



Veeam Backup & Replication and Entrust KeyControl®

Integration Guide

© 2025 Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction
1.1. Documents to read first
1.2. Product configuration
1.3. Supported features
1.4. Requirements
2. Deploy and configure Entrust KeyControl
2.1. Deploy Entrust KeyControl cluster
2.2. Request root certificate for the Entrust KeyControl vault
2.3. Install root certificate in the Entrust KeyControl vault
2.4. Create a KMIP Vault in the Entrust KeyControl
2.5. View the KMIP Vault details
2.6. Edit the KMIP Vault
2.7. Add KMIP Vault Administrators
2.8. Create the Entrust KeyControl client certificate bundle
3. Install Veeam Backup & Replication
4. Integrate Entrust KeyControl with Veeam Backup & Replication
5. Test Integration
5.1. Create a backup job
5.2. Check Veeam Backup & Replication keys stored in Entrust KeyControl
6. Additional resources and related products
6.1. nShield Connect
6.2. nShield as a Service
6.3. KeyControl
6.4. Entrust products
6.5. nShield product documentation

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:

Generate Certificate Signing Request

×.	
``	/
1	<u> </u>
e	· ·

Common Name*	
kevcontrolvault	
Locality*	
Sunrise	
State *	
FL	
Subject Alternative Names*	
kcv-10-2-node-1.interop.local,kcv-10-2-node-2.interop.local,10.194.148.215,10.194.	148.21(
eg. kc-hytrust.local, 10.241.90.241,	
Key Size *	
4096	\sim
Country*	
US	
Organization*	
Entrust	
Organization Unit*	
nShield	
Cancel Download Su	bmit

- 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:

💼 Certific	ate			×
General	Details	Certification Path		
This c	Certifi certifica All applie	cate Informati te is intended f	on for the followin	g purpose(s):
	ssued t	o: keycontrolya	ult	
]	ssued b	y: interop-CON	TROLLER-CA-4	
	Valid fro	m 1/11/2024 t	o 1/11/2025	
				Issuer Statement
				ОК

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 MSAwHgYDVQQDExdpbnRlcm9wLUNPT1RST0xMRVItQ0EtNDAeFw0yNDAxMTEyMTEx MzZaFw0zNDAxMTEyMTIxMzZaMFIxFTATBgoJkiaJk/IsZAEZFgVsb2NhbDEXMBUG CgmSJomT8ixkARkWB2ludGVyb3AxIDAeBgNVBAMTF2ludGVyb3AtQ090VFJPTExF
CgmSJomT8ixkARkWB2ludGVyb3AxIDAeBgNVBAMTF2ludGVyb3AtQ090VFJPTExF Ui1DQS00MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2rthVuA/D9c3
pRcg1OKXayMBSTEurG0H6icp09re683suJoGDxBBV1Qp0+I6v2PwkkDD46lYlhCn ycr/+UenUS0As30NM9FbWejVdYBH2JHhHZDi2A9HyprWVFb+tLktX1VXbwTXP3QO +WPIEBtXRXTyP0ivkuMVRuyEd+qwTzvldjUGd0j5pRMb2cmI/sFRKN9CjDBNxDDX

z/wKB+Kaf9n6oh7RrWXIh5+v/N3gI4EG8z2fL010TmPzWdTafg9edvSnOviKVrmT qzGmxlT6DQt8xGRecDiJMH3+9R3XvRLhflcpANdqMAZnNipDCx4re4+DBH7S8mSh Vr1nK2xybQIDAQABo2kwZzATBgkrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8E BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUYzwTn023Ko23BcNb3u5i zpQLc5QwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQELBQADggEBACmiaN0t tBkyzkxpWy5xA+ePDyCBFLuQ6W1BByI6TCPOLp6CFsmYg9NB4c61+Y5lpIQhDJFf AODT1LZRTq6b5h8v11GdNzim2wPrtjviNvmQ0Q5R/2tJzR9D3SB6Hv+bU51RP7j/ giWpEx5ImmmfG7BJ4DxWxpA2sooC02iP2TOw5GJcI+varjKNCsyYSiyYhigOpnh/ 3ZlpMv2IGB/YykLfCPL2SOtYq0LcAnniiXmxx9iylqZwi3xQPx35JLn8b2Mrq0qI 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.

Certificate Types Default Custom	
SSL Certificate *	
Browse Preview	keycontrolvault.cer
CA Certificate *	
Browse Preview	rootcacert.pem.cer
Do you want to use this CA c Yes No	ertificate to verify KMIP client certificate?
Private Key	
Browse	
Password	
Apply Cancel	

- 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.

