Commvault and Entrust KeyControl KMIP Vault

Integration Guide

2024-04-19

Table of Contents

Chapter 1. Introduction

This guide describes the integration of the Entrust KeyControl KMIP Vault Key Management Solution (KMS) with Commvault platform. Entrust KeyControl KMIP Vault can serve as a Key Management Server in Commvault 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 Key Management Server in Commvault.

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.
- Entrust KeyControl Vault nShield Online Help.

Also refer to the Commvault Online Documentation.

1.2. Product configuration

Product	Version
Windows	Windows 2022
Commvault	2023E (11.32)
KeyControl Vault	10.1.1

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 integrate the Entrust KeyControl KMIP Vault KMS with Commvault platform, complete the following tasks:

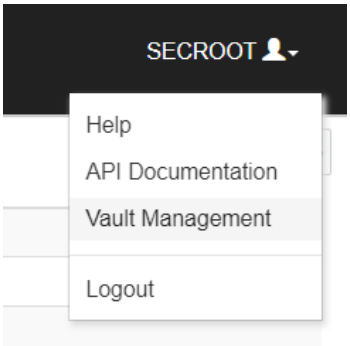
- Entrust KeyControl KMIP Vault is deployed and configured.
- Commvault Platform is deployed and configured.
- You have administrator rights to manage the KMS configuration in Commvault.

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.

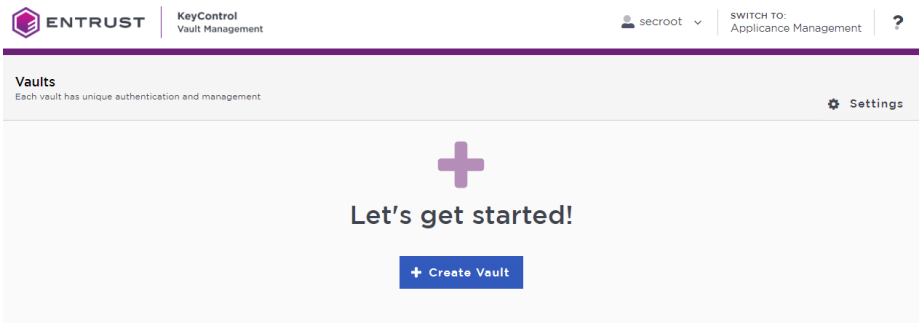
Refer to the Creating a Vault section of the admin guide for more details about it.

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. Select the user's dropdown menu and select **Vault Management**.



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

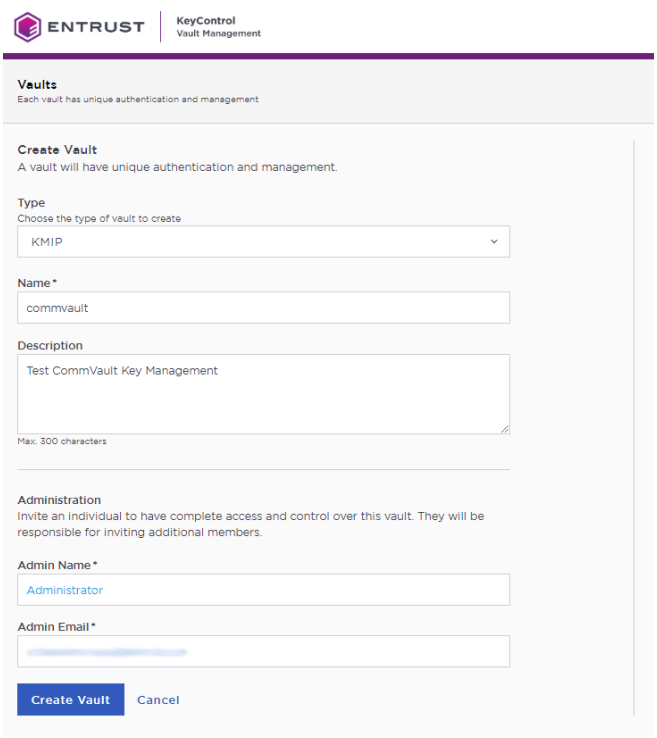
3. In the KeyControl Vault Management interface, select **Create Vault**.



KeyControl Vault supports the following types of vaults:

