Nutanix

AHV

20230302.102001

Integration Guide

ESKM

v8.54.0

utimaco®

Imprint

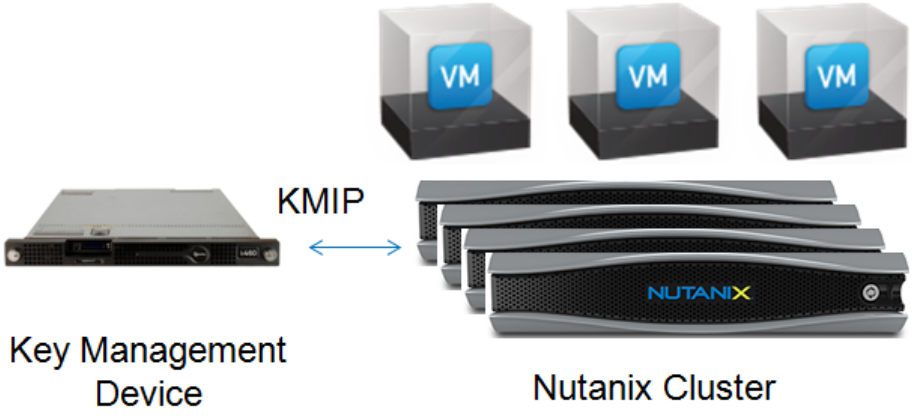
Copyright 2025	Utimaco IS GmbH
	Germanusstr. 4
	D-52080 Aachen
	Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226)
	EMEA +49 800-627-3081
	APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	07/04/2025
Status	PUBLISHED
Document No.	IG-2025-0034

Table of Contents

1 Introduction

This integration guide outlines the process between Nutanix AHV and Enterprise Secure Key Manager (ESKM) to enable secure and centralized key management for data-at-rest encryption. It uses the KMIP (Key Management Interoperability Protocol) to establish secure communication between Nutanix and ESKM. Nutanix AHV and ESKM together deliver a comprehensive solution for secure, compliant and resilient data protection.

This guide walks through the configuration process for integrating Nutanix AHV and ESKM.



For more information on Nutanix Documentation, see https://portal.nutanix.com/page/documents/details?targetId=Nutanix-Security-Guide-v6_10:wc-security-data-encryption-aos-wc-c.html

1.1 About This Guide

This guide provides information on how to configure the Nutanix to work with the Utimaco Enterprise Secure Key Manager (ESKM). It describes only the features in the Nutanix and the ESKM necessary for the configuration and integration.

For more information on installing an Utimaco Enterprise Secure Key Manager, refer to the Utimaco *ESKM Installation and Replacement Guide (Chapter 1 Installing Hardware)*.

1.2 Target Audience

This guide is intended for Nutanix AHV and Utimaco ESKM administrators.

1.3 Purpose of the Integration

This integration allows Nutanix AHV to use Utimaco ESKM to manage encryption keys securely. Nutanix AHV handles virtualization, while Utimaco ESKM stores and controls the keys used to encrypt data stored on the Nutanix cluster.

The main objectives of this integration are:

- To enable secure encryption of data.
- To manage encryption keys externally through Utimaco ESKM.
- To support compliance with data protection and security standards.
- To maintain high availability and performance of the Nutanix environment.
- To simplify encryption operations such as key rotation and rekeying.

1.4 Abbreviations

Abbreviation	Meaning
ESKM	Enterprise Secure Key Manager
KMIP	Key Management Interoperability Protocol
Nutanix AHV	Nutanix Acropolis Hypervisor
API	Application Programming Interface
AOS	Acropolis Operating System
KMS	Key Management Server
VM	Virtual Machine
CA	Certificate Authority

Abbreviation	Meaning
KEKs	Key Encryption Keys
CVM	Controller Virtual Machine

Table 1: Abbreviations

1.5 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press the **OK** button.
`Monospaced`	File names, folder and directory names, commands, file outputs, programming code samples	You will find the file example.conf in the `/exmp/demo/` directory.
Italic	References and important terms	See Chapter 3, "Sample Chapter", in the *CryptoServer - csadm Manual* or [CSADMIN].

Table 2: Document conventions

Special icons are used to highlight the most important notes and information.

Here you will find important safety information that should be followed.

This message marks the result expected after the successful execution of an instruction.

Here you find additional notes or supplementary information.

2 Document Metadata

Element	Data
Partner Name	Nutanix
Product Name	AHV
Partner Product [Version]	20230302.102001
Integration Guide [Version]	V1.0
Utimaco Product Name	ESKM
Utimaco Product [Version]	8.54.0
[Date/Year]	26/06/2025

Table 3: Document Metadata

3 Product Overview

3.1 Nutanix AHV

Nutanix AHV is a built-in solution for running and managing virtual machines on Nutanix systems. It is designed to help organizations run and manage virtual machines easily without other hypervisors like VMware or Hyper-V.

AHV works closely with Nutanix Prism to simplify VM management, reduce costs, and improve performance. To protect sensitive data, AHV supports data-at-rest encryption, which can be integrated with ESKM using the KMIP protocol.

3.2 Utimaco ESKM (Enterprise Secure Key Manager)

The Utimaco ESKM is a complete solution for generating, storing, serving, controlling, and auditing access to data encryption keys. It enables you to protect and preserve access to business-critical, sensitive data-at-rest encryption keys, either locally or remotely. ESKM is offering industry-certified Key Management Interoperability Protocol (KMIP)with market-leading support for partner applications and pre-qualified solutions, integrating out-of-the-box with varied deployments, as well as custom integrations.

3.3 Joint Value Proposition

The integration of Nutanix AHV with Utimaco ESKM delivers a powerful, secure, and easy-to-manage virtualization and encryption solution. Nutanix provides a modern, scalable, and user-friendly hypervisor platform, while Utimaco ESKM ensures strong key management for data-at-rest encryption. This solution helps:

- Run virtual workloads on a simple and scalable hypervisor (Nutanix AHV).
- Protect sensitive data using strong encryption.
- Securely store and manage encryption keys outside the cluster (Utimaco ESKM).
- Maintain high performance with minimal effort.

