VMware vSphere and Entrust Cryptographic Security Platform Key Management Vault

Integration Guide

2026-07-07

© Entrust Corporation. All rights reserved.

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 . . . 9
    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 the integration of the Entrust Cryptographic Security Platform Key Management Vault with VMware encryptions solutions, 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	9.0
Entrust	Cryptographic Security Platform	1.4
Entrust	Key Management Vault	10.5.3

1.3. Requirements

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

Chapter 2. Procedures

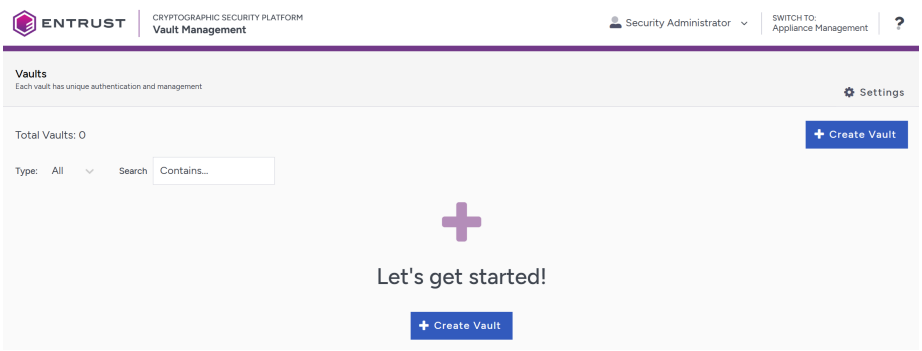
2.1. Prerequisites

Before you perform the integration, complete the following tasks:

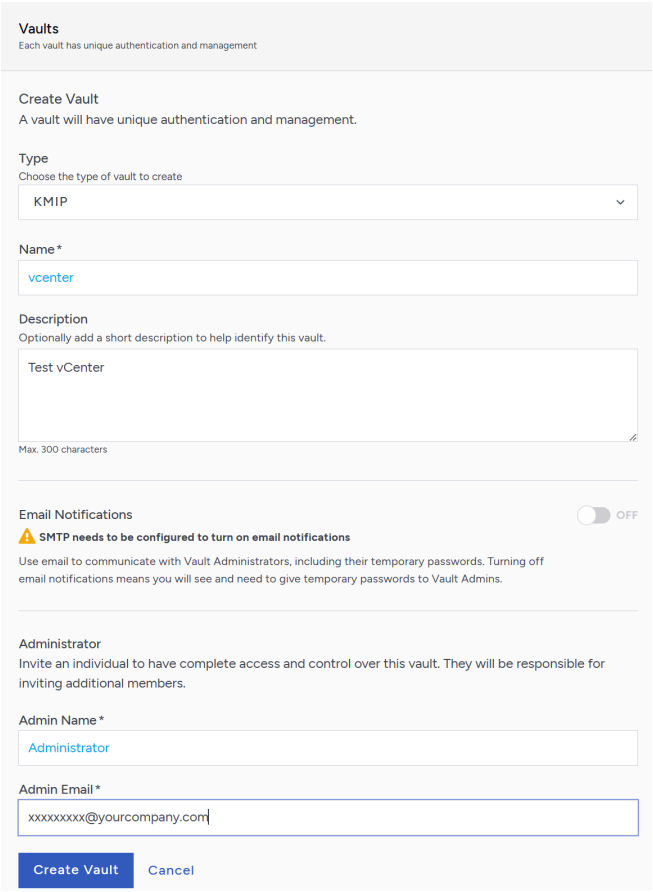
- Key Management Vault is deployed and configured.
- VMware vSphere is deployed and configured using vCenter.
- You have administrator rights to manage the KMS configuration in vCenter.

2.2. Create a KMIP Vault in the Key Management Vault server

1. Log in to the Key Management Vault server in your web browser using the **secroot** credentials to access the IP address of the server.
2. If you are not in the vault Management interface, select **SWITCH TO: Manage Vaults** in the Menu Header
3. Select **Create Vault**.