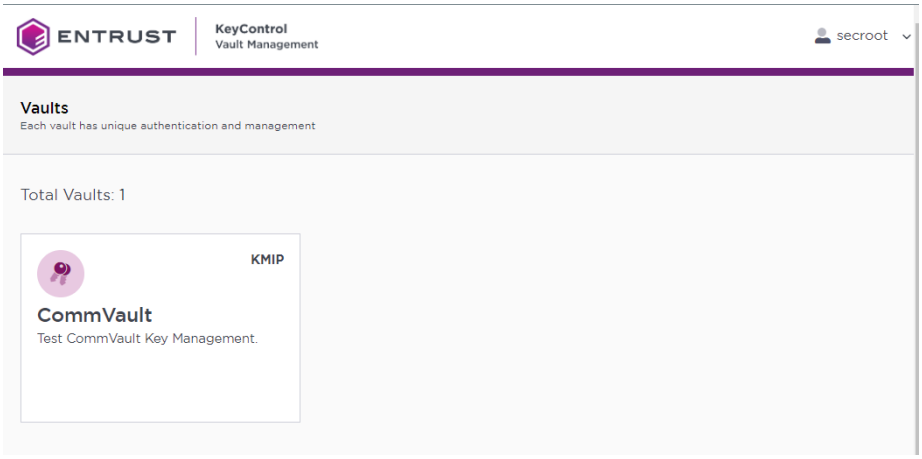
- **Cloud Key Management** - Vault for cloud keys such as BYOK and HYOK.
- **KMIP** - Vault for KMIP Objects.
- **PASM** - Vault for objects such as passwords, files, SSH keys, and so on.
- **Database** - Vault for database keys.
- **Tokenization** - Vault for tokenization policies.
- **VM Encryption** - Vault for encrypting VMs.

4. In the **Create Vault** page, create a **KMIP** Vault:
   a. For **Type**, select **KMIP**.
   b. For **Name**, enter the name of the Vault.
   c. For **Description**, enter the description of the Vault.
   d. For **Admin Name**, enter the name of the administrator of the Vault.
   e. 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 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**.

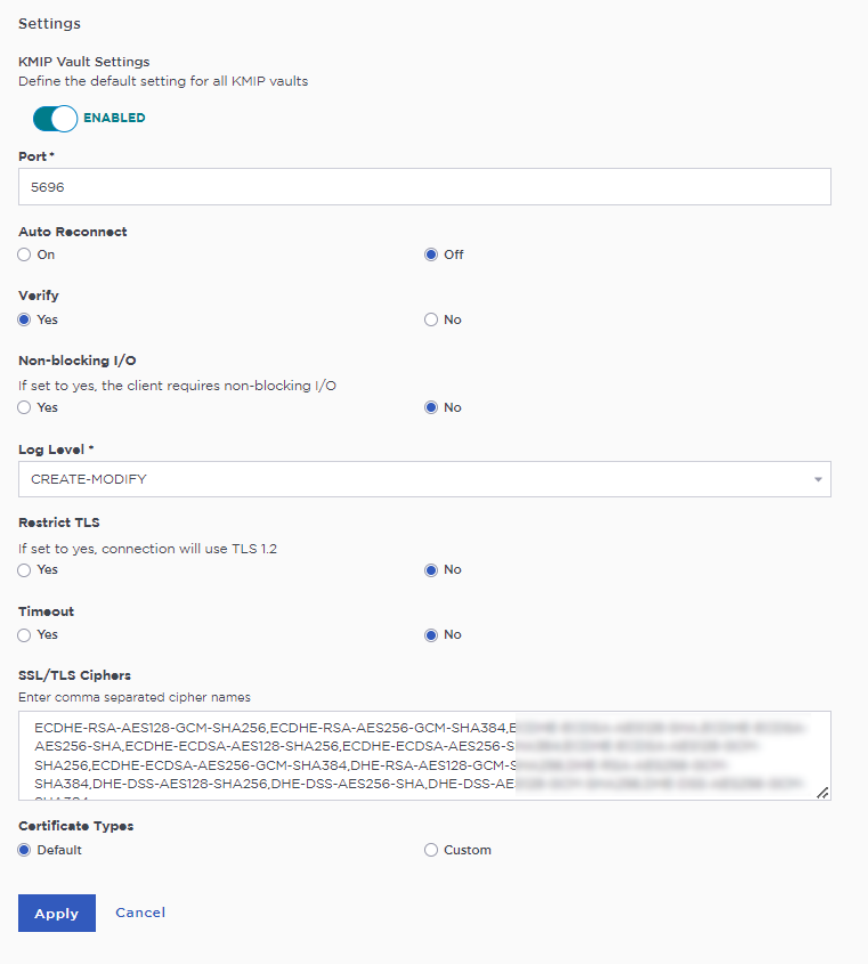
2.2.1. KeyControl KMIP Vault server settings

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 KMIP Client and Server Configuration section of the admin guide.

When using external key management, as is the case in this solution, the KeyControl server is the KMIP server and the Commvault Platform server is the KMIP client.

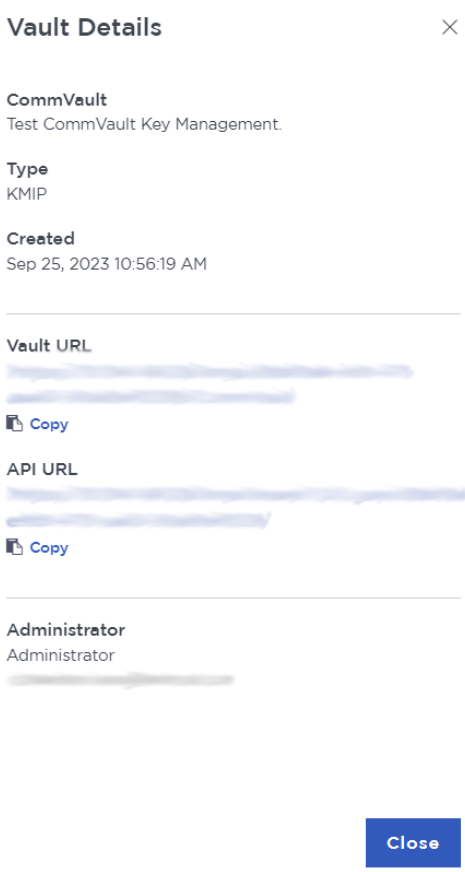
1. Select the **Settings** icon on the top right to view/change the KMIP settings.
   a. The defaults settings are appropriate for most applications.
   b. Make any changes necessary.