4 Integration Requirements and Prerequisites

Ensure that the system environment you will be using meets the following hardware and software requirements.

This guide assumes that the user has already installed and configured the required software.

4.1 Tested Versions

Operating System	Nutanix AHV	Utimaco ESKM Version
AOS 6.10	20230302.102001	8.54.0

Table 4: Tested Versions

4.2 Software Requirements

Software	Software Requirements
Utimaco ESKM	8.54.0
AOS version	6.10 or above
AHV version	20220302.102001

Table 5: Software Requirements

4.3 Prerequisites

- Ensure that the latest version of ESKM is installed and available.
- AHV cluster must be able to communicate with ESKM server over the required port (5696).
- Administrator access to Nutanix Prism.
- Administrator access to ESKM server for configuration.

5 Installation and Configuration

5.1 Setting Up ESKM

Configuring the ESKM is the initial step before proceeding with Nutanix Integration. For detailed configuration steps, refer to the "*ESKM_Installation and Replacement_Guide_8.54.0*".

After successful installation and configuration, log in to the ESKM.

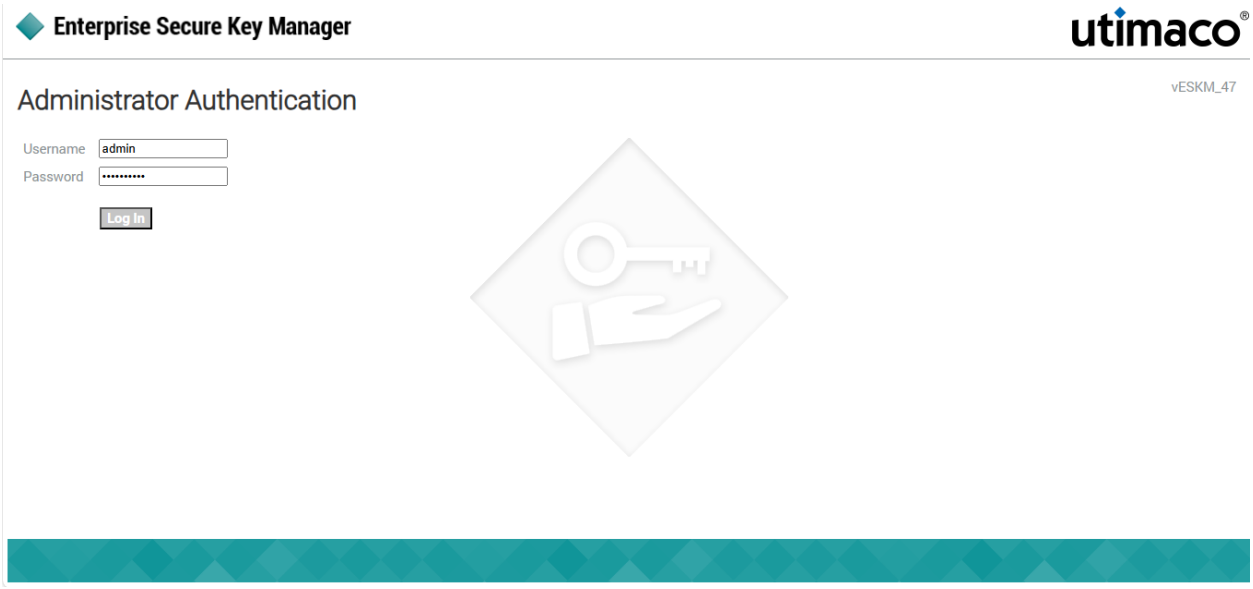


Figure 1 : ESKM Login

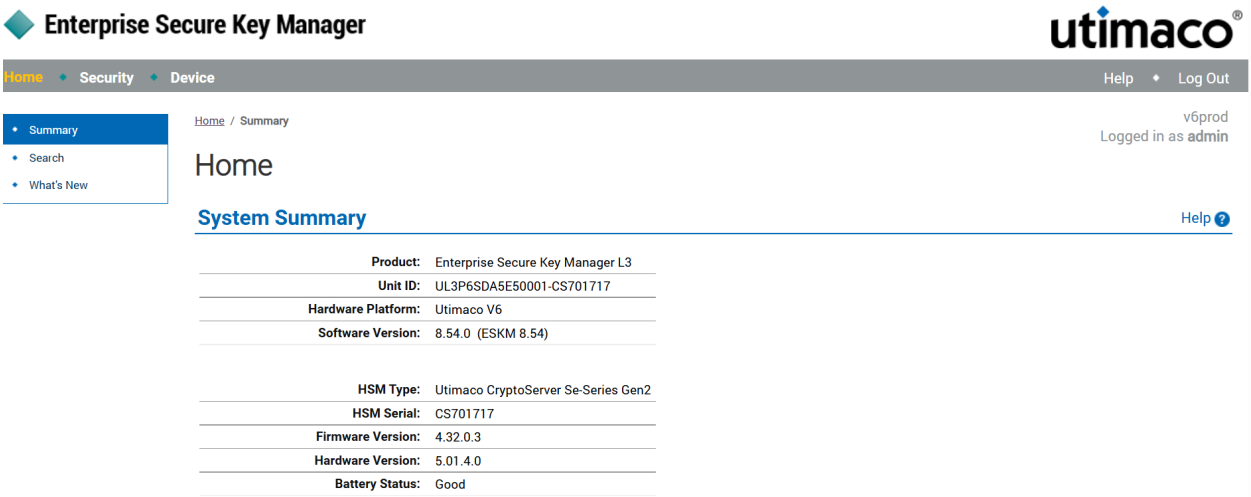


Figure 2 : ESKM Home Page

5.2 Setting Up Nutanix AHV

For assistance with setting up Nutanix AHV, contact the Nutanix support team. For more information, refer to the Nutanix Support & Insights.

6 Integration Steps

6.1 Configuring on Utimaco ESKM

ESKM server must be configured with specific values such as time zone, IP address, netmask, gateway, host name, and port number used for the ESKM Management Console interface.

