Veeam Backup & Replication and Entrust KeyControl®

Integration Guide

2025-04-02

Table of Contents

Chapter 1. Introduction

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

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.
- Veeam Backup & Replication.

1.2. Product configuration

Product	Version
Windows	Windows 2022
Veeam Data Backup & Replication	12.1.0.2131
Entrust KeyControl	10.2

1.3. Supported features

The following Entrust KeyControl features have been tested in this integration.

Entrust KeyControl Feature	Support
Deployment in Nutanix AHV from ISO	Yes

Entrust KeyControl Feature	Support
Cluster Mode	Yes
Cluster Expansion	Yes
Node Removal	Yes
Retain Configuration After Total Cluster Power-Down	Yes

Support for the following Veeam Backup & Replication features have been tested in this integration.

Veeam Backup & Replication Feature	Support
Data-at-Rest Encryption	Yes
Re-Keying	Yes

1.4. Requirements

Veeam Backup & Replication requires the following certificates:

- A certificate issued by a certificate authority to authenticate the KeyControl KMIP server.
- A client certificate created by KeyControl.

A local certificate authority (A) is required, with both Veeam Backup & Replication and KeyControl in the domain. The local CA does not have to be a subordinate of a trusted CA.

Chapter 2. Deploy and configure Entrust KeyControl

The following steps summarize the deployment of the Entrust KeyControl:

- Deploy Entrust KeyControl cluster
- Request root certificate for the Entrust KeyControl vault
- Install root certificate in the Entrust KeyControl vault
- Create a KMIP Vault in the Entrust KeyControl
- View the KMIP Vault details
- Edit the KMIP Vault
- Add KMIP Vault Administrators
- Create the Entrust KeyControl client certificate bundle

2.1. Deploy Entrust KeyControl cluster

A two-node cluster was deployed for this integration. See the KeyControl online documentation.

KeyControl can be deployed on VMware using the OVA image, or Nutanix AHV and Microsoft Hyper-V using the ISO image. These images are available from Entrust TrustedCare.

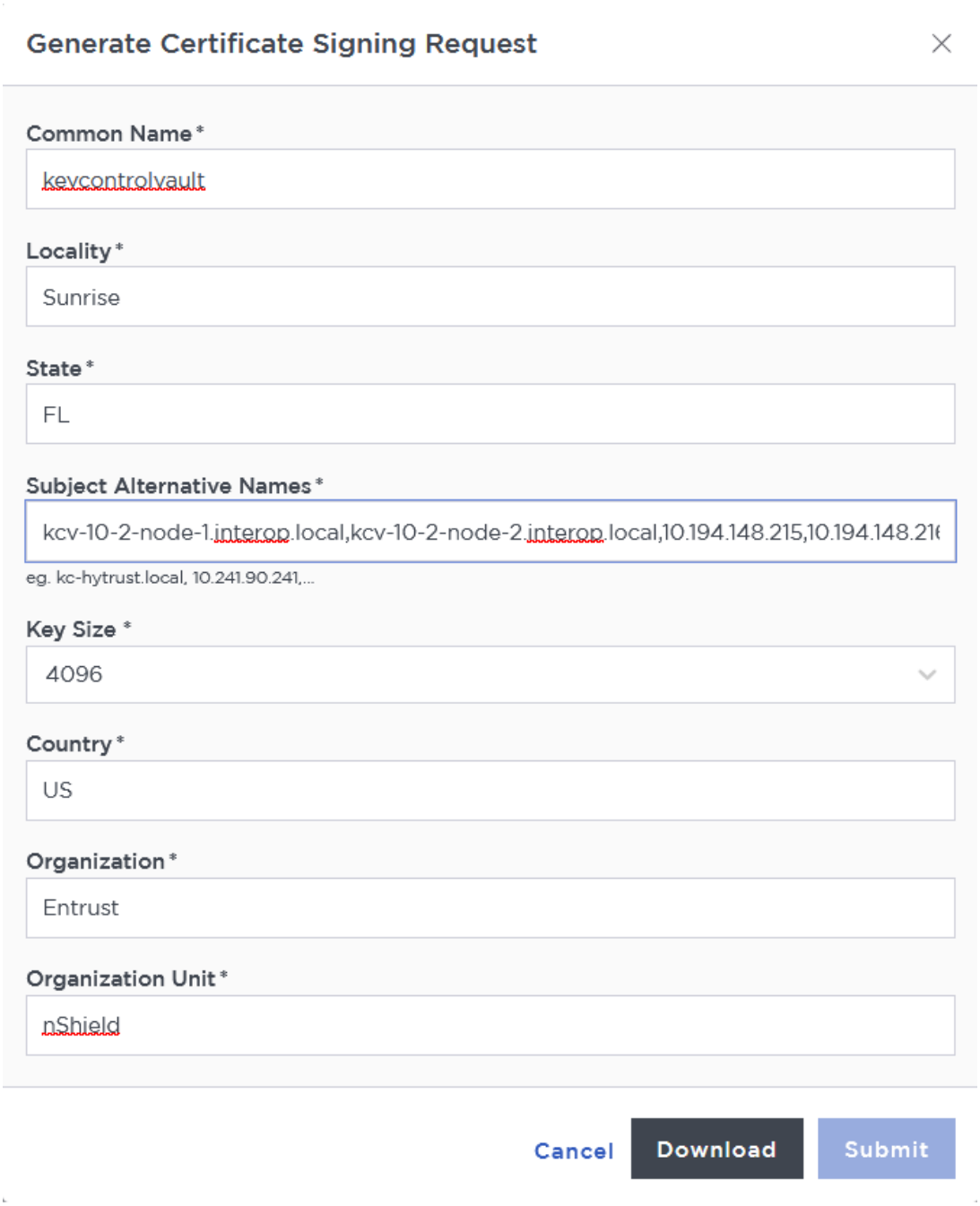
2.2. Request root certificate for the Entrust KeyControl vault

Any CA can be used, for the purpose of this integration a Microsoft Windows CA configured as a local root was utilized.

1. Log into the Entrust 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. In the **Vault Management** dashboard, select the **Settings** icon on the top right.
3. Select the **Action** icon pull-down menu. Then select **Generate CSR**.
4. Enter your information.

Include the FQDN and / or IP of all the Entrust KeyControl nodes in the **Subject Alternative Names**.

For example:



5. Issue a certificate for the CSR created above using the local root CA.
   a. Log into your local root CA with Administrator privileges.
   b. Copy the CSR created above to a local folder.
   c. Launch the **certsvr** application.
   d. Right-click on the **<certification authority name>** in the left pane and select **All Tasks / Submit new request...**.
   e. Select the copied CSR.

f. Select **<certification authority name>** / **Pending Request** in the left pane.

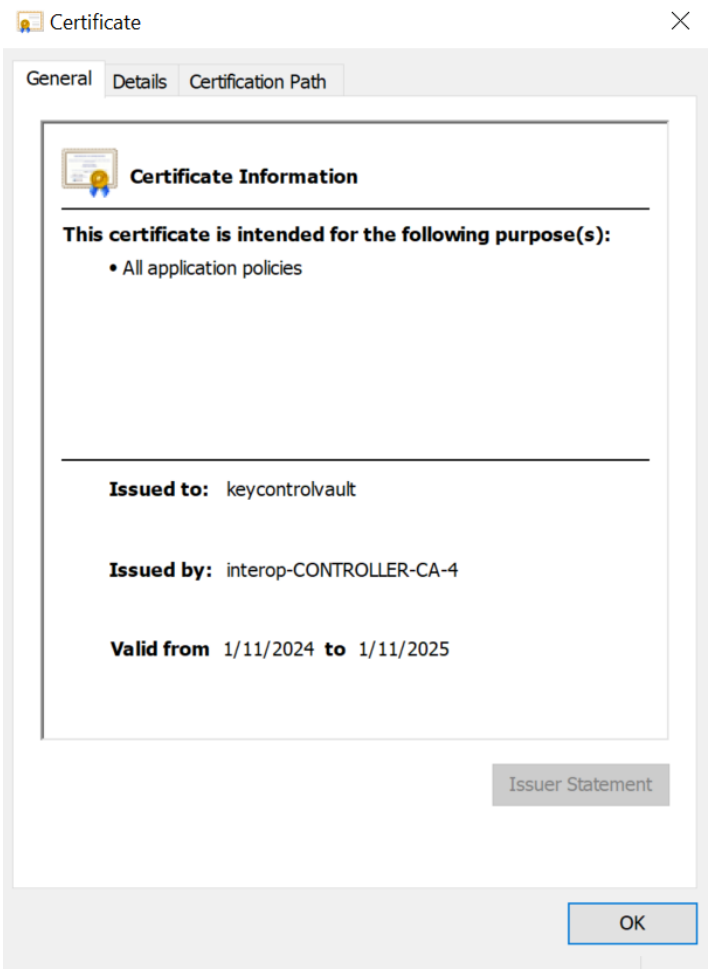
g. Right-click on the request in the right pane and select **All Tasks** / **Issue**.

h. Select **<certification authority name>** / **Issued Certificates** in the left pane.

i. Select the certificate.

j. Select the **Details** tab / **Copy to File...**. Follow the instructions, selecting **Base-64 encoded X.509** in **Export File Format**.