2. Select **Apply**.

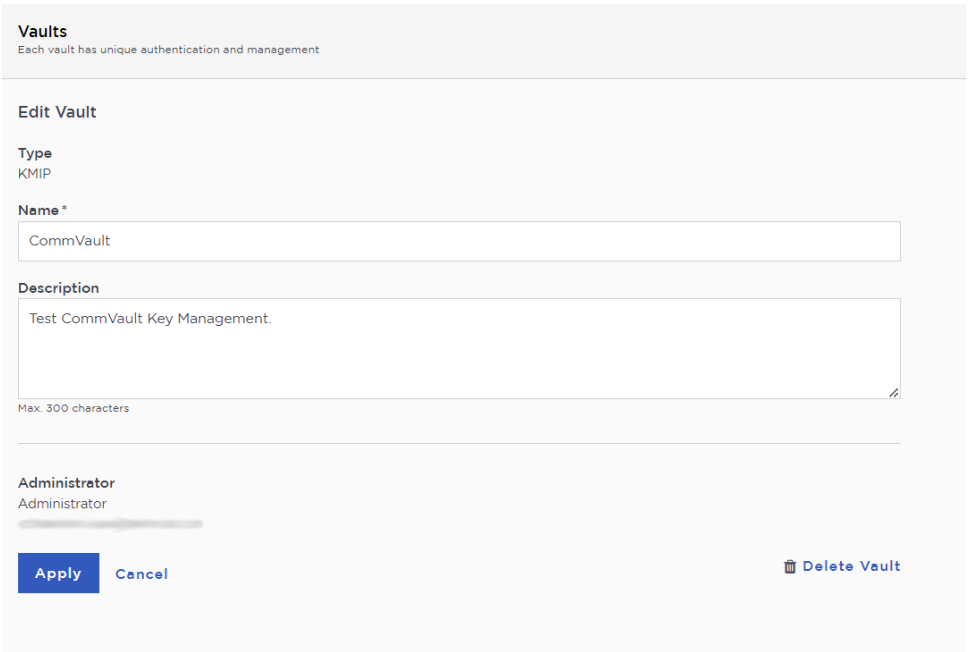
2.2.2. View details for the Vault

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



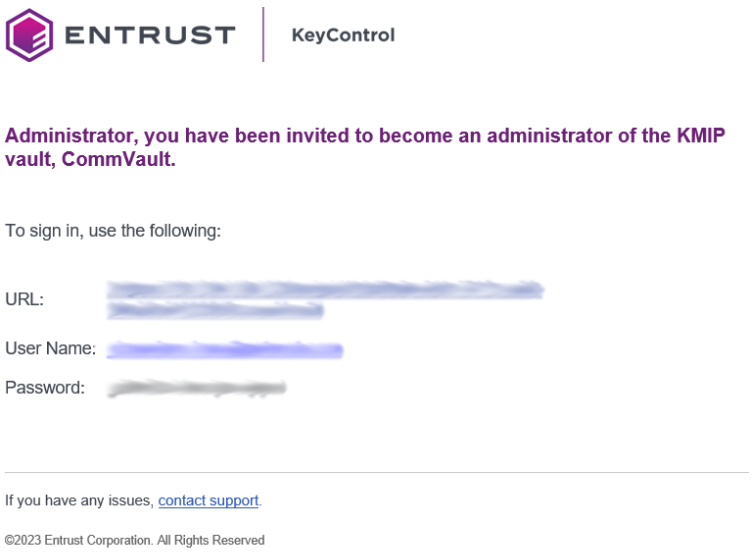
2.2.3. Edit a vault

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



2.2.4. 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.

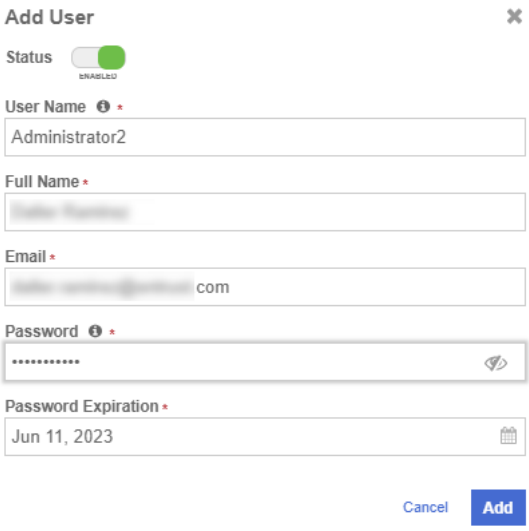
2.2.5. Setup other Administrators

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.