This section includes procedures on the following topics:

- First run
- Setting Up Cluster
- Setting Up Local CA
- Setting Up ESKM Certificate
- Setting Up KMIP Server
- Create Client Certificate
- Create Local User

6.1.1 First run

To configure the time, IP address, net-mask, gateway, host name, and port number used for the ESKM Management Console interface, please refer to the *ESKM_Installation and Replacement_Guide_8.54.0*.

6.1.2 Setting Up a Cluster

Refer to the ESKM*_Installation and Replacement_Guide_8.54.0* for the procedures to create a cluster on one ESKM node and join other ESKM Nodes to the cluster.

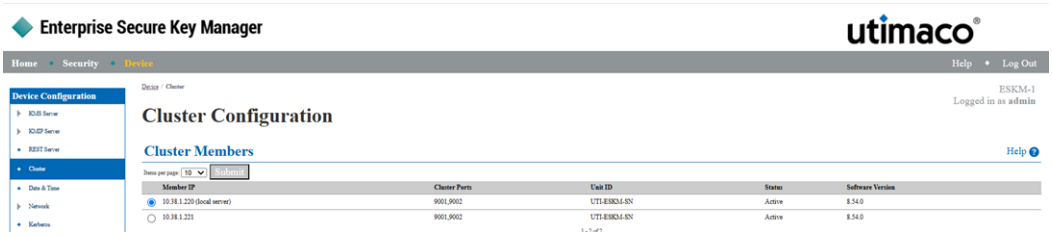


Figure 3 : KMS Server - Clustered mode

6.1.3 Setting up Local CA

The local CA is used to sign and verify the server certificate and may also be used to sign client certificate requests. To create and install a local CA, perform the following steps:

1. Log in to the **ESKM Management Console** using the admin username and the password you supplied in **First run**. For more information, refer to the ESKM_*Installation and Replacement_Guide_8.54.0*.
2. Select the **Security tab**.
3. In **Certificates & CAs**, click **Local CAs**.

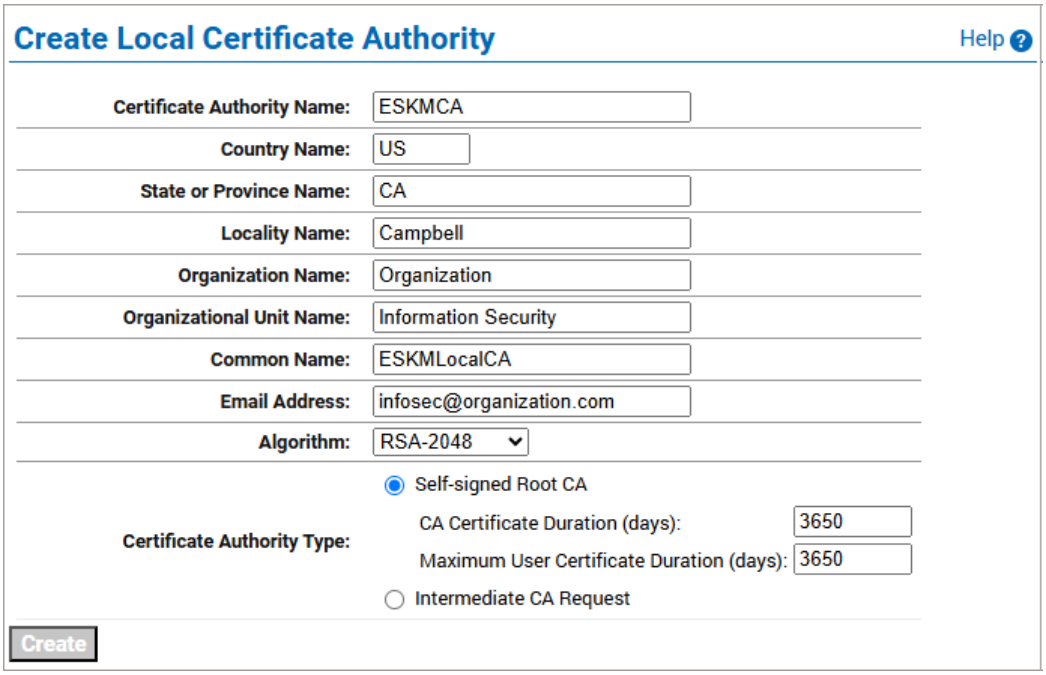


Figure 4 : Create Local CA

4. Enter a **Certificate Authority Name** and **Common Name**. These may have the same value, for example, **ESKM Local CA**.
5. Enter your organizational information.
6. Select the **Algorithm** (e.g., RSA-2048).
7. Click **Self-signed Root CA** and enter the **CA Certification Duration** and **Maximum User Certificate Duration**. These values determine when the certificate must be renewed and

should be set in accordance with your company's security policies. The default value for both is 3650 days or 10 years.

8. Click **Create**.

6.1.4 Setting Up an ESKM Certificate

The client uses ESKM server certificates to authenticate the ESKM server during the TLS/SSL handshake. ESKM supports two types of clients: ESKM clients and KMIP-enabled clients. ESKM clients communicate with the KMS server, and KMIP-enabled clients communicate with the KMIP server.

During the execution of the Setup utility, a default KMIP Server Certificate is automatically created. This certificate should only be used for testing purposes, as it is a self-signed certificate. If your ESKM system will be communicating with KMIP-enabled clients, Utimaco highly recommends that you create a new KMIP server certificate. The name you assign to these server certificates should clearly indicate their purpose. For example: ESKM KMS Server and ESKM KMIP Server.

If you will be using a third-party CA and wish to use an existing server certificate, see **Import a third-party server certificate**.

To create an ESKM server certificate, perform the following steps:

1. Click the **Security tab**.
2. In **Certificates and CAs**, select **Certificates**.
3. Enter the information required by the Create Certificate Request section of the window to create the ESKM server certificate.