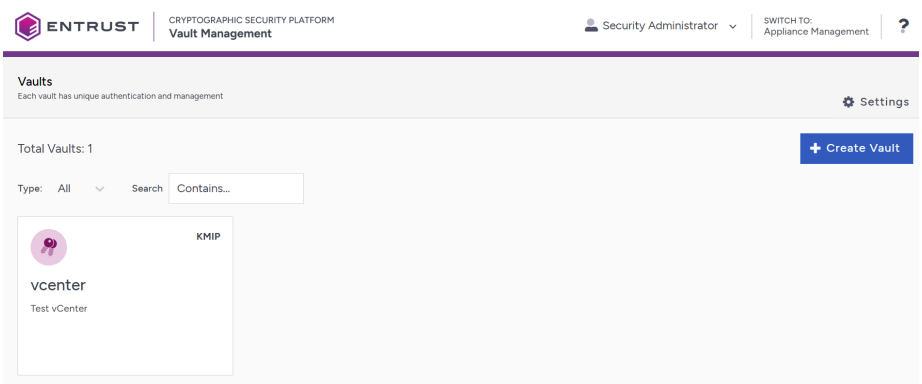


4. Create a **KMIP** Vault:
    - For **Type**, select **KMIP**.
    - For **Name**, enter the name of the vault.
    - For **Description**, enter the description of the vault.
    - For **Admin Name**, enter the name of the administrator of the vault.
    - For **Admin Email**, enter a valid email for the administrator.



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 Key Management Vault. 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 vault is added to the vault dashboard.



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

2.2.1. KMIP server settings

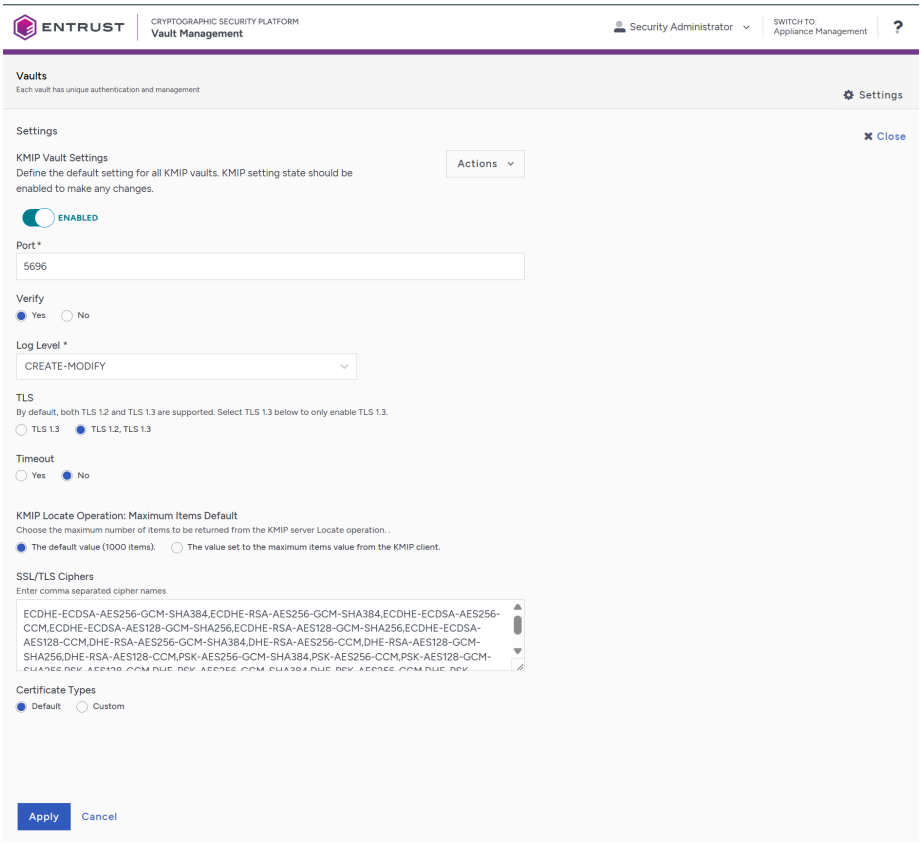
The KMIP server settings are set at the Key Management Vault appliance level and apply to all the KMIP Vaults in the appliance. After a KMIP Vault is created, they are automatically set to **ENABLED**.

