



TECHNICAL WHITE PAPER

Using Entrust KeyControl as an External KMIP in Rubrik Cluster

Benjamin Troch
September 2023
RWP-0595

Table of Contents

3	INTRODUCTION
3	Audience
3	INTRODUCTION TO ENTRUST KEYCONTROL KMS
4	KMIP AND CERTIFICATE REQUIREMENTS
4	Prerequisites
5	SETTING UP THE ENTRUST KEYCONTROL SOLUTION
5	Configuration of Entrust KeyControl
8	RUBRIK CONFIGURATION
8	Adding the Entrust KMIP server to the Rubrik Cluster
11	Key rotation
14	Removing the Entrust KMIP server from the Rubrik Cluster
18	CONCLUSION
18	SOURCES AND NOTES
18	VERSION HISTORY

INTRODUCTION

The purpose of this document is to help readers familiarize themselves with the methods to configure and integrate the Entrust KeyControl encryption Key Management Server (KMS) with Rubrik Cluster. Such information will prove valuable when evaluating, designing, or implementing the technologies described herein.

AUDIENCE

The intended audience of this document includes Rubrik and Entrust KeyControl Sales Engineers, Field and Technical Support Engineers, and customer architects and engineers who want to learn and understand how to implement the Entrust KeyControl KMIP application into their Rubrik Cluster data management solution.

INTRODUCTION TO ENTRUST KEYCONTROL KMS

Encrypting workloads helps reduce the risk of data breaches. However, managing the keys for multiple encrypted workloads is nontrivial. To ensure strong data security, encryption keys must be rotated frequently, transported and stored securely. Along with the high demand for strong data security, there is an ever-increasing business need to meet regulatory requirements for Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology (NIST) 800-53, and GDPR compliance in virtual environments.

With Entrust KeyControl, businesses can easily manage encryption keys at scale. Using Federal Information Processing Standards (FIPS) 140-2 compliant encryption, KeyControl simplifies management of encrypted workloads by automating and simplifying the lifecycle of encryption keys including key creation, storage, distribution, rotation, and key revocation. KeyControl provides a repository for keys and key management services to be done manually or via rule-based key rotation.

For environments where hardware-level protection is required, KeyControl integrates with the Entrust nShield general purpose HSM to provide a hardware root-of-trust. The integration with nShield ensures the keys are accessible only to trusted devices and administrators.

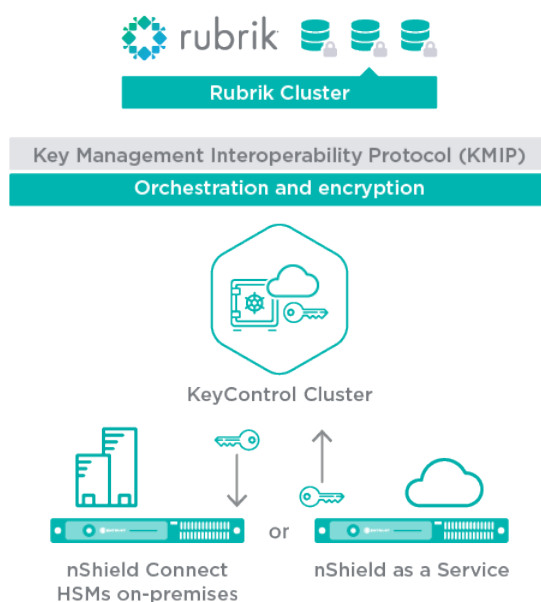


Figure 1 – Entrust Key Control High-Level Architecture

KMIP AND CERTIFICATE REQUIREMENTS

The Key Management Interoperability Protocol (KMIP) enables the communication between the Rubrik cluster and the Entrust KeyControl KMIP Server. KMIP uses Transport Layer Security (TLS) to provide a secure communication channel. Entrust KeyControl uses this channel to securely authenticate a KMIP client. X.509 certificates are used to facilitate authentication and authorization between Entrust KeyControl and the Rubrik Cluster. These certificates must be created on Entrust KeyControl and installed on Rubrik Cluster. Entrust KeyControl includes a server certificate signed by the internal Certificate Authority (CA). Alternatively, a client certificate for the Rubrik cluster can be created using tools such as OpenSSL. The certificate may be signed externally or can be self-signed.