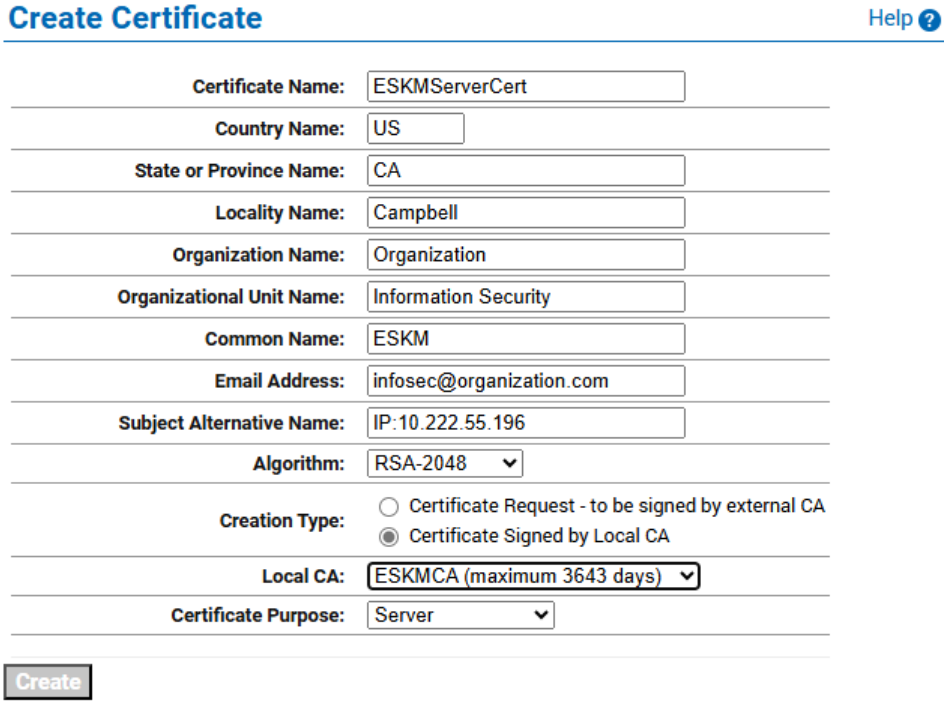


Figure 5 : Create Certificate

4. Enter a **Certificate Name** and **Common Name**, for example, ESKM_KMIP_Server.
5. Enter your Organizational information.
6. Enter/select the **Subject Alternative Name**, **Algorithm, Creation Type** as **Certificate Signed by Local CA, Local CA**(CA name you created in Setting up local CA, for example **ESKMCA**), and **Certificate Purpose**
7. Click **Create**.

Certificate Information

Help

Certificate Name:	ESKMServerCert
Key Size:	2048
Start Date:	Nov 13 08:37:33 2022 GMT
Expiration:	Nov 10 08:37:33 2032 GMT
Issuer:	C: US ST: CA L: Campbell O: Organization OU: Information Security CN: ESKMLocalCA emailAddress: infosec@organization.com
Subject:	C: US ST: CA L: Campbell O: Organization OU: Information Security CN: ESKM emailAddress: infosec@organization.com
Subject Alternative Name:	IP Address: 10.222.55.196
Purpose:	SSL Server


```
-----BEGIN CERTIFICATE-----
MIID6zCCAtOgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBojELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhDYW1wYmVsbDEVMBMGA1UEChMMT3JnYW5p
emF0aW9uMR0wGwYDVQQLExRJbmZvcm1hdGlvbiBTZWN1cml0eTEUMBIGA1UEAxML
RVNLTUxvY2FsQ0ExJzAlBgkqhkiG9w0BCQEWGGluZm9zZWNAb3JnYW5pemF0aW9u
LmNvbTAeFw0yMjExMTMwODM3MzNaFw0zMjExMTAwODM3MzNaMIGbMQswCQYDVQQG
EwJVUzELMAkGA1UECBMCQ0ExETAPBgNVBAcTCENhbXBiZWxsMRUwEwYDVQQKEwxP
cmdhbml6YXRpb24xHTAbBgNVBAsTFEluZm9ybWF0aW9uIFN1Y3VyaXR5MQ0wCwYD
VQQDEwRFU0tNMScwJQYJKoZIhvcNAQkBFhhpbmZvc2VjQG9yZ2FuaXphdGlvbi5j
b20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDZeJpAadCp0oUuwVC3
+6ICftWmFfEXk3FuKpwD1RRiVhKcbhGokbYwwp/zmdb+3KoltSho9H/uBxEz+MA8
XI5rg9sg4VDrMMwtj7SEq4eOYhFop4orEyKxUfOnB8DFFM/hoy+PBWfVw74OzYJA
/sBY8jv9Bx2M4eaIaWbgncy9F2KsMMID/y/TcCNjikSeheOTn7SdWRVoy/UORwWI
Q5nS1HXQGOonL6IGjeAd51PG19CdNeFCX2fW8bBL1mWuTZUEzAHVJA8oN1A1YoOQ
U2FFzBQmMPQinAQBXaXFhPDarQOTGe4isEUtpfkaPnoaPzLdt1Oox9aKBgMeQMKv
MKP5AgMBAAGjMTAvMAkGA1UdEwQCMAAwEQYJYIZIAYb4QgEBBAQDAgZAMA8GA1Ud
EQQIMAaHBAreN8QwDQYJKoZIhvcNAQELBQADggEBAJF02UfWn+lmlomHswi8DnG3
NkNj16OLco1POPiZrpP/s7U03tBi96GhVmb7UvwdyblAF0GEq50od8d6zGRJwC9g
rV/1A3nvQeaVV3wyYJWHWeKxtxP0CkSFn4cqYOZfAPrJ+a+01+jrhaSG0YPc4guV
21M4xbkA35UNB+vPTWwQkPMkWlu5Pn8BL2Ett87LuOtjUfanYb59CwZoQ5gxo2PO
9QU6ekRR6XvRVt/9GcaTYTulDS3x95RS3uivdbmTO77xPAIF+7ENxringMPo1pg5
lHubYnQ9aBL1qjb0r1H4bwrLja6h5647+NBEEAy/3Es4/r6BkccBuD960e3pJzM=
-----END CERTIFICATE-----
```


Download | Install Certificate | Back

Figure 6 : Certificate Information

Key Size refers to the size of the key or elliptic curve associated with this certificate.

The “certificate name” must remain the same on all ESKM servers across the cluster.