For example:



6. Export the local root CA certificate in pem format.

```
C:\Users\Administrator>certutil -ca.cert C:\Users\Administrator\Downloads\rootcacert.cer
CA cert[0]: 3 -- Valid
CA cert[0]:
-----BEGIN CERTIFICATE-----
MIIDlzCCAn+gAwIBAgIQPaxaYmRa1atOVpZms+TaZjANBgkqhkiG9w0BAQsFADBS
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFzAVBgoJkiaJk/IsZAEZFgdpbnRlcm9w
MSAwHgYDVQQDExdpbnRlcm9wLUNPTlRST0xMRVItQ0EtNDAeFw0yNDAxMTEyMTEx
MzZaFw0zNDAxMTEyMTIxMzZaMFIxFTATBgoJkiaJk/IsZAEZFgVsb2NhbDEXMBUG
CgmSJomT8ixkARkWB2ludGVyb3AxIDAeBgNVBAMTF2ludGVyb3AtQ09OVFJPTExF
Ui1DQS00MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2rthVuA/D9c3
pRcg1OKXayMBSTEurG0H6icp09re683suJoGDxBBV1Qp0+I6v2PwkkDD46lYlhCn
ycr/+UenUS0As30NM9FbWejVdYBH2JHhHZDi2A9HyprWVFb+tLktX1VXbwTXP3QO
+WPIEBtXRXTyP0ivkuMVRuyEd+qwTzvldjUGd0j5pRMb2cmI/sFRKN9CjDBNxDDX
```

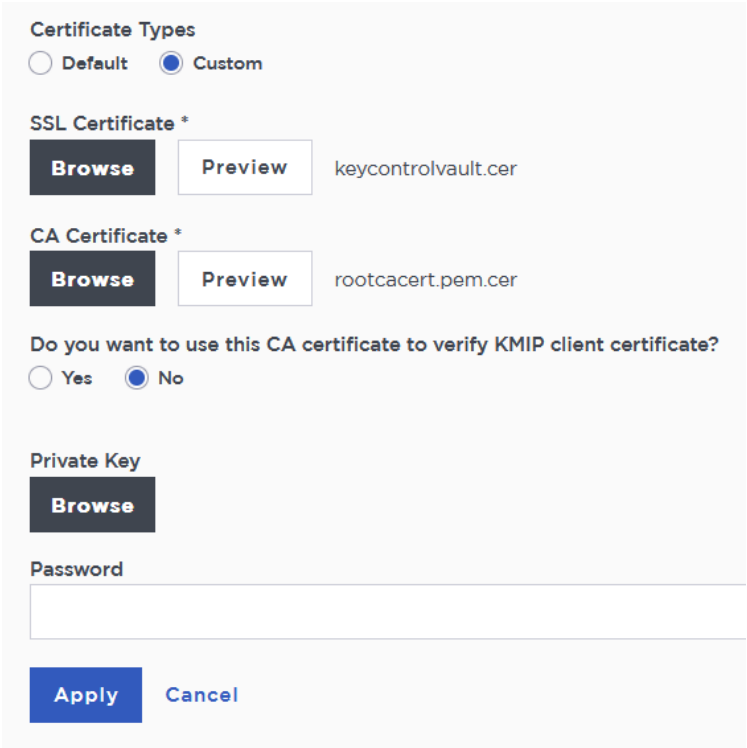
```
z/wKB+Kaf9n6oh7RrWXIh5+v/N3gI4EG8z2fL0l0TmPzWdTafg9edvSnOviKVrmT
qzGmxlT6DQt8xGRecDiJMH3+9R3XvRLhflcpANdqMAZnNipDCx4re4+DBH7S8mSh
Vr1nK2xybQIDAQABo2kwZzATBgkrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUYzwTn023Ko23BcNb3u5i
zpQLc5QwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQELBQADggEBACmiaN0t
tBkyzkxpWy5xA+ePDyCBFLuQ6W1BByI6TCPOLp6CFsmYg9NB4c61+Y5lpIQhDJFf
AODT1LZRTq6b5h8vl1GdNzim2wPrtjviNvmQ0Q5R/2tJzR9D3SB6Hv+bU5lRP7j/
giWpEx5ImmmfG7BJ4DxWxpA2sooC02iP2TOw5GJcI+varjKNCsyYSiyYhigOpnh/
3ZlpMv2IGB/YykLfCPL2SOtYq0LcAnniiXmxx9iylgZwi3xQPx35JLn8b2Mrg0qI
iMaAoCzJXU09aZcMv+ZCQ27PaowRmxx+WSdYt8ZORP+cHC+xemLyamnyxzXp07qE
MsNUdQy+Lo5h5XI=
-----END CERTIFICATE-----

CertUtil: -ca.cert command completed successfully.

C:\Users\Administrator>certutil -encode C:\Users\Administrator\Downloads\rootcacert.cer
C:\Users\Administrator\Downloads\rootcacert.pem.cer
Input Length = 923
Output Length = 1328
CertUtil: -encode command completed successfully.
```

7. Copy the `keycontrolvault` certificate and the `rootcacert.pem.cer` to a location in the Entrust KeyControl Vault server.

2.3. Install root certificate in the Entrust KeyControl vault

The KMIP server settings are set at the Entrust KeyControl appliance level and apply to all the KMIP vaults. See KMIP Client and Server Configuration.

1. Log into the Entrust KeyControl Vault server web user interface.
2. In the **Vault Management** dashboard, select the **Settings** icon on the top right.
3. Select **Custom** radio button in **Certificate Types**.
4. Browse and select the certificate as shown.



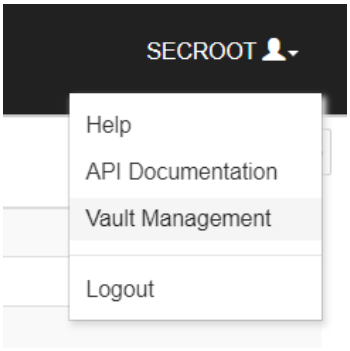
5. The other defaults settings are appropriate for most applications. Make any changes necessary.
6. Select **Apply**.

2.4. Create a KMIP Vault in the Entrust KeyControl

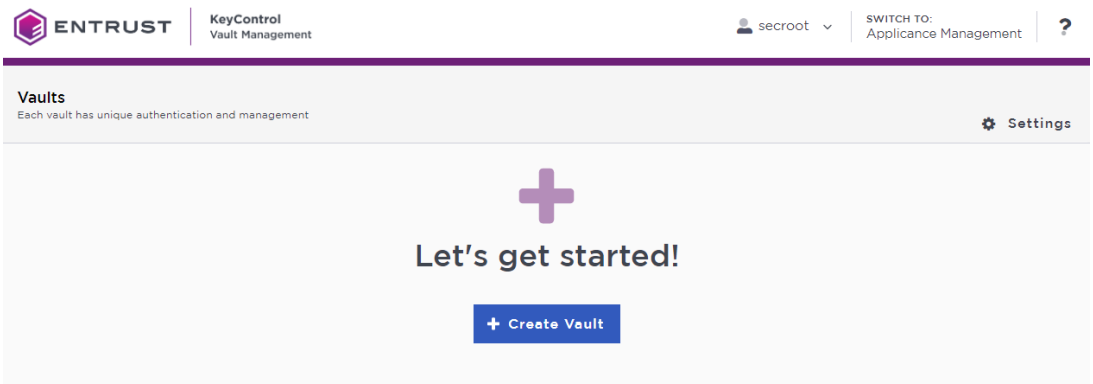
The KeyControl Vault appliance supports different type of vaults that can be used by all type of applications. This section describes how to create a KMIP Vault in the KeyControl Vault Server.