ENTRUST KeyControl Vault Management	secroot v Switch to: Applicance Management ?
Vaults Each vault has unique authentication and management	Settings
+	
Let's get started!	
+ 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
Туре	КМІР
Name	Vault name
Description	Vault description
Admin Name	Vault administrator username
Admin Email	Vault administrator email

Create Vault A vault will have unique authentication and management.
Туре
Choose the type of vault to create
кмір 🗸
Name *
Veeam
Description
Veeam Backup and Recovery integration with Entrust <u>KeyControl</u>
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*
Administrator@veeam.com
Create Vault Cancel

5. Select Create Vault. Then select Close.



The Administrator will be sent an email with a unique URL and temporary password to log in to their site. This URL will be in the Vault details for future reference.



G

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:

Administrator, you have been invited to become an administrator of the KMIP vault, CommVault.
To sign in, use the following:
URL:
User Name:
Password:
If you have any issues, <u>contact support</u> .
©2023 Entrust Corporation. All Rights Reserved

- 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.

ENTRUST	KeyControl Vault Managemer	nt
Vaults Each vault has unique authent	ication and managemen	t
Total Vaults: 2		
P	КМІР	КМІР
Test Vault Test		Veeam Veeam Backup and Recovery integrati on with Entrust KeyControl

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

For example:



KeyControl Vault for KMIP

Sign in to your account

I)

9. Notice the new vault.

For example:

ENTRUST KeyControl Vault for KMIP				Veeam 🏟 🛔 ?
	Objects	Security	LQ Audit Logs	

2.5. View the KMIP Vault details

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

Vault Details

 \times

Veeam

Veeam Backup and Recovery integration with Entrust KeyControl

Type KMIP

Created Oct 27, 2023 01:17:08 PM

Vault URL



API URL

🖪 Сору

Administrator Administrator Administrator@veeam.com

2. Select **Close** when done.

2.6. Edit the KMIP Vault

1. Select Edit when you hover over the Vault.

ENTRUST	KeyCostrol Vaul Management	≣ secrot v secrot to Applance Management ?
Vaults Each yault has unique authentica	for and managament	© Settings
Edit Vault		
Type KMIP		1 Unique URLs
Name*		Vault URL
Description		Ссору
Veeam Backup and Reco	wery integration with Entrust KeyControl	AFT URL
Administrator Administrator Administrator@veeam.com	Delete Vault	Rescue Valit In the event that the administrator of the walt gets loaded, the walk administrator of the walk gets load adhetionation and a temporary password can be sent to the rescue administrators defined within the walk Process

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.

Add User		×
Status		
User Name 🛛 *		
Administrator2		
Full Name *		
Caller Reprints		
Email *		
com		
Password 0 *		
••••••		I)
Password Expiration *		
Jun 11, 2023		
	Cancel	Add

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.

New User Suce	New User Successfully Added						
A new user has been successfully added.							
Before the user can login, you will need to add the user to either a new or existing access policy. This will determine whether the user is an Admin or User.							
Not Now	Add to Existing Policy	Create New 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.

Add	User to Access Policy			×
User				
Assign	this user to one of the following a	ccess policies.		
Filter				
	Name	Description	Role	
	Kmip Admin Policy	Default Kmip Admin Policy	Kmip Admin Role	
Showin	g 1 to 1 of 1 records (1 Selected)			

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.

Create Client Certificate		×
Add Authentication for Certificate		
User Name on Certificate *		
Veeam		
User Password on Certificate 🚯 *		
•••••		I)
Certificate Expiration *		
Oct 31, 2024		
Certificate Signing Request (CSR)		
Choose a file to upload		Browse
Encrypt Certificate Bundle		
	Cancel	Create

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

		eyControl ault for KMIP				Veeam 🔅	4	?
👫 Hor	me 👹 Client Certificates	×						
Mana	ge Client Certificate							
Filter						년 Downloa	d +	Ŭ
	Name	Valid	d From	Expiration	Generated From External CSR	Authentication		
	Veeam	Oct 31	1, 2023, 10:04:07	Oct 31, 2024, 10:04:07 AM	No	Enable		

- 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.

I I I I I I I I I I I I I I I I I I I	— D	× ~ ?				
\leftarrow \rightarrow \checkmark \uparrow I \rightarrow This PC \rightarrow Downloads \rightarrow Veeam_2023-10-31-14-09-11 \checkmark \checkmark \heartsuit Search Veeam_2023-10-31-14-09-11 \checkmark						
📌 Quick access	^	Name	Date modified	Туре	Size	
E Desktop	*	cacert.pem	10/31/2023 10:11 AM	PEM File	5 KB	
Downloads	*	Veeam.pem	10/31/2023 10:11 AM	PEM File	6 KB	
Documents	*					
E Pictures	*					

- 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.
- 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.



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.

