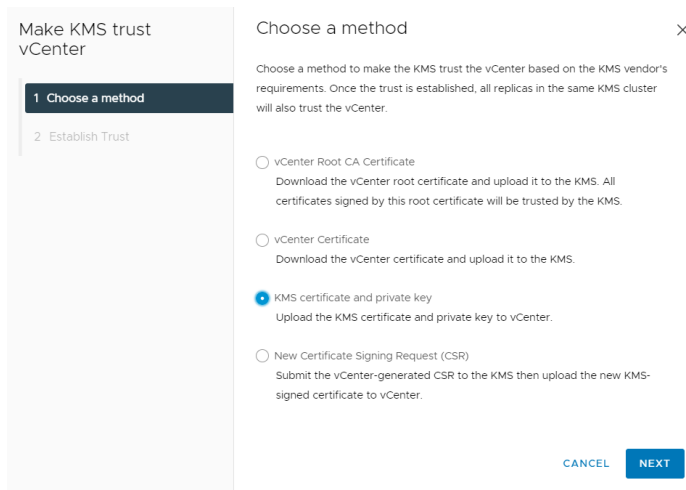
2.5. Establish a trusted connection between the KMS cluster and the Key Management KMIP vault

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

1. Continuing from the previous section, select the KMS cluster in the list, then scroll down to where the nodes are listed.
2. Select a node, then select **Establish Trust > Make KMS trust vCenter**. For example:

The screenshot shows the 'Key Providers' configuration page. The 'Key Providers' section lists 'CSP-Vault (default)' with a status of '2 KMS not connected' and '2 certificate issue(s)'. Below this, the 'Provider CSP-Vault - Key Management Servers' section shows a table of KMS trust vCenter nodes. The table has columns: Name, IP Address, Port, Connection Status, vCenter Certificate, and KMS Certificate. The first row is 'Make KMS trust vCenter' with IP 192.168.1.100 and port 5696, showing 'Client trusts server' status and a valid vCenter certificate. The second row is 'Upload Signed C...' with IP 192.168.1.100 and port 5696, showing 'Client trusts server' status and a valid KMS certificate. Below the table, the 'vCenter Trust KMS' section shows 'Make vCenter Trust KMS' and 'Upload KMS Certificate' options.

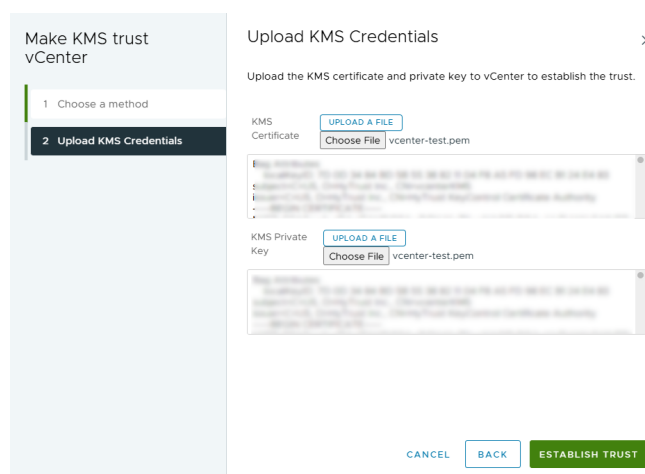
3. In the **Choose method** pane of the **Make KMS Trust vCenter** dialog, select **KMS certificate and private key**.