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**.



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



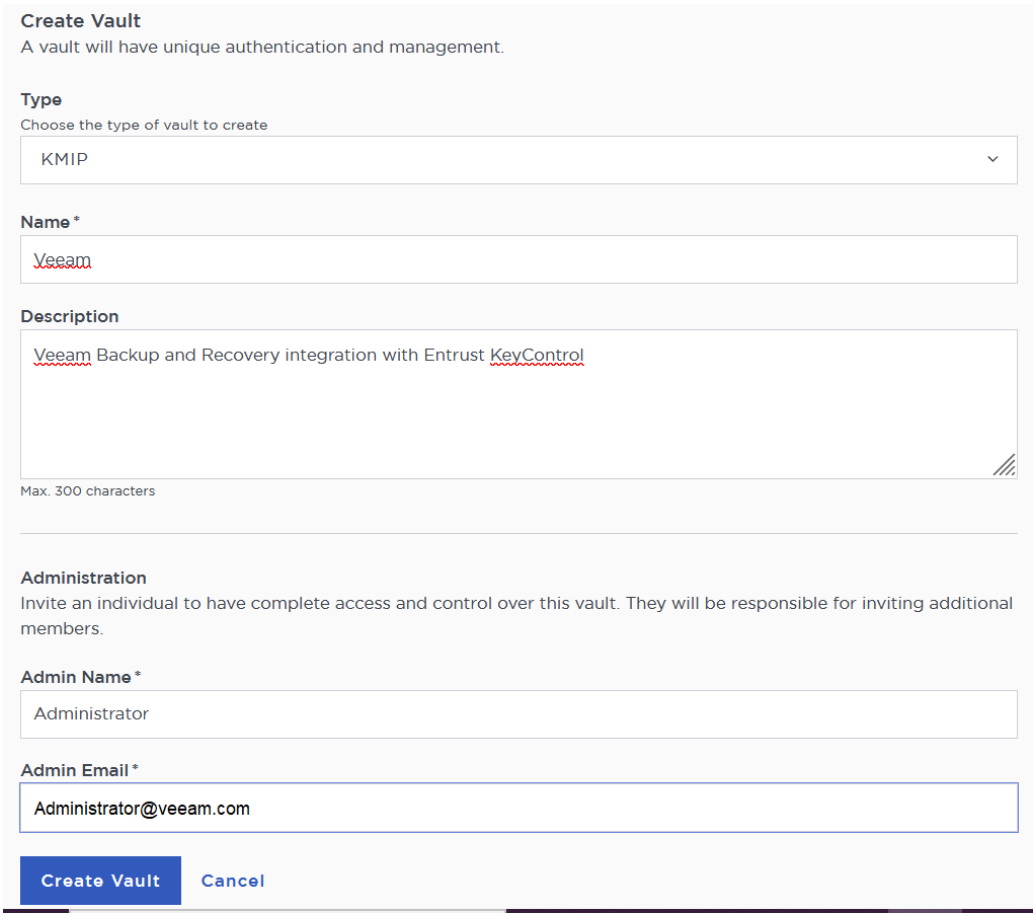
KeyControl Vault supports the following types of vaults:

- **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.

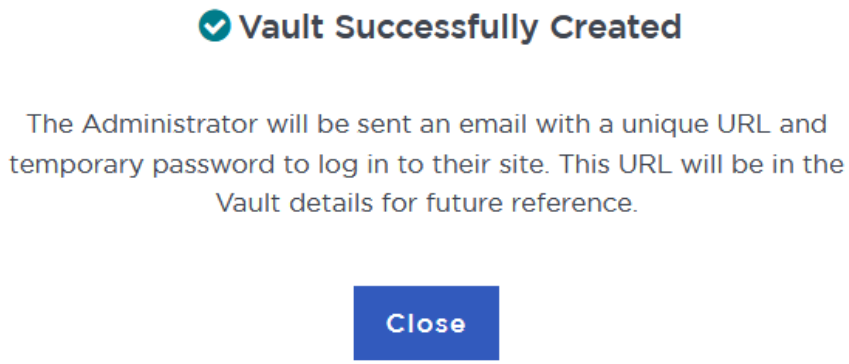
4. In the **Create Vault** page, create a **KMIP** Vault:

Field	Value
Type	**KMIP**
Name	Vault name
Description	Vault description
Admin Name	Vault administrator username
Admin Email	Vault administrator email

For example:

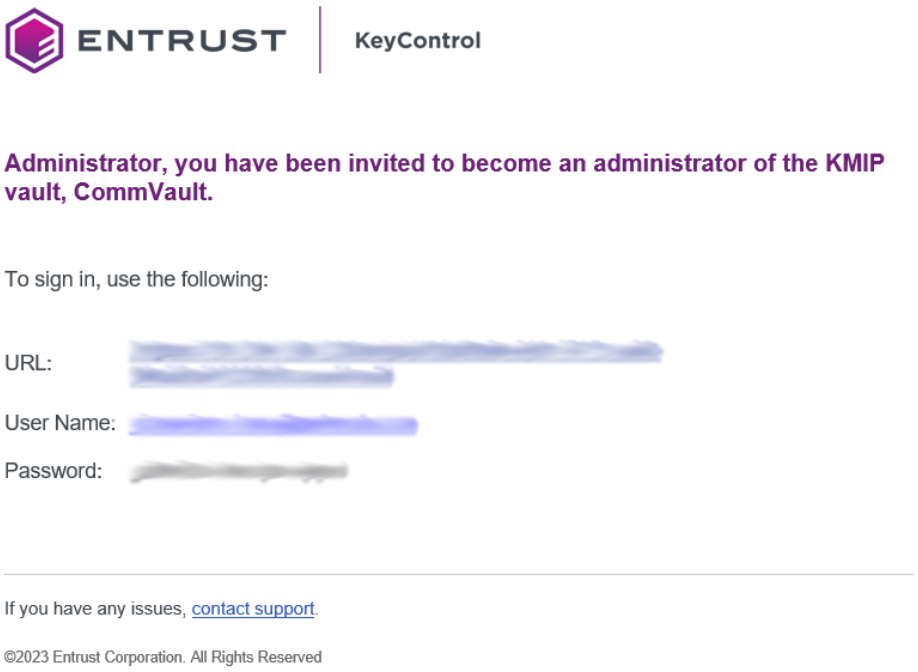


5. Select **Create Vault**. Then select **Close**.



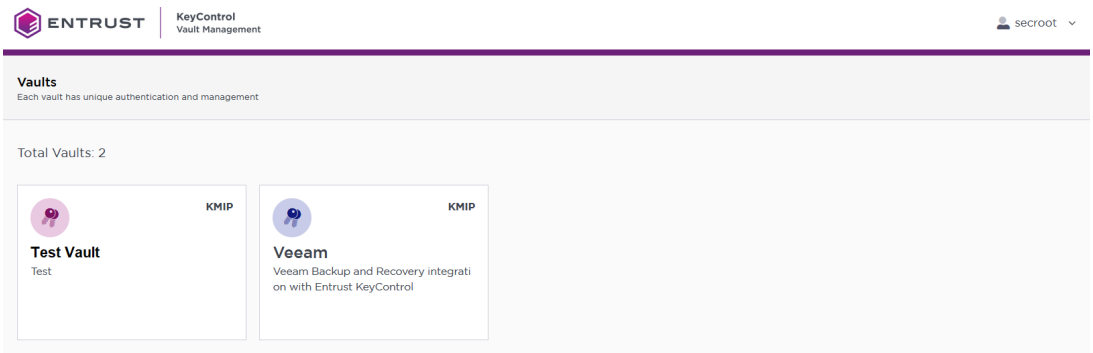
The newly created vault URL and login credentials will be emailed to the administrator's email address entered above. In closed gap environments where email is not available, the URL and login credentials are displayed at this time.