。	(ey Managen	nent Servers					×	×
E▼ Home \		Key Management S	ervers					Q
Backup Replication		Jse this dialog to ad hese server will be u backup.	d and manage your external sed to protect stored backu	Key Management p encryption keys	t Servers (KMS). which are rand	Encryption ke omly generate	eys supplied by ed for each	Veeam AI
Primary Jobs	Name 🕇			Dee			Add	Online Assistant
Home		Add KMS Server			~		Edit	
Jobs		Server:	kcv-10-2-node-1.interop.ld	ocal			Remove	Result Next Run
Success		Port: Server certificate: Client certificate:	5696 Choose a certificate Choose a certificate		Browse Browse			
A Home ↓ Inventory Backup Infrastruct Storage Infrastruct				ОК	Cancel			
Cape Infrastructure								
L'III FIIES						ОК	Cancel	
								>
1 job selected			Connected to: localhost	Build: 12.1.0.2	131 Enter	prise Plus Edit	ion NFR: 286	days remaining

 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.

Manage Certificate		×
Certificate Type Choose certificate to	be used for encrypted SSL connection.	
Certificate Type Import Certificate Summary	 Select an existing certificate from the certificate store Pick an existing certificate already present in the local certificate store of this server. Import certificate from a file Import certificate from a file (PFX, CER, PEM or other). Import certificate from a PEM file Import certificate from split PEM files (certificate and private key are in separate files). 	
	< Previous Next > Finish	Cancel

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

Manage Certificate	Select Certificate File	\times
Certificate Specify a file to impo	Browse for file:	
×	 ▶ = 3D Objects ▶ = AppData 	
Certificate Type	Application Data Brows	e
Import Certificate		
Summary	Documents	
	A Downloads	
	Registered CA Certificates	
	Veeam 2024-01-03-20-25-02	
	cacert.pem	
	cert.pem	
	key.pem	
	keypkcs1.pem	
	Veeam.pem	
	🚺 desktop.ini	
	keycontrol-10-1-1-node-1.interop.com.pem	
	🖻 📄 Favorites	
	🛛 🖻 Links	
	Local Settings	
	🕒 🖻 Music	
	My Documents	
	NetHood	
	Pictures	
	< >>	
	File types to show:	
	All files (*.*)	
	OK Cancel Finish Cance	9

- 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**.

Manage Certificate			×
Certificate Specify a PEM file to	import certific	ate from.	
Certificate Type	Certificate:	C:\Users\Administrator\Downloads\cert.pem	Browse
Import Certificate	Private key:	C:\Users\Administrator\Downloads\keypkcs1.pem	Browse
Summary	Password:	••••••	
		Password is required only if this certificate was exported with the password protection enabled.	
		< Previous Next > Finish	Cancel

- 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 1	Description	Add
kcv-10-2-node-1.interop.local		Edit
kcv-10-2-node-2.interop.local		
		Remove
L		
	OK	Cancel

 \times

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.

ENTRUST	KeyControl Vault for KMIP					Veeam 🔅	≜ ?
Home 🔹 Client Certificates	× 🕸 Settings	× (S) Objects	×				
KMIP Objects							
Filter							Actions 🛛 👻
UUID	Description	Initial Date	Last Change Date	Object Type	Archived	State	

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

For example:

UUID Object Type State Activation Date Cryptographic Us		KMIP Attributes	Custom Attributes	KMIP Identifiers	
UUID Object Type State Activation Date Cryptographic Us			Symmetric Key		
Object Type State Activation Date Cryptographic Us			Symmetric Key		
State Activation Date Cryptographic Us					
Activation Date Cryptographic Us			ACTIVE		
Cryptographic Us			Sep 25, 2023, 11:52:18	3 AM	
	age Mask	1	Encrypt,Decrypt		
Key Format Type		1	Raw		
Cryptographic Alg	orithm		AES		
Cryptographic Le	ngth	:	256		
Encrypted With K	EK	:	× No		
Initial Date		:	Sep 25, 2023, 11:52:20) AM	
Last Change Dat			Sep 25, 2023, 11:52:20) AM	

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

Close

Close

For example:

KMIP Object Details				1 of 1 🔕 文 🗙
	KMIP Attributes	Custom Attributes	KMIP Identifiers	
x-				
X-				
X-	I	My Disk Storage		
х-		My Disk Storage_Prin	nary	
х-		2		
x-FirstRetrieveTimestampStr		1695657138		
x-LastRetrieveTimestampStr		1695657138		

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

ENTRUST	KeyControl Vault for KMIP		Veeam 🌣 🛔 ?
Home [Audit Logs	×		
Audit Logs			
Filter			<u>나</u> Download
Time	Туре	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		KMIP Response - Operation: Create, Object: SymmetricKey,
Sep 25, 2023, 11:24:02 AM	Information	-	UUID: logged in successfully.
Sep 25, 2023, 10:59:50 AM	Information	-	from KMIP Client - (IP: 52060) created
Sep 25, 2023, 10:57:57 AM	Information		User logged in successfully.
Sep 25, 2023, 10:57:44 AM	Information	<u> </u>	Successfully updated password for user.

Chapter 6. Additional resources and related products

- 6.1. nShield Connect
- 6.2. nShield as a Service
- 6.3. KeyControl
- 6.4. Entrust products
- 6.5. nShield product documentation