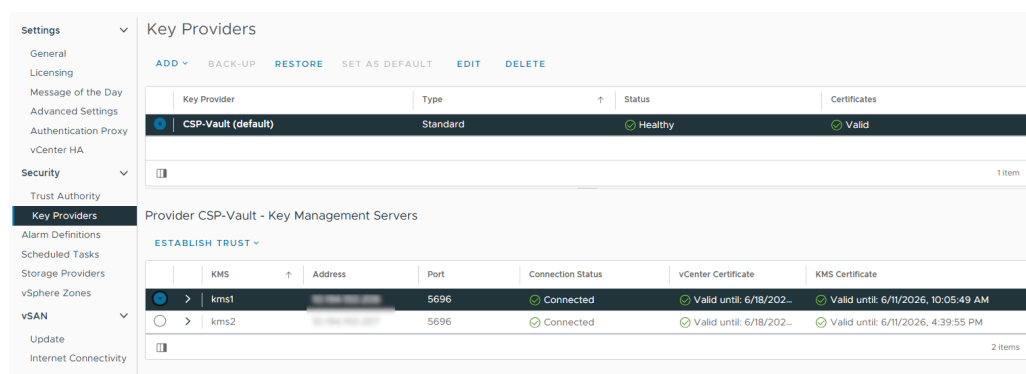
4. Select **Next**.

5. In the **Upload KMS Credentials** pane of the **Make KMS Trust vCenter** dialog, upload the **certname.pem** file created earlier. Upload this file as both the KMS certificate and the private key:

- For **KMS certificate**, select **Upload file**. Select the **certname.pem** file, then select **Open**.
- For **Private key**, select **Upload file**. Select the **certname.pem** file again, then select **Open**.
- Select **Establish Trust**.



6. Wait for the KMS cluster's connection status in vCenter to change to **Connected**. For example:



2.6. Enable Encryption for virtual machines

Use a VMware storage policy to enable encryption:

1. Launch the vSphere Web Client and sign in to the vCenter server.
2. Select the VM to encrypt.
3. Make sure 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 **VM Encryption Policy** storage policy, then select **OK**.

This reconfigures the VM. For example:

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Reconfigure virtual mach...	test-encryption-vm	22%	Reconfiguring Virtual Machi...	VSPHERE.LOCAL\Administrator	4 ms	06/18/2025, 10:31:22 ...		
Move entities	CSP - Vault	Completed		VSPHERE.LOCAL\Administrator	5 ms	06/18/2025, 10:29:59 ...	06/18/2025, 10:29:59 ...	

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

2.6.1. Check encryption at the VM level

To verify encryption at the VM level:

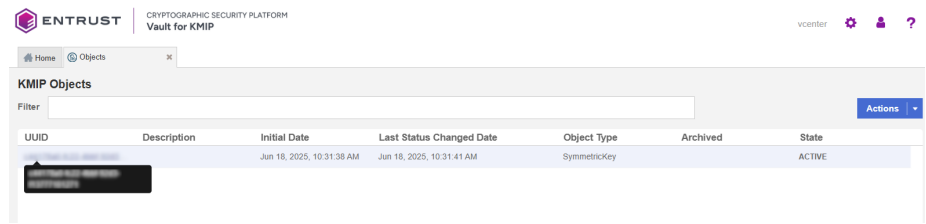
1. Launch the vSphere Web Client and sign in to the vCenter server.
2. Locate a VM and select it.
3. In **VM View**, select the **Summary** tab.
4. Under **Virtual Machine Details > Encryption**, the status should be:

Encrypted with standard key provider

2.6.2. Check encryption by looking for the keys in the Key Management KMIP Vault

To verify encryption by checking for keys:

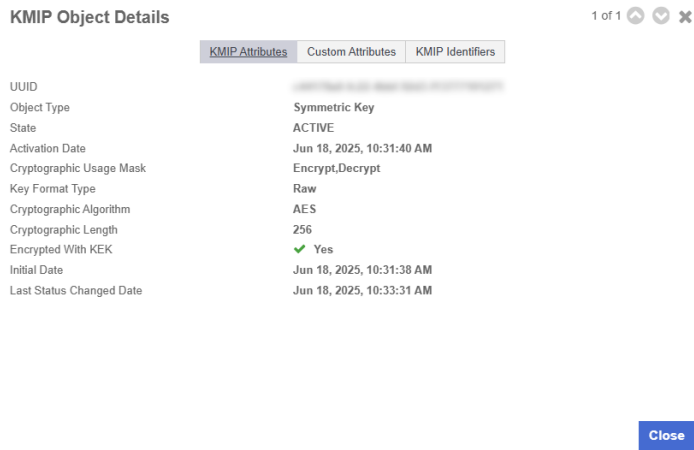
1. In a web browser, sign in to the KMIP Vault.
2. Select the **Objects** tab to view a list of **KMIP Objects**. The list includes the newly created keys. For example:



The screenshot shows the Entrust Cryptographic Security Platform KMIP Vault interface. The 'Objects' tab is selected, displaying a table of KMIP Objects. The table has columns for UUID, Description, Initial Date, Last Status Changed Date, Object Type, Archived, and State. A single object is listed with a UUID, a description, and a state of 'ACTIVE'.

UUID	Description	Initial Date	Last Status Changed Date	Object Type	Archived	State
[Redacted]	[Redacted]	Jun 18, 2025, 10:31:38 AM	Jun 18, 2025, 10:31:41 AM	SymmetricKey		ACTIVE

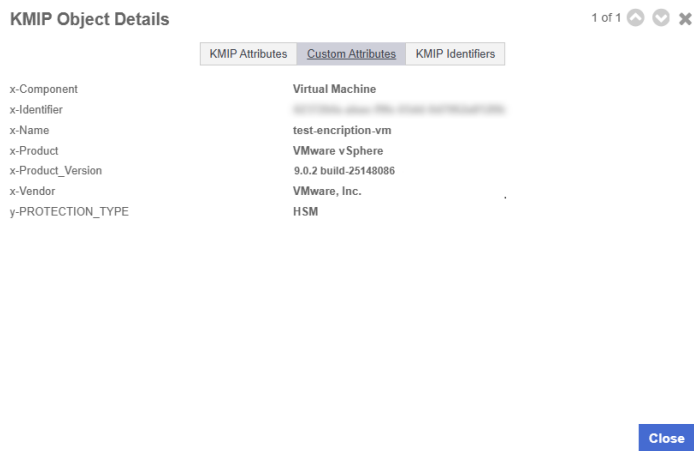
3. Select a key to display its **KMIP Object Details**. For example:



The screenshot shows the 'KMIP Object Details' page with the 'KMIP Attributes' tab selected. The page displays various attributes of the selected key, including UUID, Object Type, State, Activation Date, Cryptographic Usage Mask, Key Format Type, Cryptographic Algorithm, Cryptographic Length, Encrypted With KEK, Initial Date, and Last Status Changed Date.

Attribute	Value
UUID	[Redacted]
Object Type	Symmetric Key
State	ACTIVE
Activation Date	Jun 18, 2025, 10:31:40 AM
Cryptographic Usage Mask	Encrypt, Decrypt
Key Format Type	Raw
Cryptographic Algorithm	AES
Cryptographic Length	256
Encrypted With KEK	✓ Yes
Initial Date	Jun 18, 2025, 10:31:38 AM
Last Status Changed Date	Jun 18, 2025, 10:33:31 AM

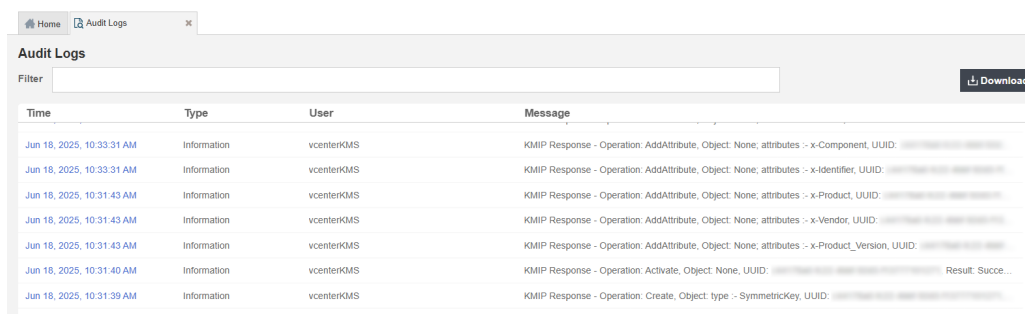
4. Select the **Custom Attributes** tab to confirm that VMware vSphere uses the key.