Example email:



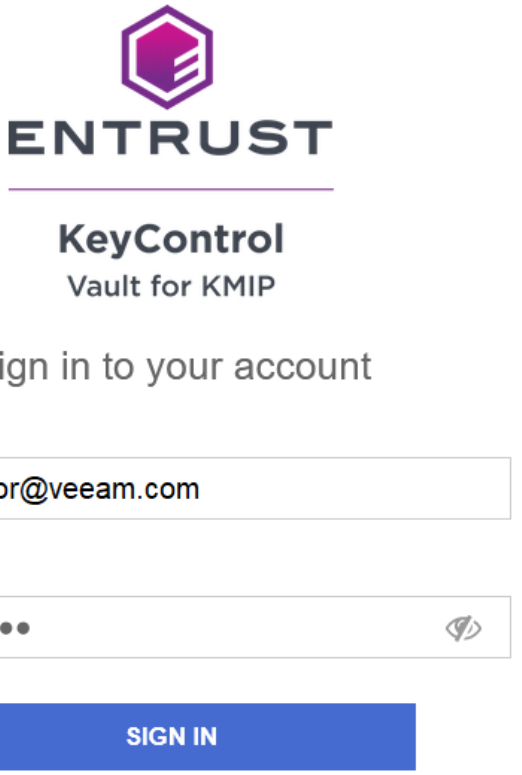
6. Bookmark the URL and save the credentials. Then select **Close** if the URL and login credentials are displayed.
7. The newly created Vault is added to the **Vault Management** dashboard.

   For example:



8. Login to the URL provided above with the temporary password. Change the initial password when prompted. Sign in again to verify.

   For example:



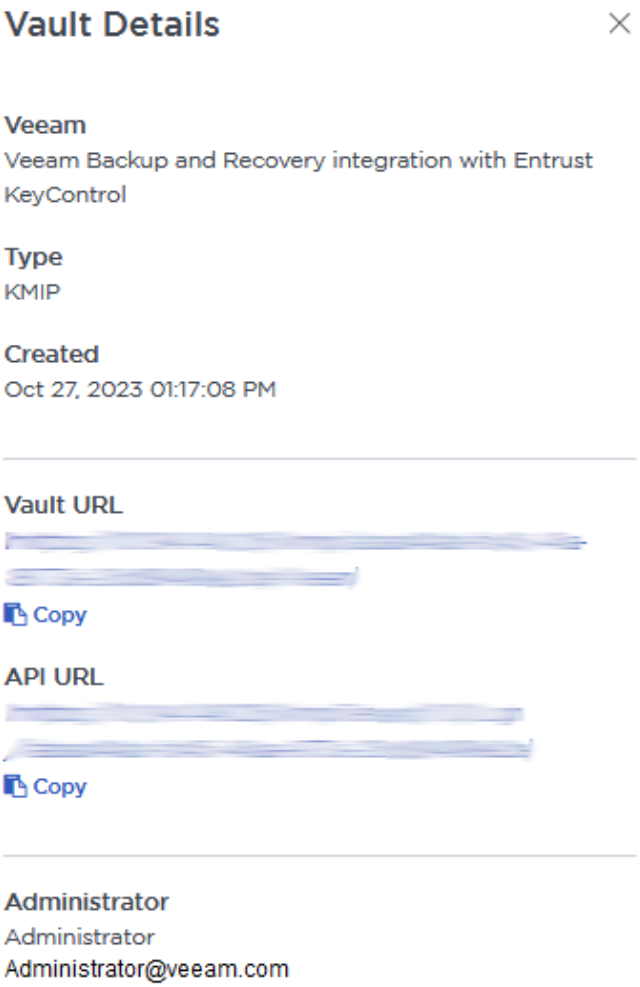
9. Notice the new vault.

   For example:

2.5. View the KMIP Vault details

1. Hover over the Vault and select **View Details**.

   For example:

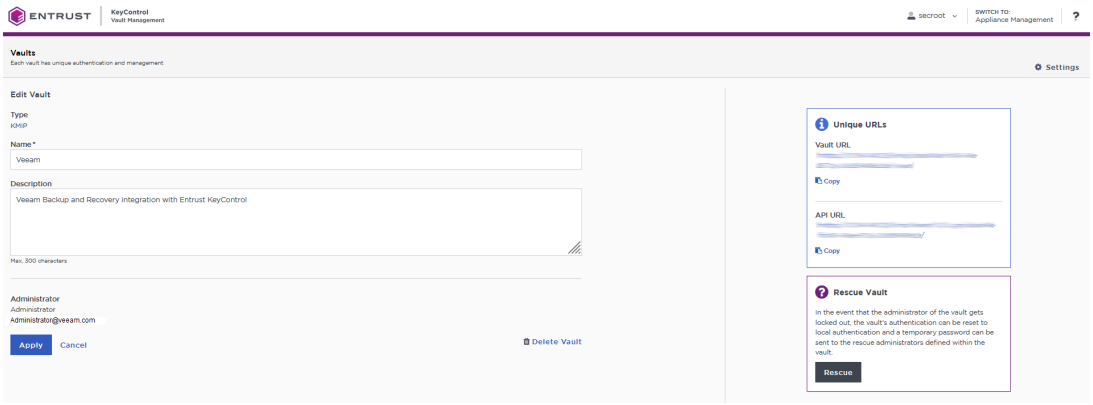


2. Select **Close** when done.

2.6. Edit the KMIP Vault

1. Select **Edit** when you hover over the Vault.

   For example:



2. Select **Apply** when done.

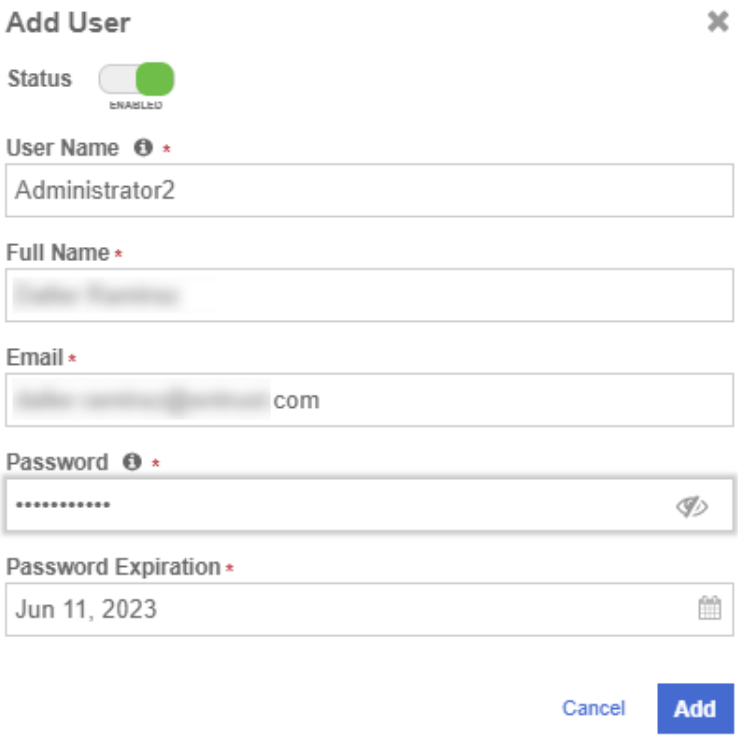
2.7. Add KMIP Vault Administrators

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.

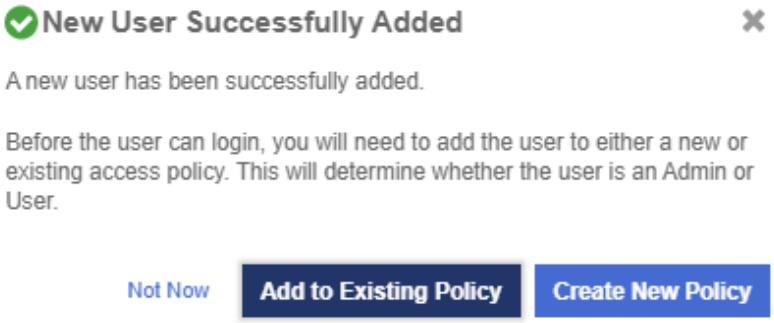
      For example:



c. Select **Add**.