Once configured, Rubrik Cluster will request a Key Encryption Key (KEK) from KeyControl for the Rubrik cluster. These KEKs securely wrap (encrypt/decrypt) the Data Encryption Keys (DEKs) created and stored locally in Rubrik Cluster. The DEKs are used to encrypt and decrypt the data in the cluster. Rubrik Cluster reaches out to KeyControl to retrieve the KEKs after a reboot. If KeyControl is unavailable, the data in the Rubrik cluster will remain locked and will be inaccessible.

PREREQUISITES

Table 1 indicates the versions of the products tested in this integration guide.

Rubrik Cluster	Entrust KeyControl
5.3.0 or later	5.4 or later

Table 1 – Rubrik and Entrust KeyControl version requirements

Rubrik Cluster version 5.3.0 or later is installed and operational

- The Rubrik Cluster must be configured to use encryption
 - Encryption can only be enabled at the cluster level during the bootstrap process.
- Entrust KeyControl version 5.4 or later is installed and operational
 - The Entrust KeyControl KMS is contactable by the Rubrik cluster on port 5696 or a custom KMIP port

The following key points should be understood on the Entrust KeyControl and Rubrik Cluster integration:

- Once encryption is enabled at the cluster level in Rubrik Cluster, it cannot then be disabled in the future.
- Rubrik Cluster supports multiple external KMS servers on the same cluster
- Once a TLS connection with the Entrust KeyControl has been established, Rubrik Cluster maintains that connection unless services are restarted or stopped. This results in a persistent TLS connection. When the connection to the KMIP server is not available at boot time the disks on the Rubrik cluster cannot be decrypted and the Rubrik cluster cannot be accessed.

IMPORTANT: Encryption is to be enabled at bootstrap as it can't be done later **without resetting and forfeiting** existing data.

SETTING UP THE ENTRUST KEYCONTROL SOLUTION

After downloading, deploying and configuring the Entrust KeyControl OVA, the Entrust KeyControl module will be reachable through an HTTPS web interface on the configured IP address.

IMPORTANT: The following information is provided as an example and is current as of version 5.4 of Entrust KeyControl and Rubrik Cluster 5.3. Always consult the Entrust and Rubrik product documentation for the latest procedure on setting up Entrust KeyControl with Rubrik Cluster.

CONFIGURATION OF ENTRUST KEYCONTROL

Following steps are required to get the Entrust KeyControl KMIP server up and running in a basic configuration:

1. Log in with the user and password combination configured during deployment of the OVA. The Entrust KeyControl main management page is displayed.
2. Navigate to the KMIP section of the Entrust KeyControl management interface as displayed in *Figure 2*.

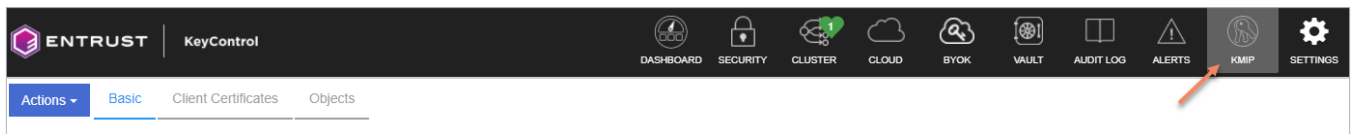


Figure 2 – Management pane of KeyControl web console

3. On the KMIP tab, the status of the KMIP server is displayed.
4. Select **Enabled** from the State drop-down menu
5. Select minimum **Version 1.2** from the Protocol drop-down menu.
6. Change the port number and the TLS protocol minimum version if required. *Figure 3* shows an example configuration.