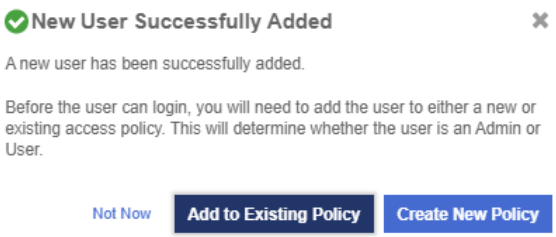
b. Add the user by providing the information requested in the **Add User** dialog.



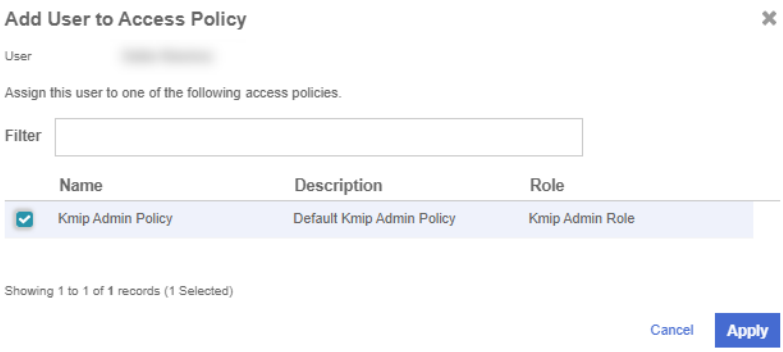
c. Select **Add**.

After the user is added, a window appears which requests selection of the policy to be used by this user.

3. Select **Add to Existing Policy**.



4. On the **Add User to Access Policy** dialog, select the **KMIP Admin Policy** and select **Apply**. The new user is added as an administrator to the Vault.



2.3. Establishing trust between the KeyControl KMIP Vault and the Commvault platform

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

The process below will show how to integrate Commvault platform 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.
   a. The **Create Client Certificate** dialog box appears.
4. In the **Create Client Certificate** dialog box:

   a. Select **Add Authentication for Certificate**.
   b. Enter the username.
   c. Enter the password.
   d. In the **Certificate Expiration** field, set the date on which you want the certificate to expire.
   e. Select **Create**.

   These settings will be used later when the certificates are used in Commvault.

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

5. 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`.

6. Unzip the file so that you have the `certname.pem` and `cacert.pem` file available in the Commvault server for reference.
7. 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 `commvault.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`.

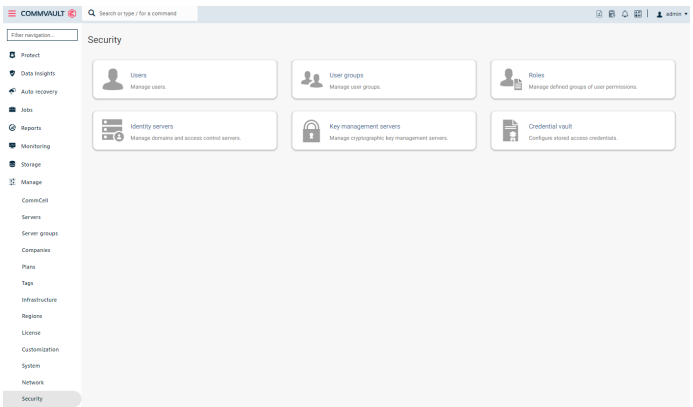
   These files will be used in the Commvault Key Management Server configuration later.

2.4. Adding a Key Management Interoperability Protocol Server - KeyControl to Commvault

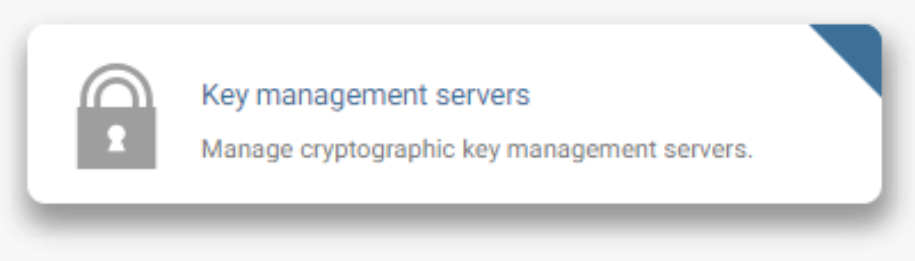
For more detail on how to do this, see Adding a Key Management Interoperability Protocol Server in the Commvault online documentation.

1. Launch the Commvault Web Client and log into to Commvault.
2. From the navigation pane, go to **Manage** > **Security**.