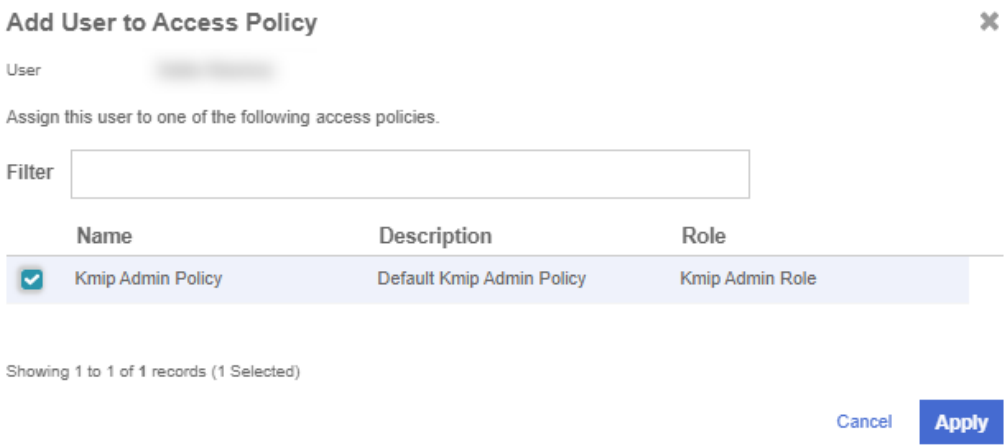
After the user is added, a window appears which requests selection of the policy to be used by this user.

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.

For example:



2.8. Create the Entrust KeyControl client certificate bundle

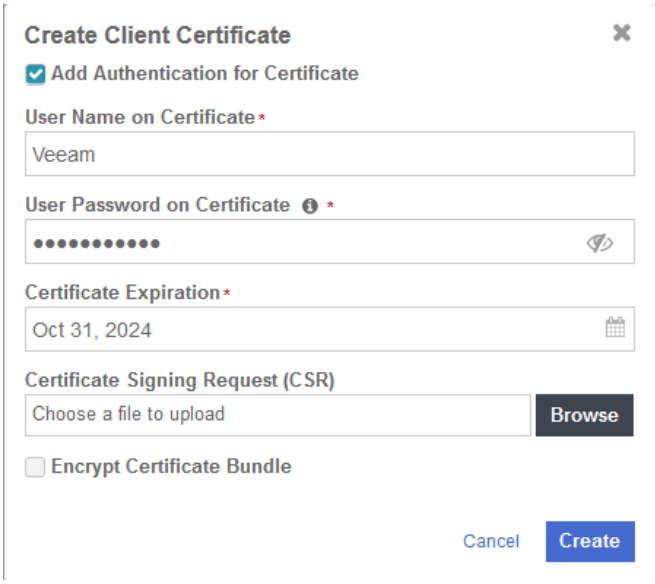
Certificates are required to facilitate the KMIP communications from the Entrust KeyControl KMIP Vault and Veeam Backup & Replication application and conversely. The built-in capabilities in Entrust KeyControl are used to create and publish the certificate.

1. Login to the KMIP Vault with the URL and credentials from Create a KMIP Vault in the Entrust KeyControl.
2. Select **Security**, then **Client Certificates**.

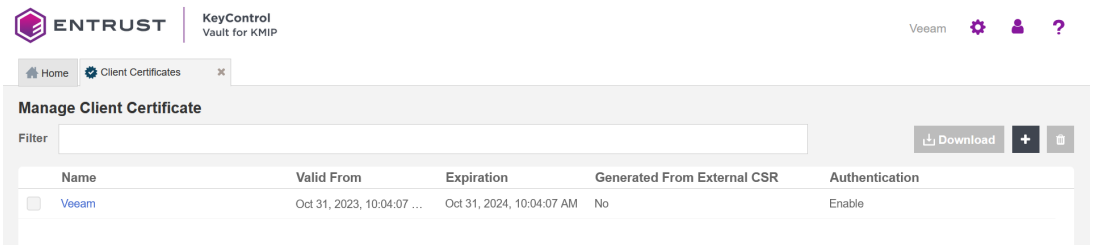
3. In the **Manage Client Certificate** page, select the **+** icon on the right to create a new certificate. The **Create Client Certificate** dialog box appears.
4. In the **Create Client Certificate** dialog box:

    a. Select **Add Authentication for Certificate**.
    b. Enter the username.
    c. Enter the password.
    d. Enter the expiration date.
    e. Leave **Certificate Signing Request (CSR)** field as default.
    f. Select **Create**.

    For example:



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



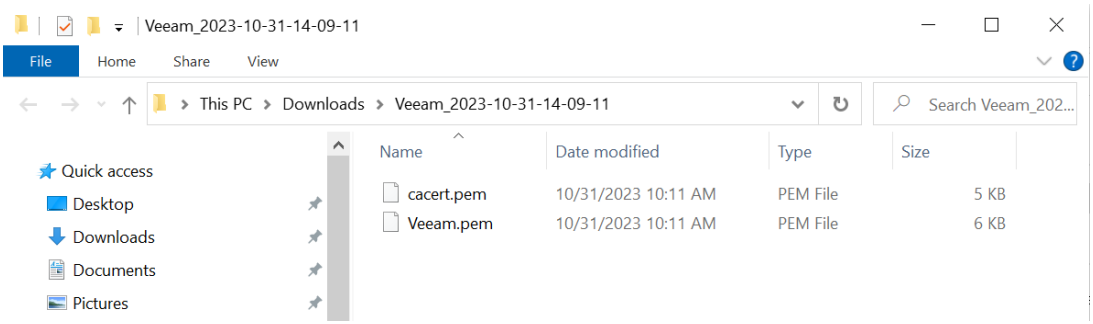
5. Select the certificate and select the **Download** icon to download the certificate.
6. Unzip the downloaded file. It contains the following:

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

     The client certificate section of the `certname.pem` file includes the lines "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" and all text between them.

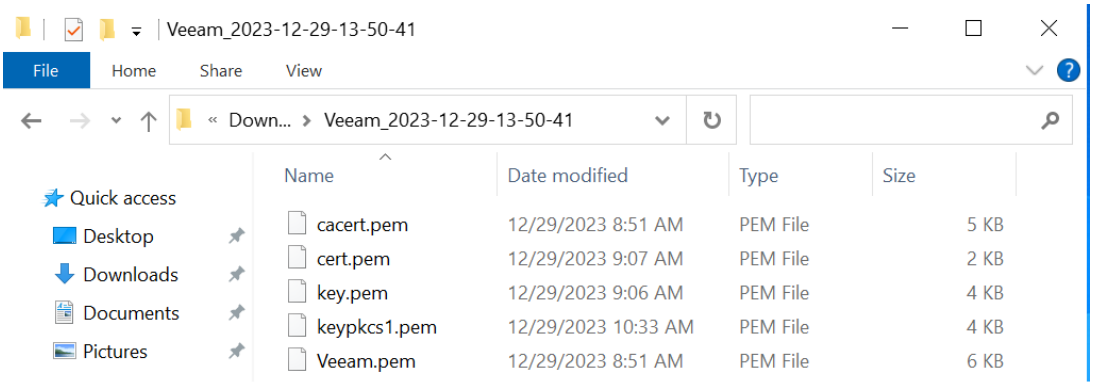
     The private key section of the `certname.pem` file includes the lines "-----BEGIN PRIVATE KEY-----" and "-----END PRIVATE KEY-----" and all text in between them.

   - A `cacert.pem` file which is the root certificate for the KMS cluster. It is always named `cacert.pem`.



7. Create two new files named `cert.pem` and `key.pem`. File `cert.pem` content is the client certificate section of `Veeam.pem`. File `key.pem` content is the private key section of `Veeam.pem`.
8. Convert `key.pem` into a PKCS #11 format by using the following command. choco install openssl. Save these Files for later use in Veeam Backup & Replication KMS Configure Section.

```
> openssl pkey -in key.pem -out keypkcs1.pem -traditional
```