Figure 3 – KMIP configuration tab

Begin by creating a client certificate. This client certificate is used by the Rubrik device to securely authenticate the Entrust KeyControl server. On the KMIP tab, click the **Client Certificates** tab as seen in *Figure 4*.

Figure 4 – Client certificate tab

On the **Client Certificates** tab, a new certificate must be created with parameters specific to the environmental and security policies with your organization.

To create a Client Certificate, click the **Actions** tab on the top right and select **Create Certificate**. *Figure 5* shows the options available on this tab.

×
Create a New Client Certificate

Certificate Name

Certificate Expiration

📅

Certificate Signing Request (CSR) Load File

CSR needs to be in base64 encoded PKCS#10.

Certificate Password

🔒

Confirm Password

👁️

Cancel
Create

Figure 5 – New Client Certificate Details

For the Rubrik use case, it is enough to fill out the certificate name and an expiration date for the certificate. The password fields must be left blank. After filling out the form, click the **Create** button at the right-hand side of the pane.

Note: If your organization does not allow the use of self-signed certificates or uses a certificate authority, use this dialogue to start the certificate signing request process.

Back in the **Client Certificates** pane the newly created certificate is shown. When it is selected, the details that were just entered are visible as shown in *Figure 6*.

RubrikEdge6	Wed Oct 06 2021 18:11:42 GMT+0200 (Central European Summer Time)	-
RubrikNewCert	Fri Oct 08 2021 16:52:42 GMT+0200 (Central European Summer Time)	:

Details

Certificate Name:	RubrikNewCert
Certificate Password:	Change
Certificate Expiration:	10/08/2022
Certificate Expires In:	365 Days
Certificate Generated From External CSR:	False

Figure 6 – Client Certificate details

Download the certificate to import it into the Rubrik appliance. Click the blue **Actions** button again and select **Download Certificate**. A zip file with the name of the certificate will be downloaded to your workstation. Save this in a secure, known location, as we will need this later in the process. The client certificate package contains two certificates:

- cacert.pem
- NameOfYourCertificate.pem

RUBRIK CONFIGURATION

The internal key manager in the Rubrik appliance uses a Trusted Platform Module (TPM) chip embedded on the Rubrik appliance to manage encryption keys, whereas the external key manager like Entrust KeyControl is a system that uses an independent server to manage the encryption keys.

ADDING THE ENTRUST KMIP SERVER TO THE RUBRIK CLUSTER

During the installation of the Rubrik cluster, enable encryption by answering “Yes” during the bootstrap process.

IMPORTANT: Enabling encryption must be done during bootstrap. Encryption cannot be enabled after the bootstrap process.

Make sure the Entrust certificates that were downloaded in the previous step are available.

The Rubrik user guide explains the process of configuring the KMIP server and key rotation. From the Rubrik GUI perform following steps:

First, import the client certificate that was created during the setup of the Entrust KeyControl KMIP server. Do this by going to Certificate Management in the Rubrik GUI

1. Click the **gear icon** on the right top side of the Rubrik GUI
2. Select **System Configuration**
3. Select **Certificate Management**
4. Copy the certificate from the cacert.pem and create a new certificate with it in the Certificate Management page on Rubrik as shown in *Figure 7*.