Import a third-party server certificate

An externally generated public/private key pair can be imported into the ESKM system for use as a server certificate. The encrypted private key data and the public key certificate must be present in the third-party server certificate file. For example:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBAB.........vvbKI=
-----END ENCRYPTED PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDhjCCA.........MKH9Fk
-----END CERTIFICATE-----
```

In addition, the password for the private key file must be known. To import a third-party server certificate, perform the following steps:

1. In **Certificates & CAs**, click **Certificates** to display the Import Certificate section.
2. Provide the source location of the certificate file.
3. Enter the **Certificate Name** and private key password.
4. Click **Import Certificate**.

6.1.5 Setting Up a KMIP Server

The KMIP server provides the interface to clients that use the KMIP protocol. Transport Layer Security (TLS) is required, therefore you must specify the name of the server certificate.

To configure the KMIP server, perform the following steps:

1. Select the **Device** tab.
2. In the **Device Configuration** menu, click **KMIP Server** to display the **KMIP Server Configuration** window.
3. In the **KMIP Server Settings** section, click **Edit**.

4. Configure the KMIP Server Settings. Utimaco recommends the default values of 5696 for the Port and 3600 for the Connection Timeout. If necessary, change the Port and Connection Timeout values. For Server Certificate, select the name of the certificate you created in Setting up ESKM certificate.

If your ESKM server is operating in FIPS-compliant mode, you must specify a KMIP server certificate that meets FIPS requirements.

If your ESKM servers are in a cluster and you are selecting a new KMIP server certificate from the "Server Certificate:" field, you must make sure that all of the ESKM servers in the cluster already have a KMIP server certificate installed with this same name.

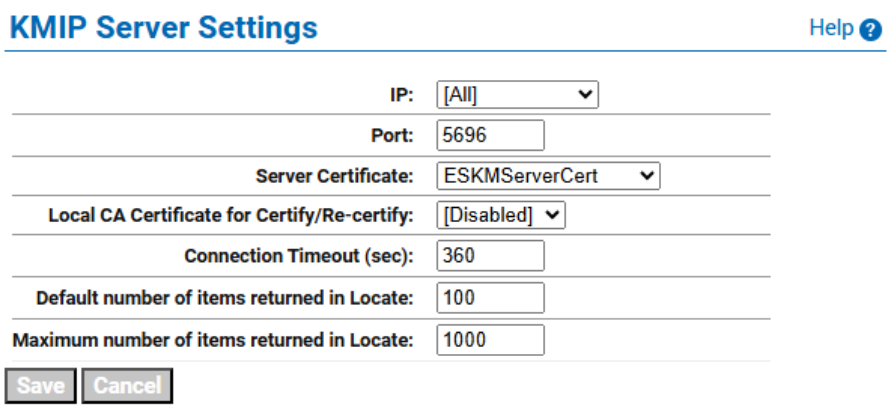


Figure 7 : KMIP Server Settings

5. Click **Save**.

Changing the KMIP server setting causes the KMIP server to restart.

6.1.6 Create Client Certificates

1. In the **Security** > **Certificates& CAs**, Select **Local CAs**.
2. Select the Local CA which is used to sign the CSR.

3. Select **Sign Request**. The following window appears.
4. Select **Certificate Purpose** as **Client**.
5. Paste the one of the CSRs downloaded from the Data-at-Rest Encryption.

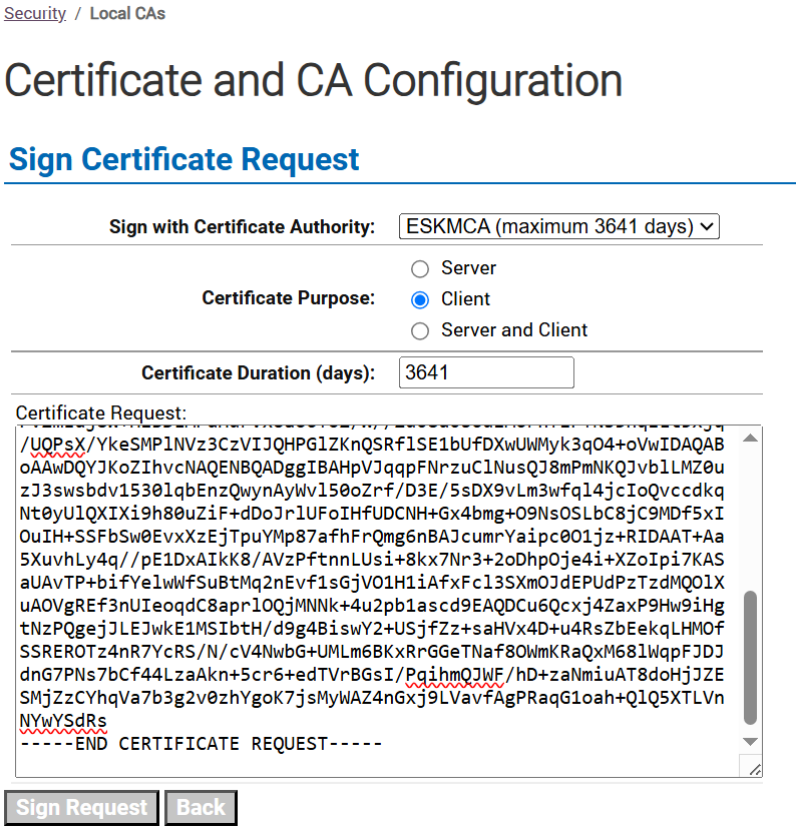


Figure 8 : Sign Request

6. Click **Sign Request**.