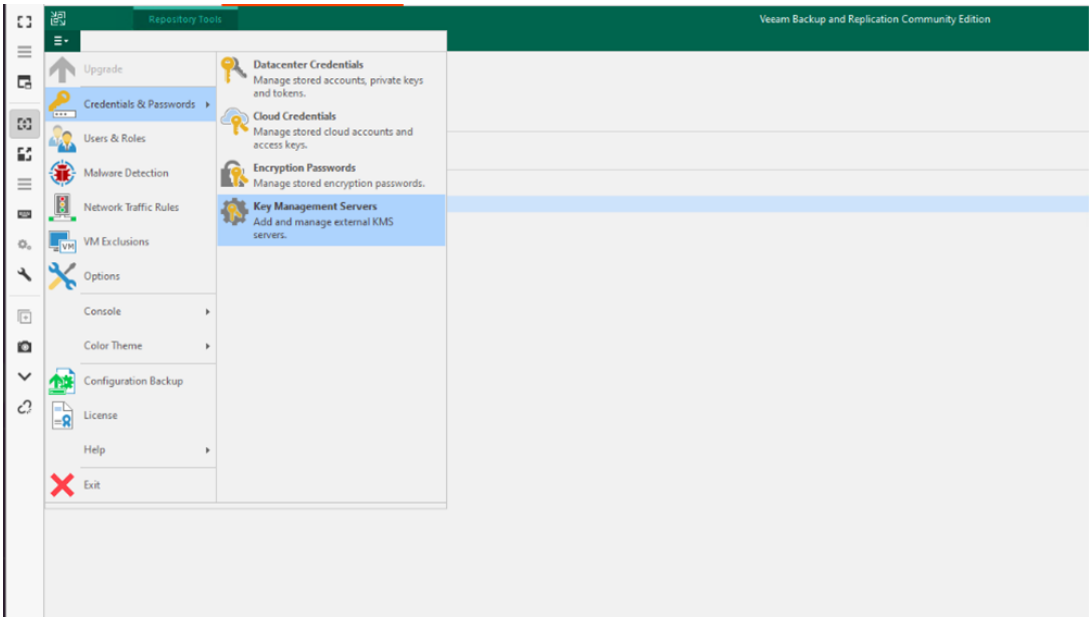
Chapter 3. Install Veeam Backup & Replication

1. Download the Veeam Backup & Replication image version v12.1 or newer from the Veeam Product Download Page. The KMS feature is available from v12.1 onwards.
2. Install the Veeam Backup & Replication as shown in the Veeam Backup & Replication Quick Start Guide.

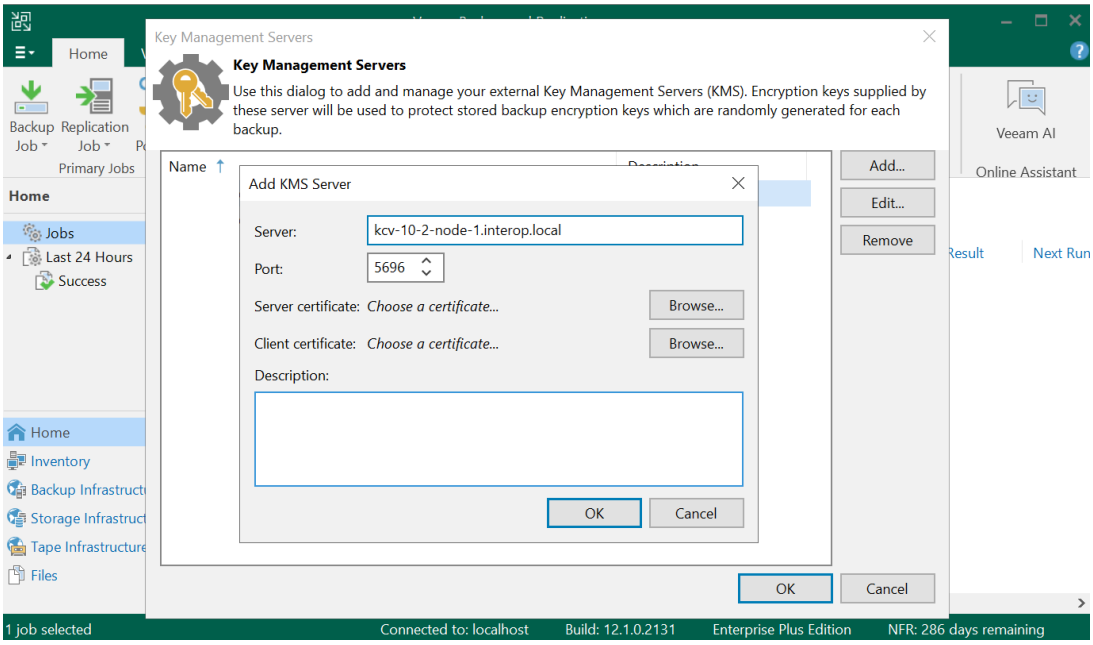
Chapter 4. Integrate Entrust KeyControl with Veeam Backup & Replication

Follow these steps to register Entrust KeyControl as a KMS in Veeam Backup & Replication. For more detail on how to do this, see Adding a Key Management Interoperability Protocol Server in the Veeam Backup & Replication online documentation.

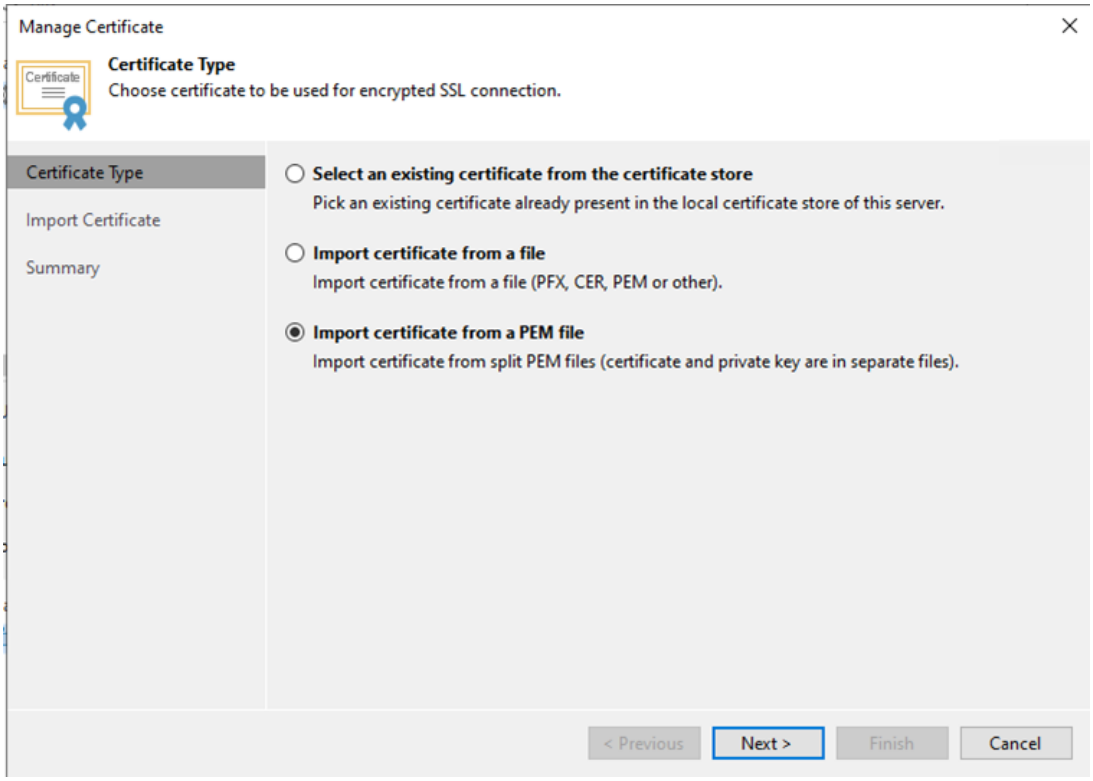
1. Select **Windows Start / Veeam / Veeam Backup & Replication Console**.
2. Login with the Windows credentials.
3. Select the menu icon the top left **Credentials & Passwords / Key Management Servers**.