To use external key management and configure the Key Management Vault KMIP settings, refer to the Cryptographic Security Platform Key Management Vault for KMIP section of the admin guide.

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 on the top right to view/change the KMIP settings.

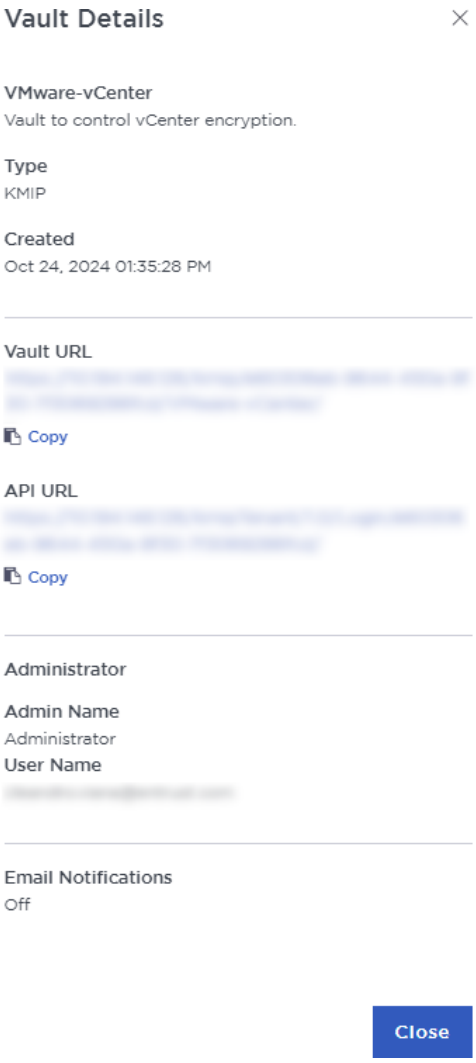
   The defaults settings are appropriate for most applications. Make any changes necessary.