Add Certificate

Display Name
ENTRUST - TLS CERTIFICATE - CACERT

Description (Optional)
ENTRUST - TLS CERTIFICATE - CACERT

Certificate

```

-----BEGIN CERTIFICATE-----
MIID4jCCAsqgAwIBAgIEYVVMtjANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJV
UzEVMBMGA1UEChMMSHlUcnVzdCBJbmMuMTEwLWYyVQDEYhIeVRydXN0IEtLeUNv
bnRyb2w2Y2VydGlmYWVhdGUgQXV0aG9yaXR5MB4XDTEwMDYwMTAwMDAwMFoXDTE0
MTIzMTIzNTkxMDVowVzELMAkGA1UEBhMCVVMxFTATBgNVBAoTDEh5VHJlc3QgSW5j
LjExMC8GA1UEAxMoSHlUcnVzdCBJbmMuMTEwLWYyVQDEYhIeVRydXN0IEtLeUNv
cmI0eTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAONzPk9nqe1M5H9U
mNGIDLXQU3/TZzf9bb7gdf8bVu/2Zz86nGjEkRdBLPQMxUieXAWS7IBGFawYJMpU
pczsX28dFr9z1FK5w2c0SLD2SLcY4T6H0LopdKdeP125x7gIHDNq2crjRVKbLnly
CTFAjQT/vbyDGUjzfQ6ea9qH9j0WUoeXt41URcUJha9pEv241Ij8jJc6eQiSEKW6
A0ThF9aMhiJyIjvs+XGVnccjSs2E5uY75vQGTdsD3zA/EgvrkiYDECDdEq0QeFGN
04mRh/Ycues2p7ZILootUSNlq816t5/yt0soESkK6DmScDaSGuqZK6S77b68J7g
lIFHicCAwEAAaOBtTCBsjAdBgNVHQ4EFgQUdwiLEfQurrIonQztZd5e0Q646Xkw
gYIGA1UdIwR7MHMAFHciXh0LQ6yKJ0M7WxeXtE0u0L5oVukWTBXMqswCQYDVQQG
EwJVUzEVMBMGA1UEChMMSHlUcnVzdCBJbmMuMTEwLWYyVQDEYhIeVRydXN0IEtLe
UNvbnRyb2w2Y2VydGlmYWVhdGUgQXV0aG9yaXR5R5ggRhUya2MAwGA1UdEwQFMAMB
AfhwDQYJKoZIhvcNAQELBQADggEBAAMgjSEHe1qADTdeZu9UMjkGH1EV6l7sp4Q3
yu+B132gk1GnP0TuMJIB9dhpTJ3ZjcrzfwFGX00KPCH2g8KHN+EnMZtavgZ3q+N
iHNG/8L7aRXT9CJ8RKn5Q4KwuuHRBbceZLHwXgUAiFopKyUaEX8g6bDdHhIKQAVn
0N5h16LV2XnQ7sS9WrdGGCeZG6RyjpIbH+pskvi4NX1azeuFNyRmcbynP7EE04b
B0F3qyLl0m3Jlhki3Y65aDZGx2E/0JjgdY+feSvuZ0dK8IIdv+bs1mitgE+5rNM3
SgI+1rB0ufB8iXAn8F2SrmVKnQlUnJ0FP1GznVqVKnreb80Wg=
-----END CERTIFICATE-----

```

Please copy and paste the certificate here.

Key Type

CSR
 Key
 None

Cancel
Add

Figure 7 – Add Entrust certificate to Rubrik

1. Give the certificate a meaningful name and description
2. For the Key Type, select **None**
3. Click **Add** to add the certificate to the Rubrik cluster

Once the certificate is added, it is used to securely communicate with the Entrust KMIP server. This connection can now be established:

Navigate to the **Manage Encryption** page in the Rubrik GUI:

1. **Gear right top side**
2. **System Configuration**
3. **Manage Encryption**
4. Here there are two tabs – **Key Rotation Status** and **KMIP Settings**.
5. Go to **KMIP Settings** to add the Entrust KMIP server IP
6. Press **Add KMIP Server**, as shown in *Figure 8* below

The screenshot shows a dialog box titled "Add KMIP Server". It contains two input fields: "Server Address" with the value "172.22.9.65" and "Port" with the value "5696". Below these fields is a text instruction: "Select a TLS Certificate. If you have not imported your TLS Certificate, import it from the [Certificate Management page](#)." Underneath, a list of certificates is shown, with "ENTRUST - TLS CERTIFICATE - CACERT" selected and marked with an 'X'. Below the list is a prompt: "Select certificate from list or type certificate name". At the bottom of the dialog, there are two buttons: "Cancel" on the left and "Add" on the right.