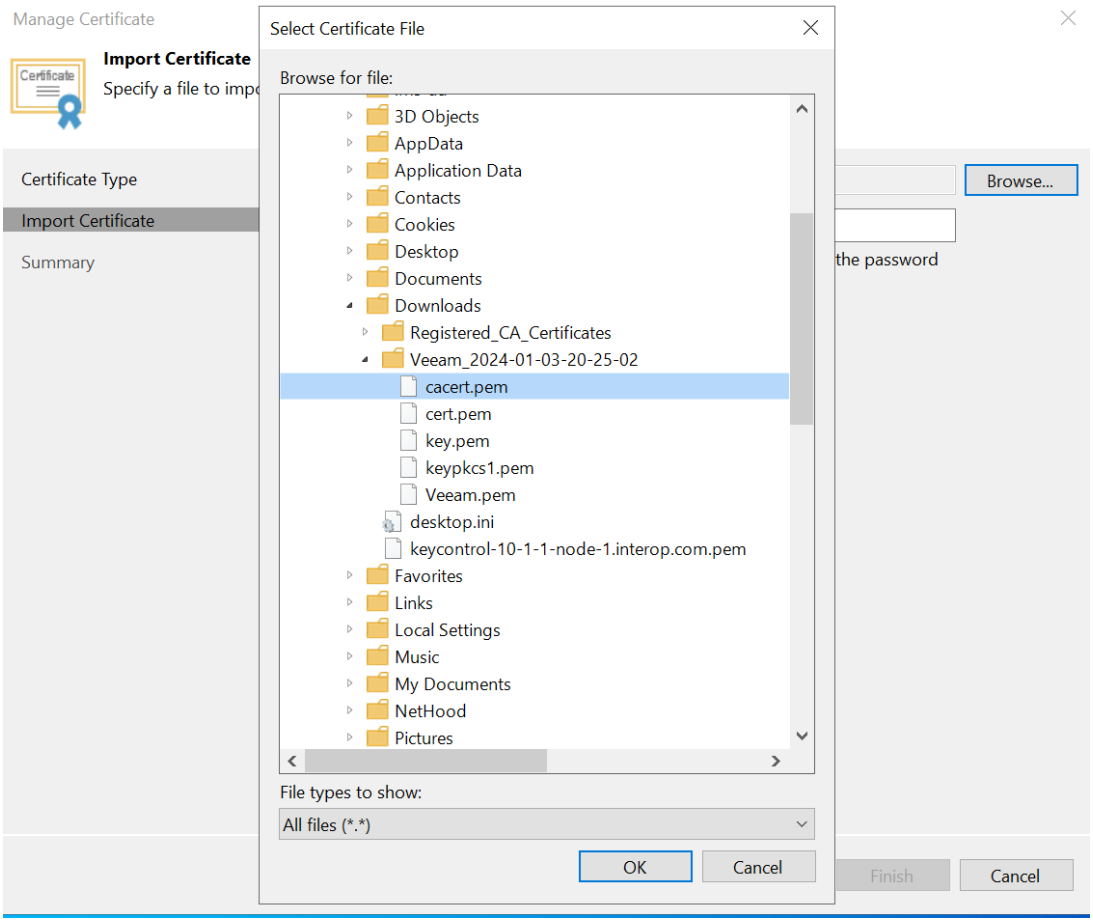
4. Enter the Server Name. Ensure that the default Port number is set to 5696.



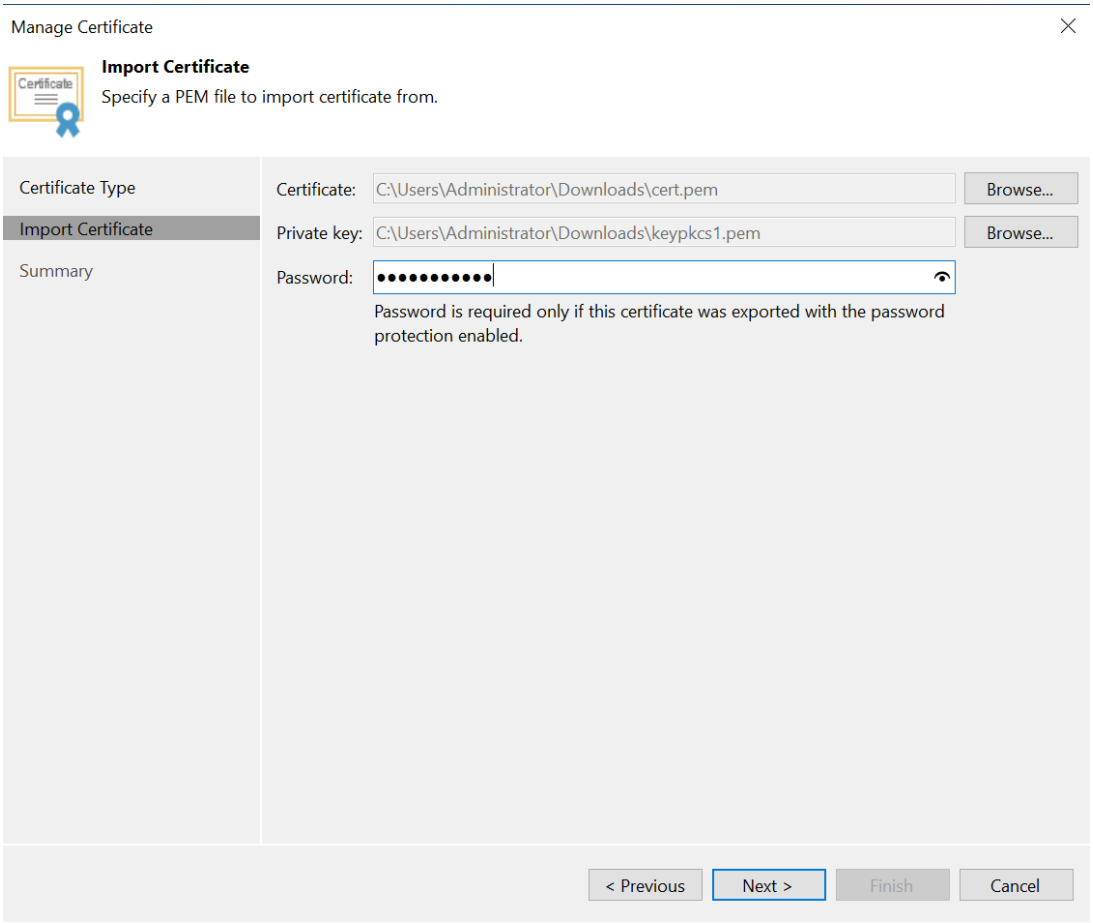
5. Browse and add the **Server certificate** `cacert.pem` created in Create the Entrust KeyControl client certificate bundle. Choose **Import certificate from a PEM file** in **Certificate Type**.



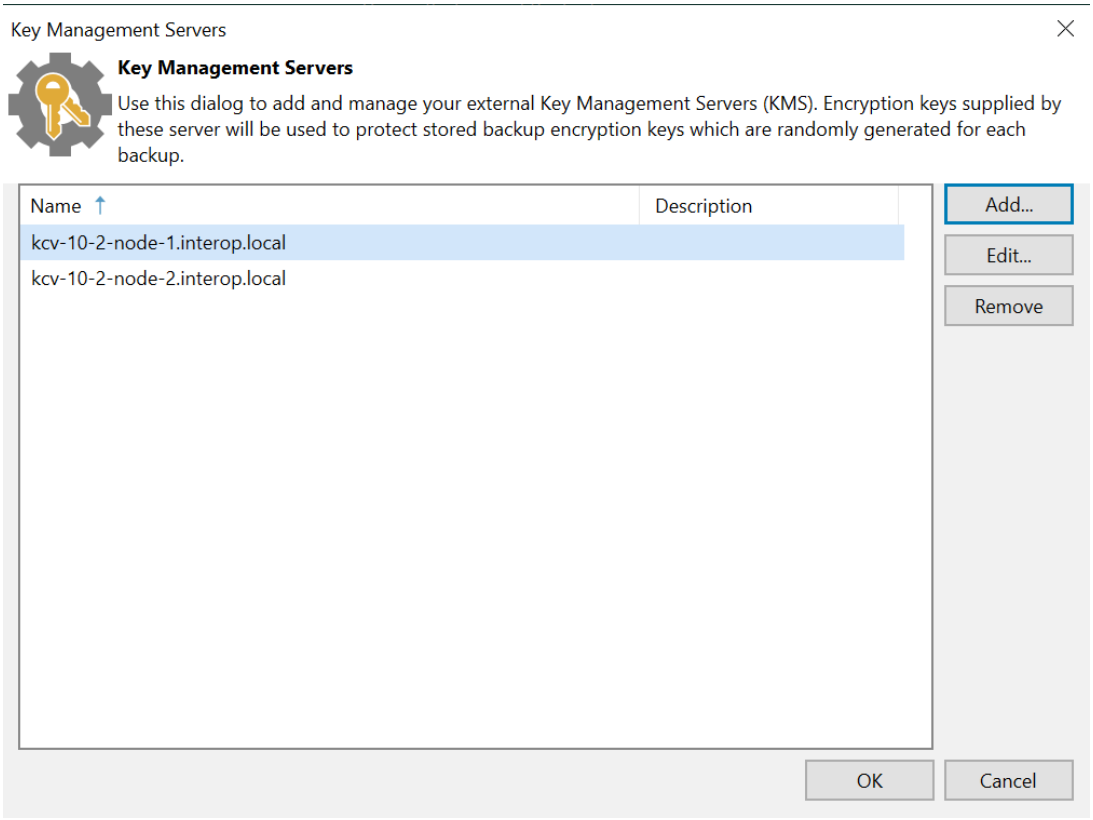
6. Select **Next** and **Finish**.