2. Select **Apply**.

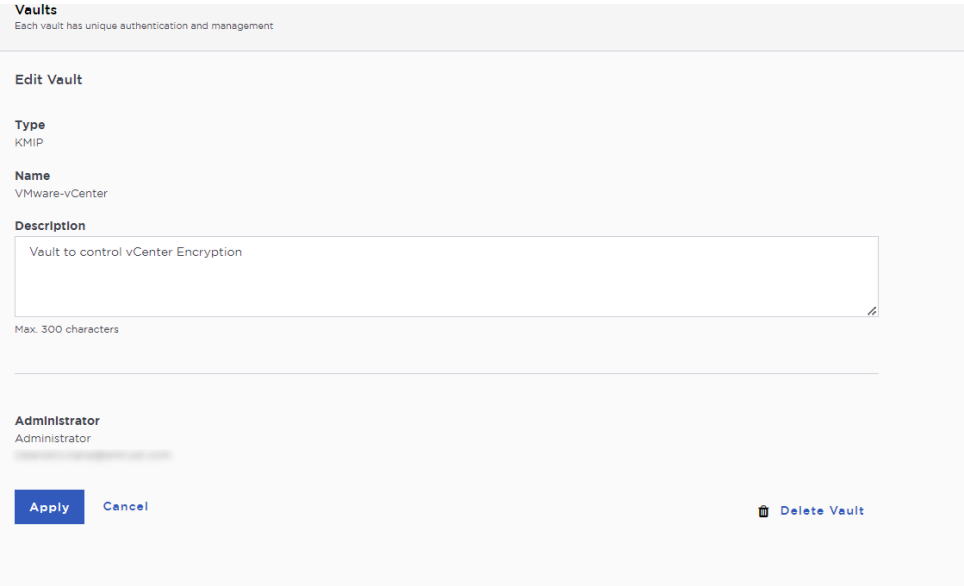
2.2.2. View details for the vault

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



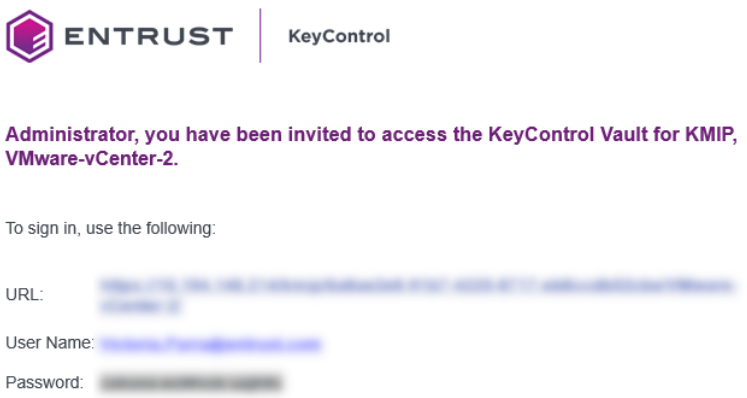
2.2.3. Edit a vault

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



2.2.4. Manage 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. Set up 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**.

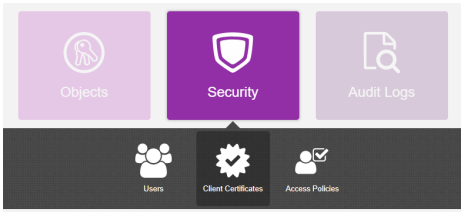
2.3. Establish trust between the Key Management KMIP Vault and the VMware vCenter

Certificates are required to facilitate the KMIP communications from the Key Management Vault KMIP Vault and the vCenter application and conversely. The built-in capabilities in the Key Management 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 Cryptographic Security Platform Key Management Vault Generated CSR.

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

    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.

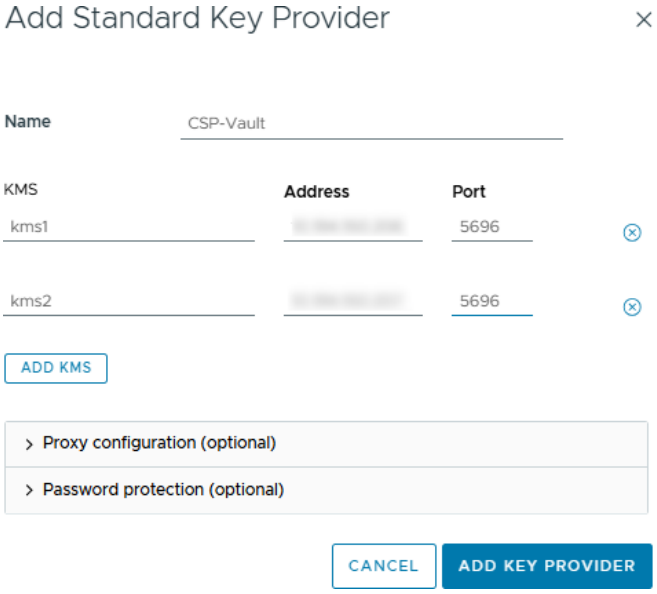
2.4. Create the KMS cluster in vCenter

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 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**.