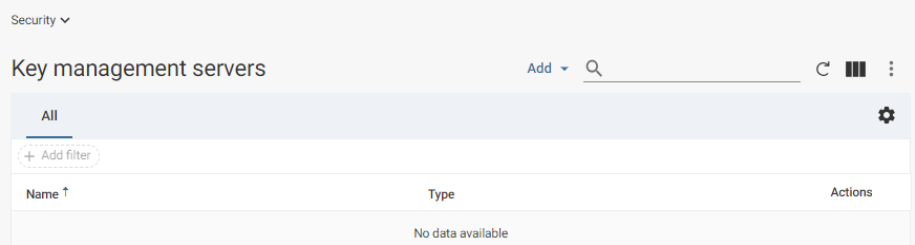
   The **Security** page appears.



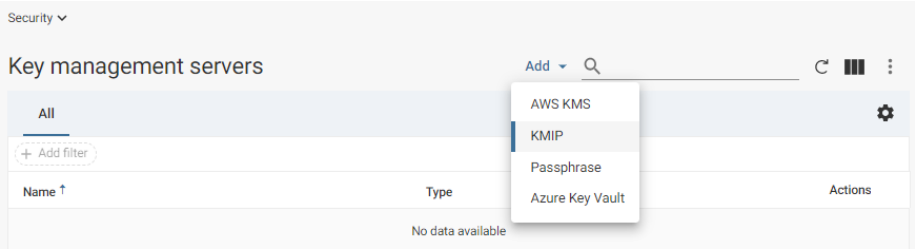
3. Select the **Key management servers** tile.



The **Key management servers** page appears.



4. Select **Add** at the top right, and then select **KMIP**.

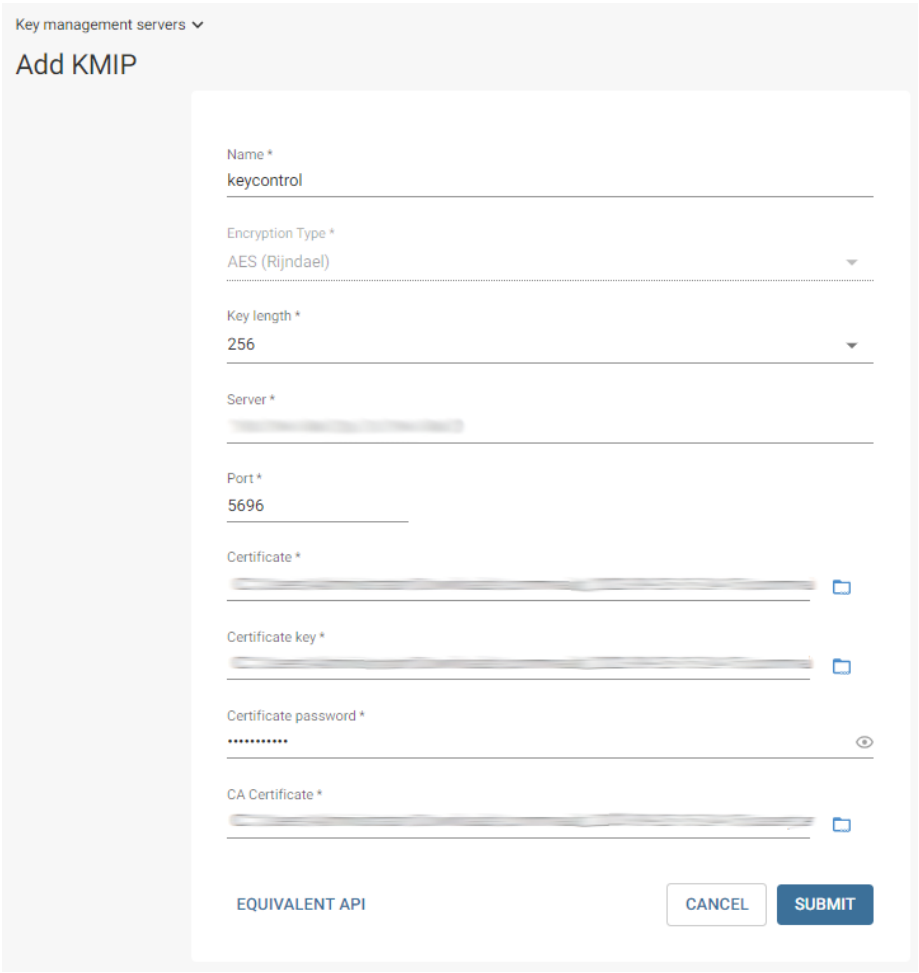


The **Add KMIP** dialog box appears.