Figure 8 – Adding a KMIP server to Rubrik

After adding the KMIP server to the Rubrik cluster, the client settings can be configured with a set of options for client authentication:

- Password only
- Client certificate only
- Both

Type the username and password required by the key manager. If a username and password are not required, leave these blank.

If option 2 or 3 are selected, specify the TLS certificate that was defined in the previous step when the KMIP server was added to the Rubrik cluster.


For this setup, configure the Rubrik cluster to automatically log into the KMIP server with the client certificate that was downloaded from Entrust KeyControl.

Configure Client Settings


Client Authentication Mode

Password Only
 Client Certificate Only
 Both

Username

admin 

Select a TLS Certificate. If you have not imported your TLS Certificate, import it from the [Certificate Management page](#).

Entrust KMIP - RubrikEdge6.pem 

.....

Select certificate from list or type certificate name

Cancel Update

Figure 9 – Configure Rubrik client settings

KEY ROTATION

After the KMIP server is successfully added to the Rubik cluster, it can now safely rotate keys with Entrust KeyControl. To do this complete following steps:

1. In the GUI go to the **gear icon** and select **Manage Encryption**
2. Go to the **Key Rotation Status** tab
3. Click **Rotate Keys** on the top right side of the screen.


Key Rotation Status		KMIP Settings		Rotate Keys
Node ID	Key Manager	Start Time	Status	
VRVW423EBFF24	External (KMIP)	10/08 3:09 pm	Succeeded	

Figure 10 – Rotate encryption keys on Rubrik

4. Click Continue on the **One-Time Key Rotation** screen.

One-Time Key Rotation

Please choose a key manager to perform the one-time rotation.

Internal Key Manager (Rubrik TPM)

 External Key Manager (KMIP-compliant)

Cancel
Continue

Figure 11 – One-Time key rotation

5. Select **External Key Manager (KMIP-compliant)** to use the configured Entrust KeyControl server.
6. Go to the Rubrik Cluster activity log to monitor the change to the external Entrust KMIP server after the initial key rotation as seen in *Figure 12*.

Activity Log
[See All](#)

✓

Successfully rotated data encryption keys protected by KMIP key rubrik_74faa40e-239b-478b-8055-39826e244ef5_1634913552607 on KMIP cluster List(172.22.9.65).
Just Now

✓

admin started a job to rotate data encryption keys protected by KMIP.
10/22 2:39 pm

✓

Successfully configured KMIP on all nodes.
10/22 2:38 pm

Figure 12 – Switch to external KMIP server successful

Date	User	Message
10/11/2021, 5:43:44 PM	System	KMIP Response: Create SymmetricKey 497d4f3b-32cf-4042-b236-4ac43d0f0c66 Success
10/11/2021, 5:43:44 PM	System	KMIP Request: Create SymmetricKey
10/11/2021, 3:57:23 PM	Security Administrator	User secroot logged in from ipaddr 172.29.4.3

Figure 13 – Key rotation logs

On the Entrust console, the initial key rotation can also be monitored for success. An example is shown in *Figure 13*: A KMIP request from Rubrik to Entrust KeyControl to Create Symmetric Key and a response is shown with a valid key.

Alternatively, on Rubrik the REST API can also be used to query for token rotation logs and to initiate a token rotation. The Rubrik REST API endpoint used for this is the following:

GET /internal/cluster/me/security/key_rotation

When looking at the output of the rotation log query, the successful log rotations can be seen:

```
{
  "rotationId":
  "SOFTWARE_KEY_ROTATION_24bc86ea-94c7-417a-bb2a-6d472c35f57b_2b4d837e-bcc8-45ad-b817-8e0248c250f3",
  "nodeId": "VRVW423EBFF24",
  "status": "success",
  "keyProtection": "kmip",
  "keyRecovery": true,
  "startTime": "2021-10-07T09:49:39.362Z",
  "endTime": "2021-10-07T09:51:38.394Z"
},
```