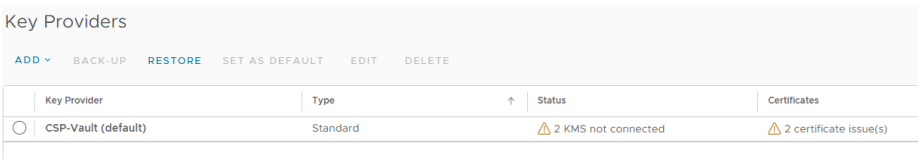


7. Open and set **Proxy Configuration** if you are using a proxy.

    Password protection is optional.

8. Provide the information if the certificate created in the Key Management 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**.

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

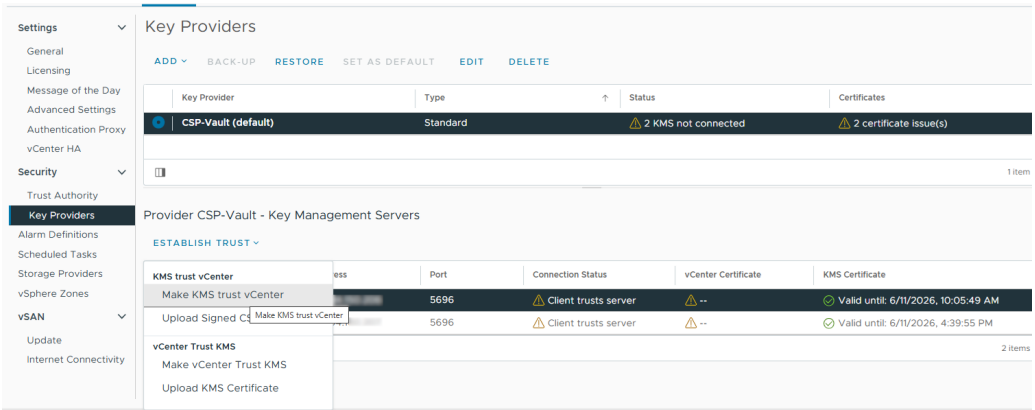


    If you get a message stating that it **"Cannot retrieve the requested certificate"**, it may be related to the **TLS Configuration** in the Key Management Vault Appliances. This issue is related to using earlier versions of vCenter where **TLS Extended Master Secret** is not supported. Suggested fixes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

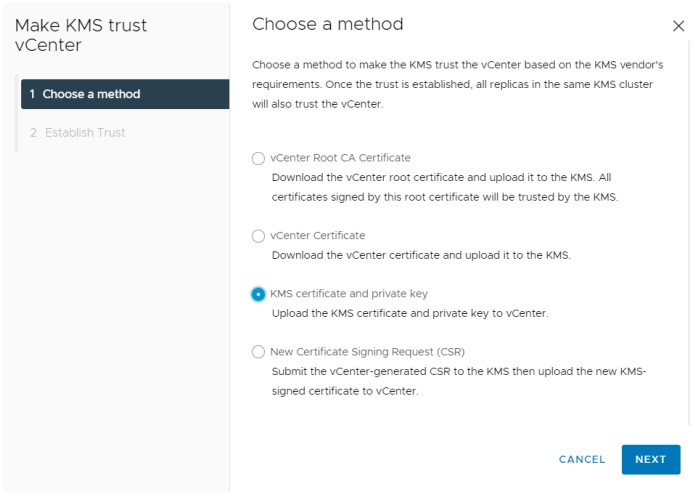
2.5. Establish a trusted connection between the KMS cluster and the Key Management KMIP vault