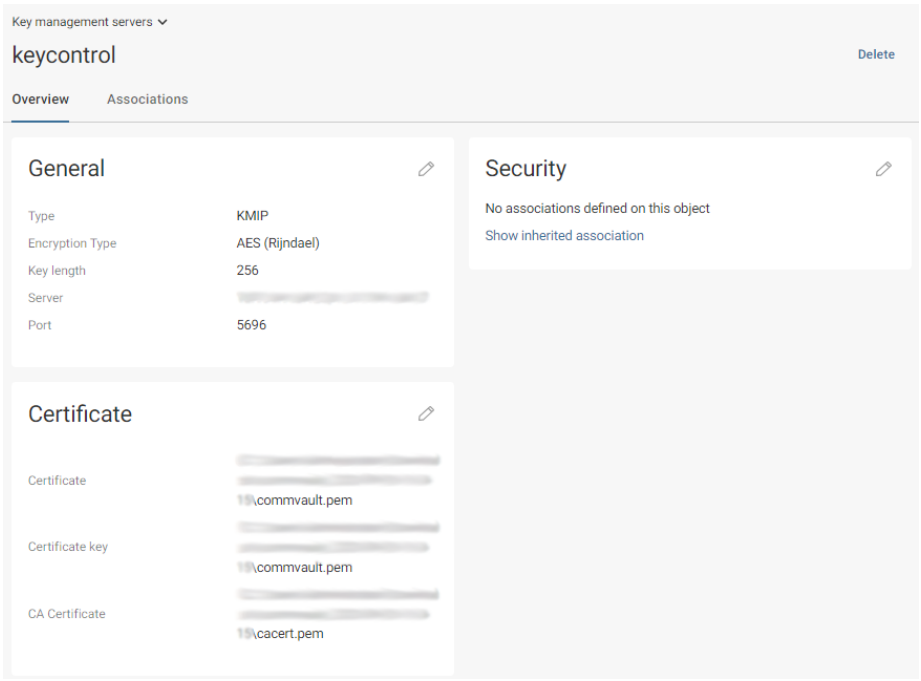
5. Complete the following steps:
   a. **Name**: Enter the name of the key provider (`keycontrol`).
   b. **Key length**: Select the key length to use with the Advanced Encryption Standard (AES) Rijndael cipher.
   c. **Server**: Enter the IP address or the hostname of the third-party key management server.
      i. If the server is a cluster server, then specify the IP addresses or the hostnames of all the servers in the cluster, separated by a comma.
      ii. **Note:** If you use third-party key management servers, and you decide to migrate clients from one CommCell environment to another CommCell environment, then both the source CommCell environment and the destination CommCell environment must use the same third-party key management server.

d. **Port**: Enter the port that is used by the key management server.
    i. If the server is a cluster server, then all the servers in the cluster must use the same port.
e. **Passphrase**: If you set a passphrase when you generated the certificate, then enter the passphrase.
f. **Certificate**: Select the location of the client certificate file. It is in the certificate download zip file from KeyControl. Unzip the file, place in a location and use the location of the file. This file is the `certname.pem` file in the zip file. In our example `commvault.pem`
g. **Certificate key**: Select the location of the client certificate key. This is the same file as the file used for **Certificate** field above.
h. **CA Certificate**: Select the location of the key management server certificate authority (CA) certificate. This file is the `cacert.pem` file located in the same location as the certificate file used above.

6. Select **Submit**.



The KMIP server pane gets displayed with the name of the KMIP server and its configuration.



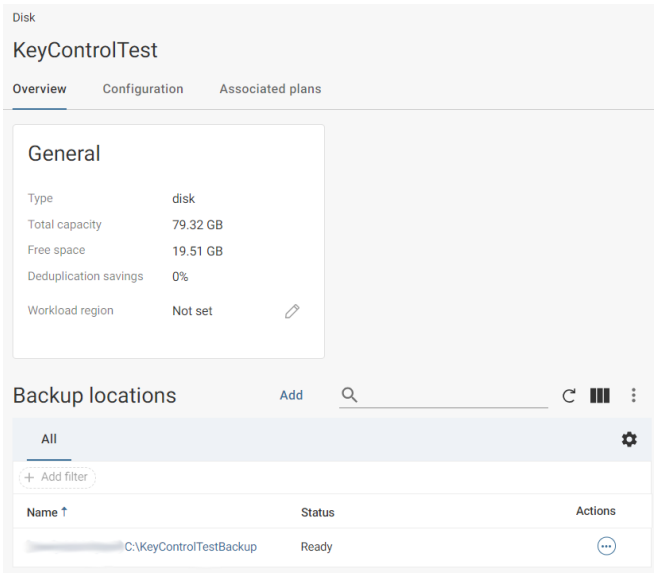
2.5. Test the Key Management server

You can test if Commvault is able to use KeyControl as the Key Management server by Configuring Software Encryption on Disk Storage: Configuring Software Encryption on Disk Storage.

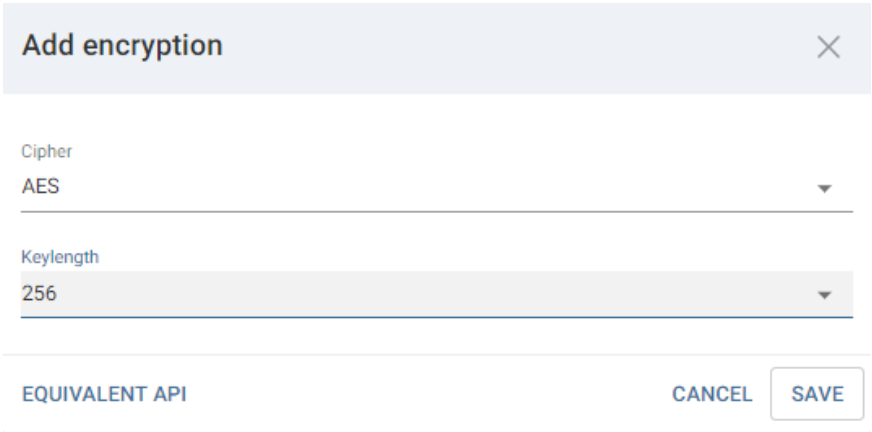
First, Create a Disk Storage pool as outlined in the online documentation.