When posting to the REST API, a KMIP key rotation can be initiated. This rotation will return the following REST body message after a successful rotation. The Rubrik REST API endpoint we use for this action is the following:

POST /internal/cluster/me/security/key_rotation

The payload of the API POST must contain the following JSON:

```
{
  "keyProtection": "kmip",
  "keyRecovery": true
}
```

Example REST response body

```
Download
{
  "id":
  "SOFTWARE_KEY_ROTATION_29f4ef61-354c-4c49-b49e-1282528e4027_99f0f298-27f9-42df-aeed-
  f5cee78367c5::0",
  "status": "QUEUED",
  "progress": 0,
  "startTime": "2021-10-19T11:58:18.067Z",
  "links": [
    {
      "href":
      "https://10.1.1.1/api/internal//cluster/me/security/request?request_id=SOFTWARE_
      KEY_ROTATION_29f4ef61-354c-4c49-b49e-1282528e4027_99f0f298-27f9-42df-aeed-
      f5cee78367c5::0",
      "rel": "self"
    }
  ]
}
```

IMPORTANT: Rubrik REST API endpoints may change as Rubrik software evolves, always check the latest Rubrik REST API documentation for your release.

This way, KMIP key rotations between Entrust and Rubrik can be automated using common configuration management tools or scripting languages to keep the data on the Rubrik cluster securely encrypted at any given time and in line with internal security requirements and policies.

REMOVING THE ENTRUST KMIP SERVER FROM THE RUBRIK CLUSTER

When removing the KMIP server from a platform that has an internal hardware Key Manager or Trusted Platform Module (TPM) there are a certain number of steps to be followed. When bootstrapping the Rubrik cluster and the option to encrypt the data is selected Rubrik Cluster will automatically use the internal TPM after bootstrap. The procedure to enable an external KMIP server is the same as described in this document. If the external KMIP server needs to be removed and we want to fall back to the internal TPM key rotation following steps need to be completed.

1. In the GUI go to the clog wheel and select **Manage Encryption**
2. Go to the **Key Rotation Status** tab
3. Click **Rotate Keys** on the top right side of the screen This will trigger a final key rotation on the external KMIP server.
4. Select **External Key Manager** as seen in *Figure 14*.

One-Time Key Rotation

Please choose a key manager to perform the one-time rotation.

Internal Key Manager (Rubrik TPM)
 External Key Manager (KMIP-compliant)

Cancel
Continue

Figure 14 – One-Time key rotation

5. Wait until the key rotation is completed for all nodes as seen in *Figure 15*.

Node ID	Key Manager	Start Time	Status
RKLAB-RVM195S006903	External (KMIP)	11/08 12:14 pm	Succeeded
RKLAB-RVM195S007037	External (KMIP)	11/08 12:14 pm	Succeeded
RKLAB-RVM195S007071	External (KMIP)	11/08 12:14 pm	Succeeded
RKLAB-RVM195S007115	External (KMIP)	11/08 12:14 pm	Succeeded

Figure 15 – Key rotation successful

6. Perform another key rotation and select Internal Key Manager (Rubrik TPM) as seen in *Figure 16*.

One-Time Key Rotation

Please choose a key manager to perform the one-time rotation.

Internal Key Manager (Rubrik TPM)
 External Key Manager (KMIP-compliant)

Cancel
Continue

Figure 16 – Select internal TPM

7. On the Key Rotation Status page, we can now see that the Key Manager is set back to **Internal (TPM)** as seen in *Figure 17*.

Key Rotation Status		KMIP Settings	
Node ID			Key Manager
RKLAB-RVM195S006903			Internal (TPM)
RKLAB-RVM195S007037			Internal (TPM)
RKLAB-RVM195S007071			Internal (TPM)
RKLAB-RVM195S007115			Internal (TPM)

Figure 17 – Monitor Key Manager status

- Once the Rubrik Cluster is successfully returned to rotate encryption keys on the internal hardware TPM module the external KMIP server can be removed by going to KMIP settings and removing the server by clicking the 3 dots next to the server and selecting **Remove External KMIP server**.