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

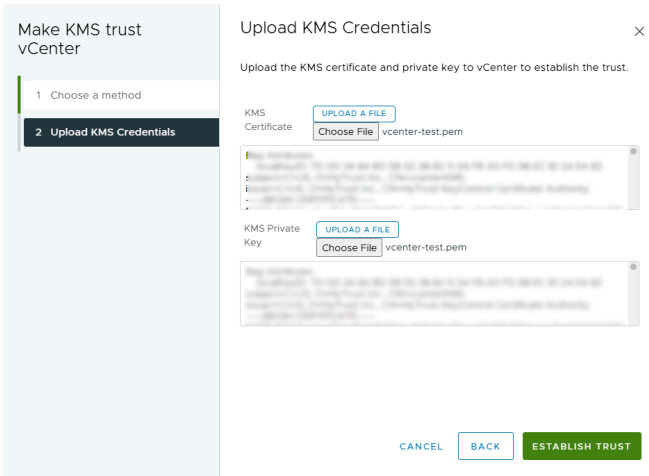
1. Continuing from the previous section, select the KMS cluster in the list, then scroll down to where the nodes are listed.
2. Select one of the nodes, then select on **Establish Trust** > **Make KMS trust vCenter**. For example:



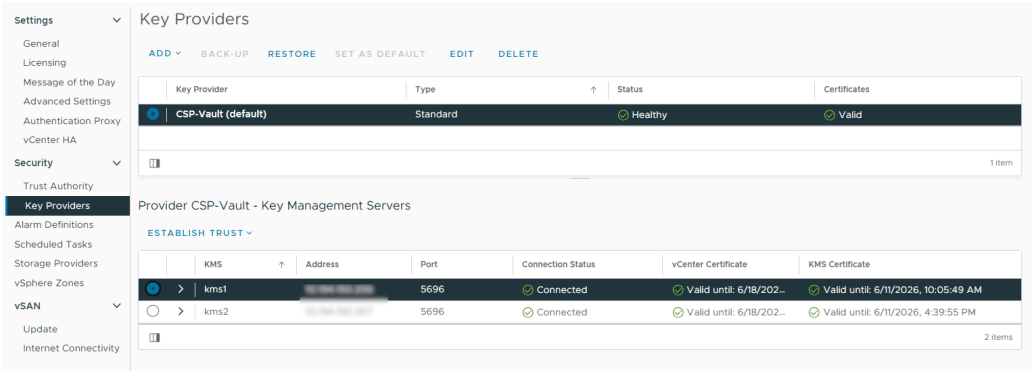
3. In the **Choose method** pane of the **Make KMS Trust vCenter** dialog, select **KMS certificate and private key**.



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**.



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

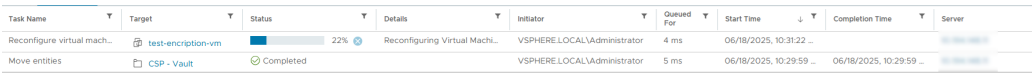


2.6. Enable Encryption for virtual machines

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:



   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 check encryption at the VM level:

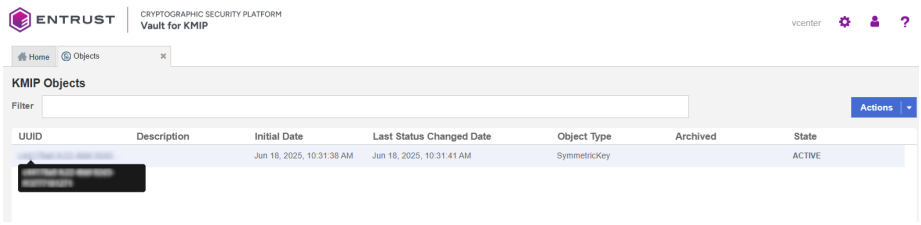
1. Launch the vSphere Web Client and log into the vCenter server.
2. Locate a VM and select it.
3. In **VM View**, select the **Summary** tab.
4. Under **Virtual Machine Details** > **Encryption**, the status should be:

```
Encrypted with standard key provider
```