Now, let's change it so it uses the Key Management Server (KeyControl) to encrypt it.

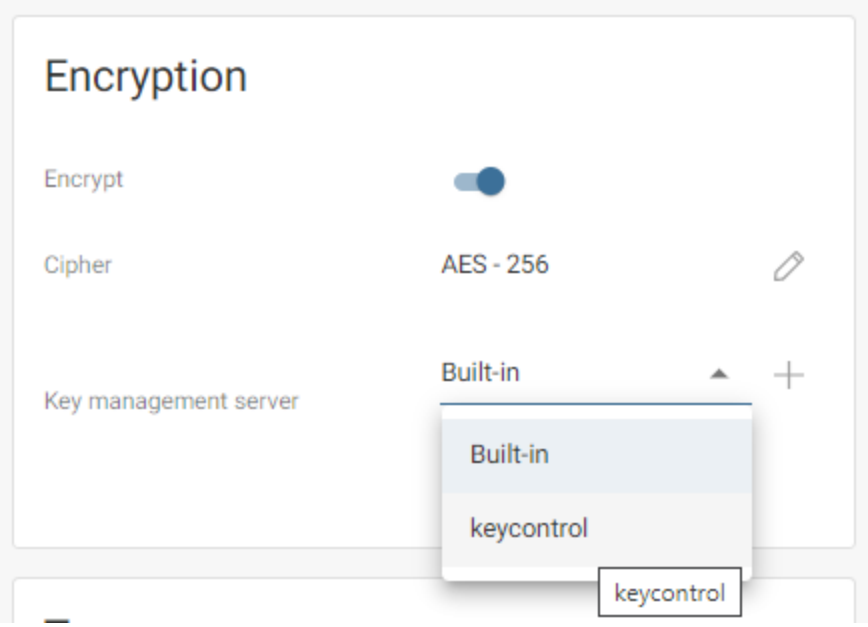
1. From the navigation pane, go to **Storage** > **Disk** > **disk_storage**. (The disk storage just created)
    a. The Disk page appears.
2. Select the disk storage to add software encryption.
    a. The disk storage page appears.



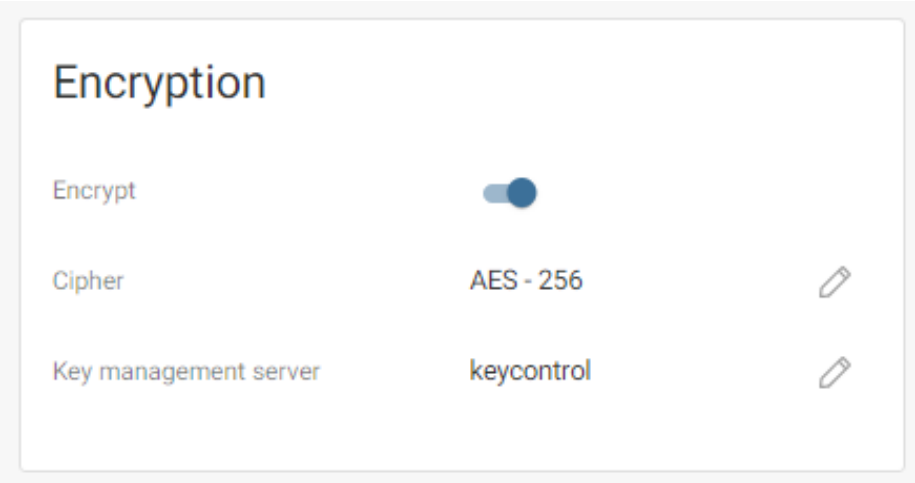
3. On the **Configuration** tab, in the **Encryption** section, move the **Encrypt** toggle key to the right.
    a. The **Add encryption** dialog box appears.
4. Enter the encryption details:
    a. From the **Cipher** list, select an encryption method.
    b. From the **Keylength** list, select an encryption key length.



    c. Click Save.
5. In the **Encryption Title**, edit the **Key Management Server**.
    a. Change it from **Built-in** to the Key management server used during the Key Management server configuration. Select an existing server or add a new server.



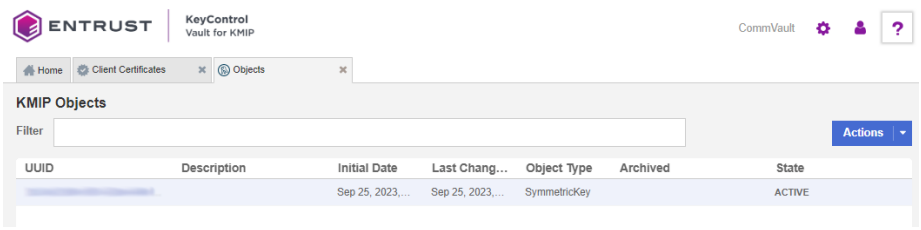
6. Select Save.