7. Browse to add the **Client certificates**. Choose **Import certificate from a PEM file** in **Certificate Type**.
8. Import the `cert.pem` and `keypkcs1.pem` created in Create the Entrust KeyControl client certificate bundle. Then select **Next** and **Finish**.



9. Select **OK** to verify the KMS server is validated.
10. Add the other nodes in the cluster following the steps above.


Key Management Servers
Key Management Servers
Use this dialog to add and manage your external Key Management Servers (KMS). Encryption keys supplied by these server will be used to protect stored backup encryption keys which are randomly generated for each backup.
Name
Description
kcv-10-2-node-1.interop.local
kcv-10-2-node-2.interop.local
Add...
Edit...
Remove
OK
Cancel

Chapter 5. Test Integration

The following steps summarize the integration testing of the Entrust KeyControl in cluster mode and Veeam Backup & Replication:

- Create a backup job
- Check Veeam Backup & Replication keys stored in Entrust KeyControl

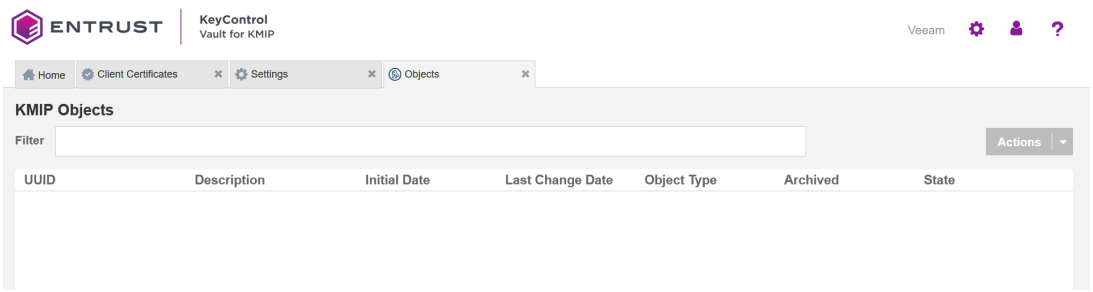
5.1. Create a backup job

5.2. Check Veeam Backup & Replication keys stored in Entrust KeyControl

Check Veeam Backup & Replication disk storage encryption keys created in Entrust KeyControl:

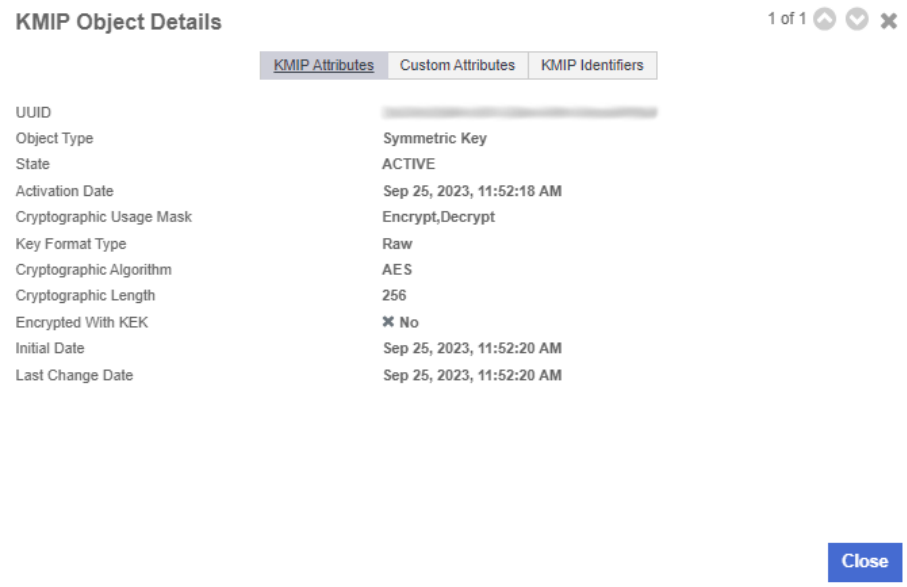
1. Login to the KMIP Vault with the URL and credentials from Create a KMIP Vault in the Entrust KeyControl.
2. Select the **Objects** tab to view a list of **KMIP Objects**. Notice the newly created keys.

   For example:



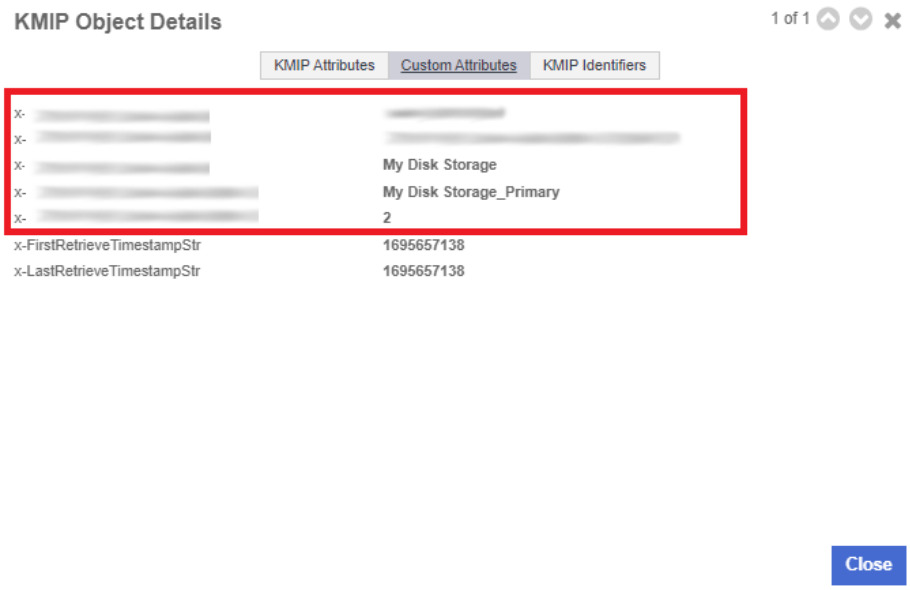
3. Select one of the keys to display its **KMIP Object Details**.

   For example:



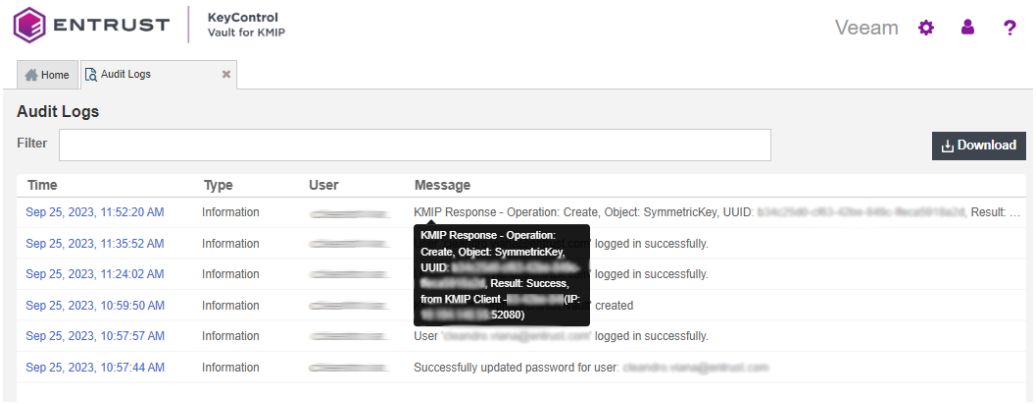
4. Select the **Custom Attributes** tab to verify it is the key used by Veeam Backup & Replication.

   For example:



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
Veeam
Home
Audit Logs
Audit Logs
Filter
Download
Time
Type
User
Message
Sep 25, 2023, 11:52:20 AM
Information
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.
KMIP Response - Operation: Create, Object: SymmetricKey, UUID:
Result: Success, from KMIP Client -
(IP:
52080)
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.

Chapter 6. Additional resources and related products