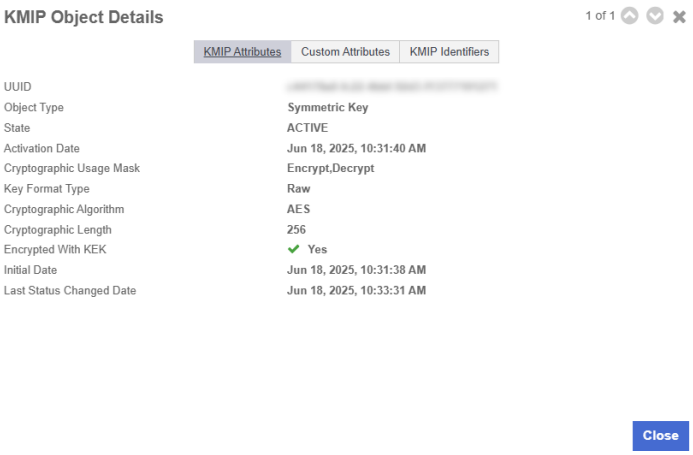
2.6.2. Check encryption by looking for the keys in the Key Management KMIP Vault

To check encryption by looking for keys:

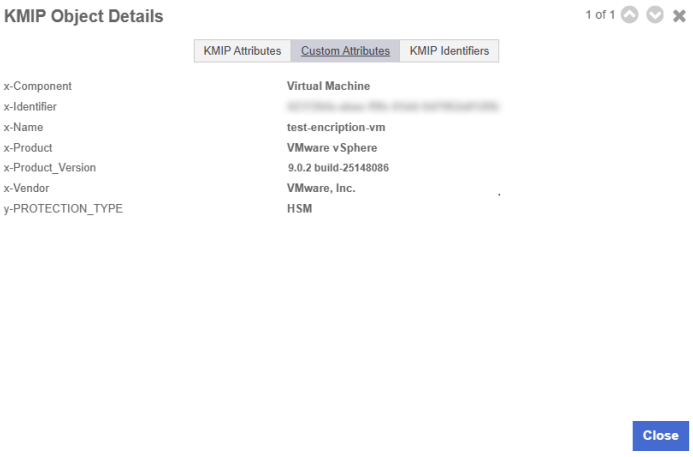
1. Log into the KMIP Vault using the login URL.
2. Select the **Objects** tab to view a list of **KMIP Objects**. This will include the newly-created keys. For example:



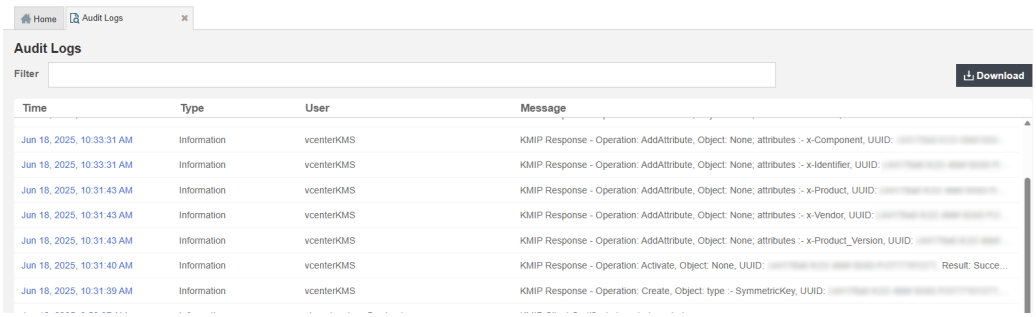
3. Select one of the keys to display its **KMIP Object Details**. For example:



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 Virtual Machine Encryption on the Broadcom 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 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 the vSAN does not absorb that storage, you can deploy the appliances on the datastore that is not in the vSAN. Alternatively, you can deploy the appliances in another hypervisor.

Chapter 3. Integrating with an HSM

For guidance on integrating the Entrust Key and Secrets Management with a Hardware Security Module (HSM), consult with your HSM vendor. If you are using an Entrust nShield HSM, refer to the Entrust Cryptographic Security Platform Key Management Vault: nShield HSM Integration Guide for instructions on how to configure 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