When removing the KMIP server from a platform that has no internal hardware Key Manager or Trusted Platform Module (TPM) follow the following steps to roll back to a static encryption password. The KMIP server can be removed by first initiating a key rotation and reverting to static encryption password as seen in *Figure 18*.

One-Time Key Rotation

Please choose a key manager to perform the one-time rotation.

External Key Manager (KMIP-compliant)
 Password

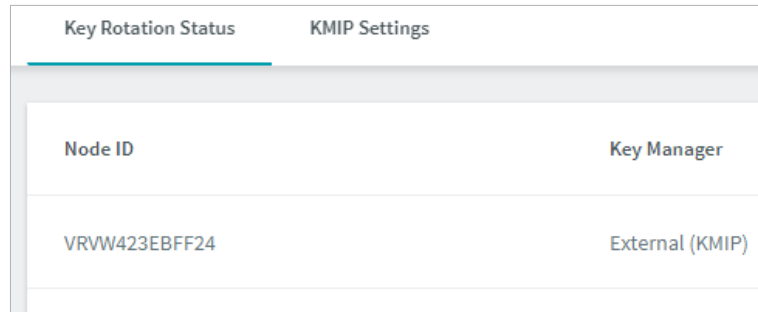
New Encryption Password

Confirm New Encryption Password

Cancel
Continue

Figure 18 - Key rotation on servers without TPM module

1. **Change the encryption method to Password** and enter a new encryption password
2. Click **Continue**
3. After the key rotation is finished, the GUI will show **Password** instead of **External (KMIP)** as soon in *Figure 19*.



Node ID	Key Manager
VRVW423EBFF24	External (KMIP)

Figure 19 – Key rotation logs

IMPORTANT: When changing a Rubrik device back to using an encryption password the disks need to be manually decrypted after a reboot. In order to do this, log in to the admin CLI through either the console or SSH and run the following command:

```
VRVW423EBFF24 >> cluster provide_encryption_password
```

After this is done, it takes about 5 to 10 minutes for the cluster to use the provided encryption password to decrypt the data disks and start the Rubrik web GUI. This can be monitored running the following command:

```
VRVW423EBFF24 >> cluster service_status
```

IMPORTANT: Rubrik CLI commands change over time as cluster upgrades happen, so always check the latest user guide to verify the correct command.

CONCLUSION

Using the joint solution from Entrust and Rubrik superior data encryption is enabled with Rubrik clusters. With this solution, all your data is safely and immutably stored with on-demand or fully automated key rotation over a secure connection. This is how Rubrik and Entrust work together to protect and encrypt your data in the most secure possible manner.

SOURCES AND NOTES

Rubrik REST API documentation on managing KMIP servers

<https://rubrikinc.github.io/api-doc-v1-6.0/#section/Passwords/Managing-KMIP-Servers>

Rubrik REST API documentation on certificate lifecycle management

<https://rubrikinc.github.io/api-doc-v1-6.0/#section/Role-Management/Role-Lifecycle-Management>

Rubrik Support containing latest release notes and user guides

<https://support.rubrik.com>

VERSION HISTORY

Version	Date	Summary of Changes
1.0	November 2021	Initial Release
1.1	September 2023	Product name updates



Global HQ

3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik is a cybersecurity company, and our mission is to secure the world's data. We pioneered Zero Trust Data Security™ to help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, delivers data protection and cyber resilience in a single platform across enterprise, cloud, and SaaS applications. Our platform automates policy management of data and enforcement of data security through the entire data lifecycle. We help organizations uphold data integrity, deliver data availability, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked. Rubrik is a registered trademark of Rubrik, Inc. All company names, product names, and other such names in this document are registered trademarks or trademarks of the relevant company.