The screenshot shows the 'KMIP Object Details' page with the 'Custom Attributes' tab selected. The page displays various custom attributes of the selected key, including x-Component, x-Identifier, x-Name, x-Product, x-Product_Version, x-Vendor, y-PROTECTION_TYPE, and Virtual Machine.

Attribute	Value
x-Component	Virtual Machine
x-Identifier	[Redacted]
x-Name	test-encryption-vm
x-Product	VMware vSphere
x-Product_Version	9.0.2 build-25148086
x-Vendor	VMware, Inc.
y-PROTECTION_TYPE	HSM

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



The screenshot shows the 'Audit Logs' section of a web application. It includes a 'Filter' input field and a 'Download' button. Below is a table with four columns: Time, Type, User, and Message. The table contains seven log entries, all of which are 'Information' type and from the user 'vcenterKMS'. The messages describe KIMP Response operations: AddAttribute, Activate, and Create, with various attributes and UUIDs.

Time	Type	User	Message
Jun 18, 2025, 10:33:31 AM	Information	vcenterKMS	KIMP Response - Operation: AddAttribute, Object: None, attributes -> x-Component, UUID: [redacted]
Jun 18, 2025, 10:33:31 AM	Information	vcenterKMS	KIMP Response - Operation: AddAttribute, Object: None, attributes -> x-identifier, UUID: [redacted]
Jun 18, 2025, 10:31:43 AM	Information	vcenterKMS	KIMP Response - Operation: AddAttribute, Object: None, attributes -> x-Product, UUID: [redacted]
Jun 18, 2025, 10:31:43 AM	Information	vcenterKMS	KIMP Response - Operation: AddAttribute, Object: None, attributes -> x-Vendor, UUID: [redacted]
Jun 18, 2025, 10:31:43 AM	Information	vcenterKMS	KIMP Response - Operation: AddAttribute, Object: None, attributes -> x-Product_Version, UUID: [redacted]
Jun 18, 2025, 10:31:40 AM	Information	vcenterKMS	KIMP Response - Operation: Activate, Object: None, UUID: [redacted] Result: Succ...
Jun 18, 2025, 10:31:39 AM	Information	vcenterKMS	KIMP Response - Operation: Create, Object: type -> SymmetricKey, UUID: [redacted]

For more information on this topic, refer to [Virtual Machine Encryption](#) on the Broadcom documentation site.

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

For instructions on enabling Data-At-Rest encryption on an existing vSAN cluster, see [Using Encryption in a vSAN Cluster](#) on the Broadcom documentation site.



Do not encrypt the CSP Vault Appliance with its own keys. This will prevent the vSAN from powering back on after a power cycle because it cannot access the keys. You can add a datastore to ESXi hosts. As long as vSAN does not absorb that storage, you can deploy the appliances on a datastore outside vSAN. Alternatively, you can deploy the appliances in another hypervisor supported by [Key Management Vault](#).

Chapter 3. Integrating with an HSM

For guidance on integrating Entrust Key and Secrets Management with a Hardware Security Module (HSM), consult your HSM vendor. If you are using an Entrust nShield HSM, refer to [Hardware Security Modules with CSP Vault](#) for instructions on configuring Entrust Key and Secrets Management with FIPS 140-3 or FIPS 140-2 certified protection. Additionally, post-quantum support is available with new nShield HSM firmware.

Chapter 4. Additional resources and related products

4.1. nShield HSMs

4.2. nShield as a Service

4.3. Entrust CSP Key Manager

4.4. Entrust products

4.5. nShield product documentation