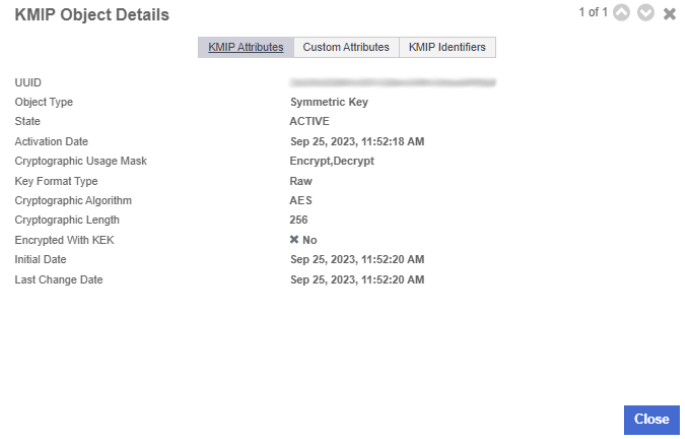
2.5.1. Check KeyControl by looking for the Commvault Keys in the Entrust KeyControl KMIP Vault

Check the disk storage encryption Commvault by looking for keys created in KeyControl:

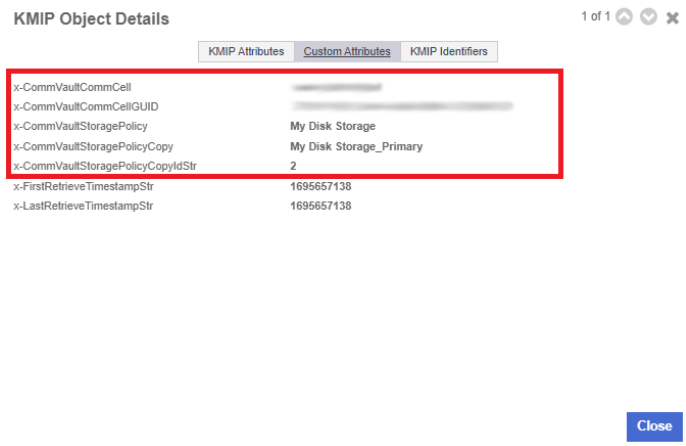
1. Log into the KMIP Vault using the login URL.
2. Select the **Objects** tab to view a list of **KMIP Objects**. This will include the newly created keys. For example:



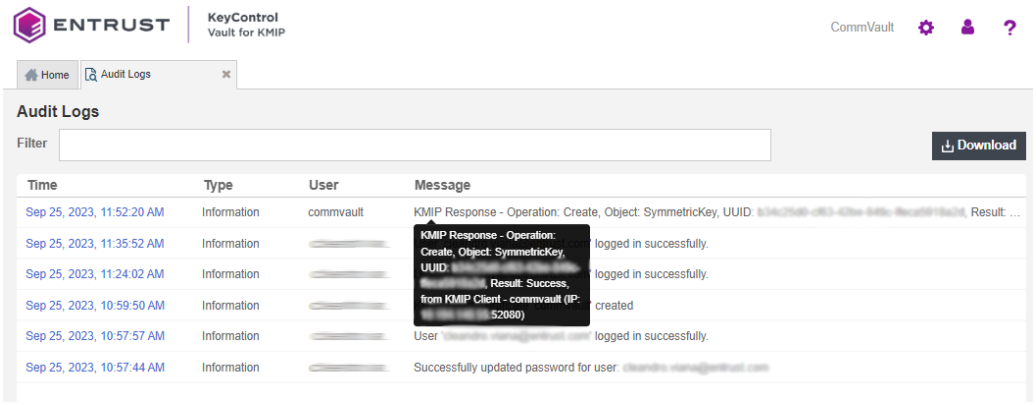
3. Select one of the keys to display its **KMIP Object Details**. For example:



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:


ENTRUST
KeyControl
Vault for KMIP
CommVault
Home
Audit Logs
Audit Logs
Filter
Download
Time
Type
User
Message
Sep 25, 2023, 11:52:20 AM
Information
commvault
KMIP Response - Operation: Create, Object: SymmetricKey, UUID:
Result: ...
Sep 25, 2023, 11:35:52 AM
Information
logged in successfully.
Sep 25, 2023, 11:24:02 AM
Information
logged in successfully.
Sep 25, 2023, 10:59:50 AM
Information
created
Sep 25, 2023, 10:57:57 AM
Information
User
logged in successfully.
Sep 25, 2023, 10:57:44 AM
Information
Successfully updated password for user
KMIP Response - Operation: Create, Object: SymmetricKey, UUID:
Result: Success, from KMIP Client - commvault (IP:
52080)

Chapter 3. Additional resources and related products