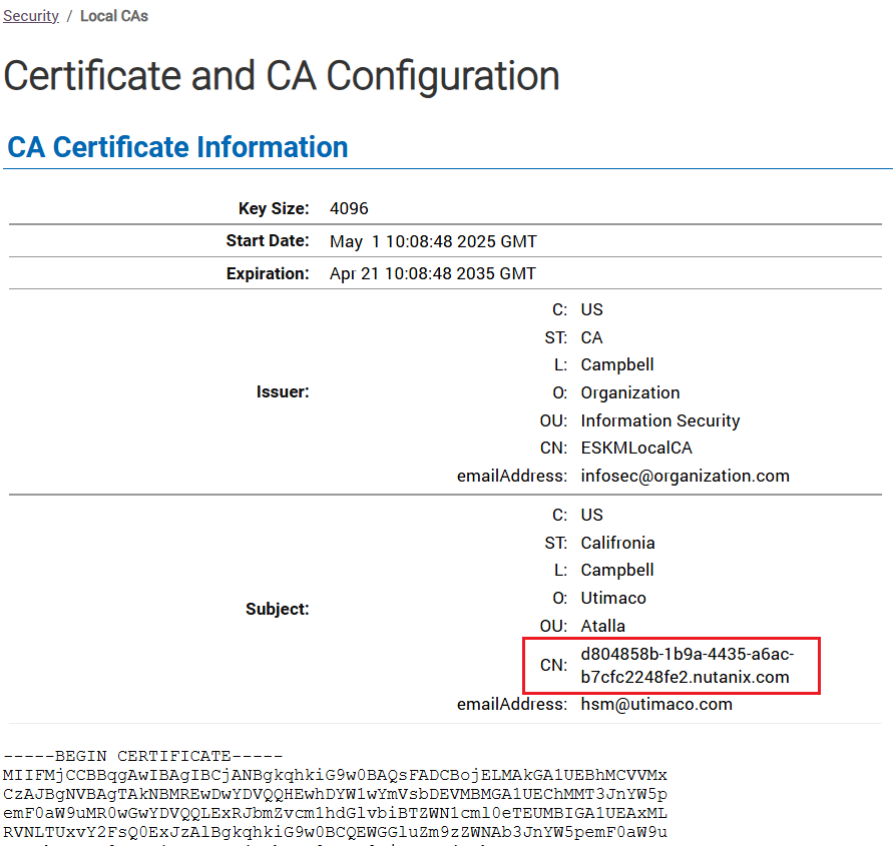


Figure 9 : CA Certificate Information

7. Note the **Common Name**.
8. Download the signed certificate.

6.1.7 Create a Local User

1. In the **Security** > **Local Users & Groups** > **Local Users**, create an ESKM local user using **Common Name**. For more information, refer to the *ESKM_User_Guide-8.54.0.*

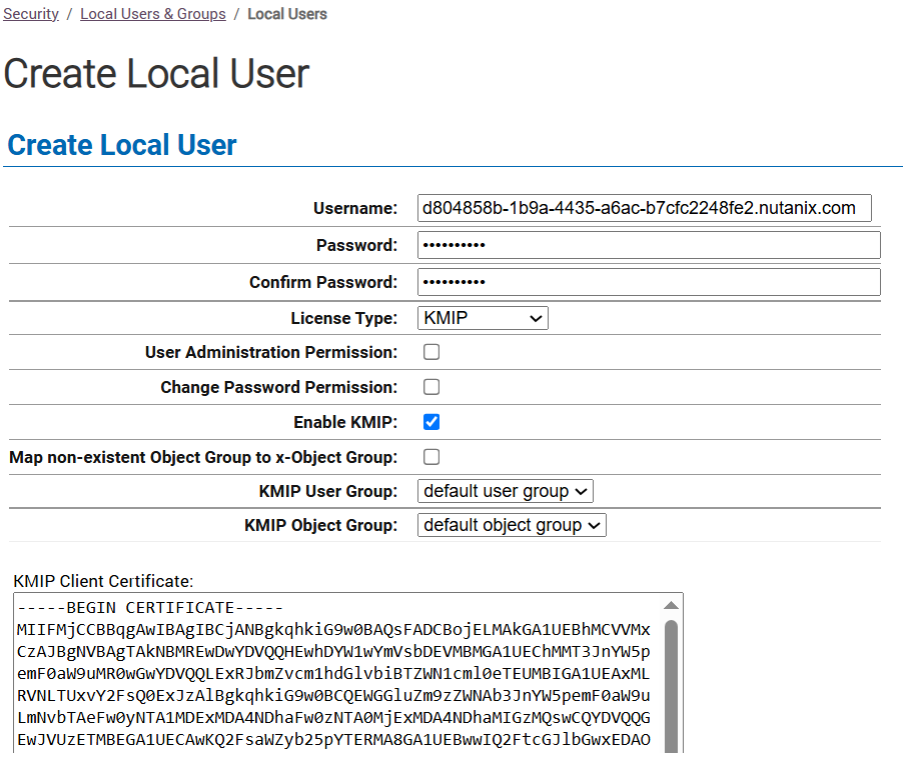


Figure 10 : Create Local User

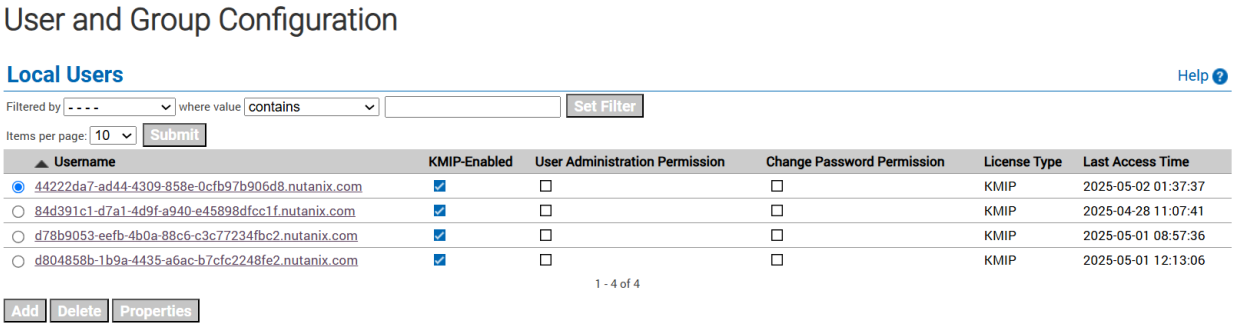


Figure 11 : Local Users

6.2 Configuring on Nutanix AHV

This section provides the step-by-step procedure for integrating ESKM with Nutanix.

1. Log in to **Nutanix Prism Element** as an **Administrator**.

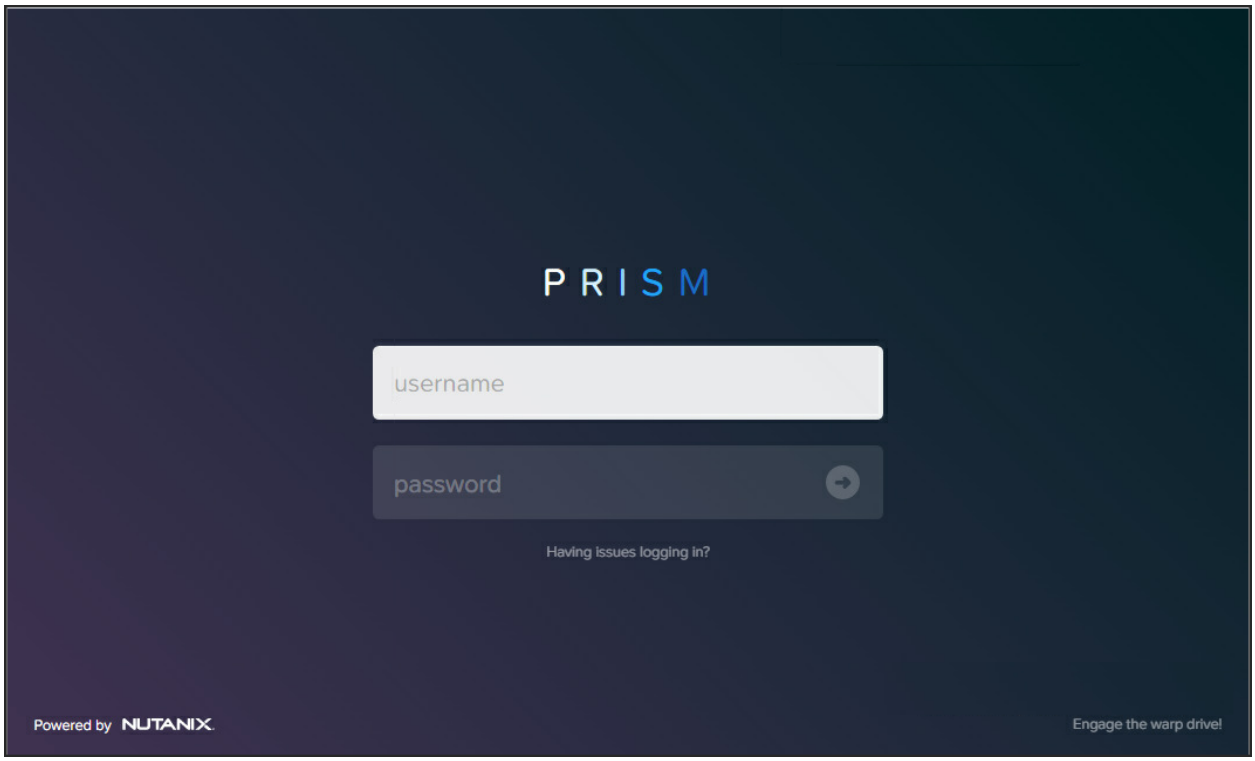


Figure 12 : Login Page

2. Select **Data at Rest Encryption** in the **Settings** page. The **Data-at-Rest Encryption** page appears.

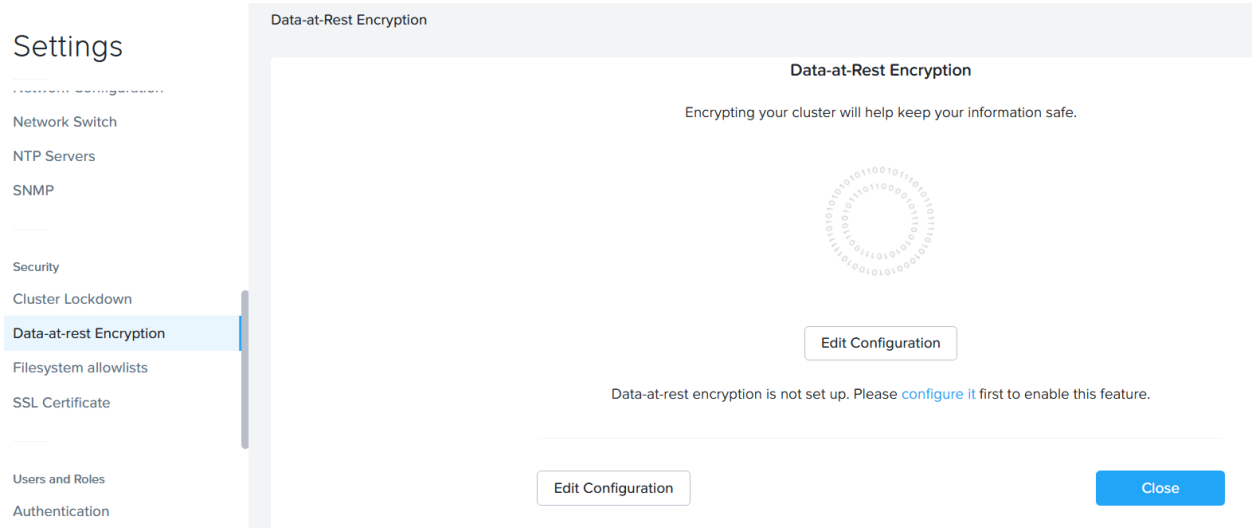
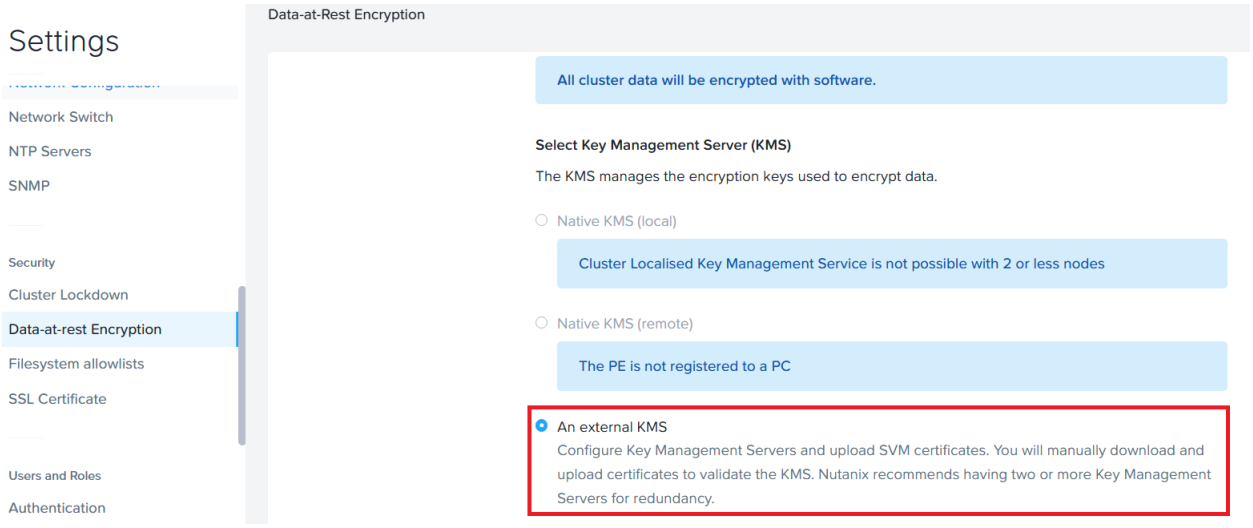


Figure 13 : Data-at-Rest Encryption

3. Click **Create Configuration**. Clicking the **Continue Configuration** button, **configure it** link, or **Edit Config** button does the same thing: it displays the **Data-at-Rest Encryption** configuration page.

4. Select the **Key Management Server** as **An external KMS**.



5. In the **Certificate Signing Request Information** section, do the following:

   - Enter appropriate credentials for your organization in the **Email**, **Organization**, **Organizational Unit**, **Country Code**, **City**, and **State** fields, and then click the **Save CSR Info** button.

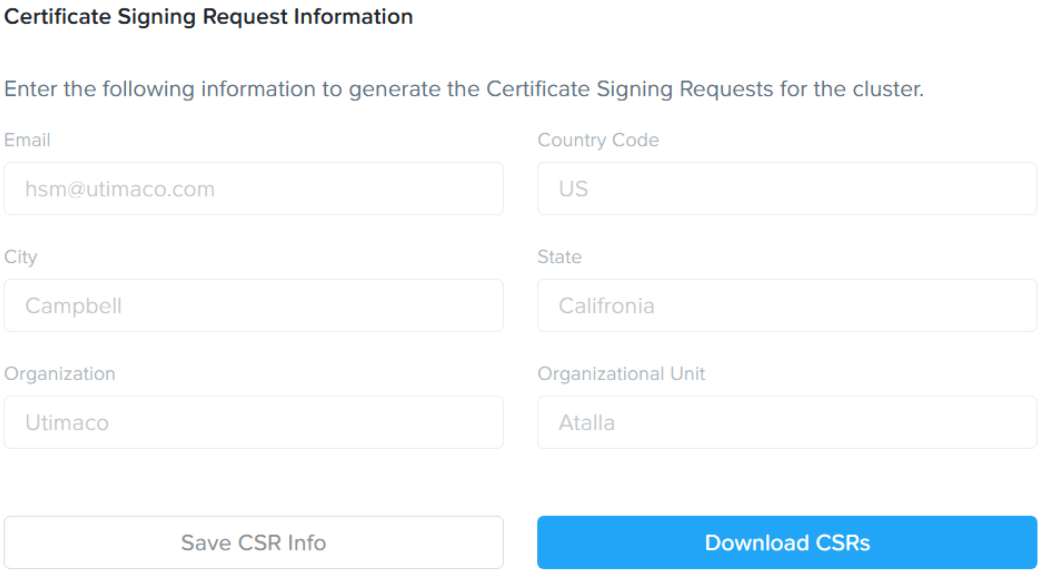


Figure 14 : Certificate Signing Information

- The entered information is saved and used when creating a certificate signing request (CSR). To specify more than one **Organizational Unit** name, enter a comma-separated list.
- Click the **Download CSRs** button, and in the **Certificate Signing Requests** screen, click the **Download CSRs for all nodes** to download a file with CSRs for all the nodes or click a **Download** link to download a file with the CSR for that node.

You can update this information until an SSL certificate for a node is uploaded to the cluster, at which point the information cannot be changed (the fields become read-only) without first deleting the uploaded certificates.

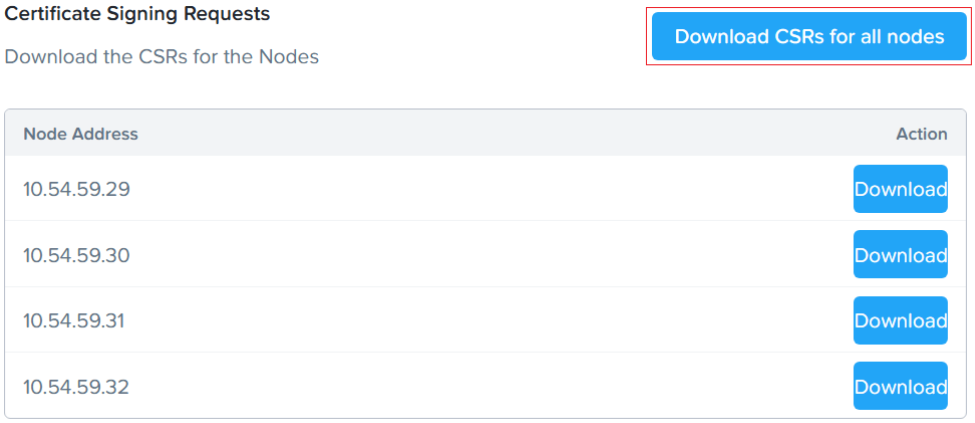


Figure 15 : Download CSRs for all Nodes

After completing step 5, follow the steps below in the ESKM Management Console.

- Create Client Certificates. For detailed information, refer to Create Client Certificates.
- Create an ESKM local user. For detailed information, refer to Create a Local User.
- Repeat the same step for all the CSRs.

6. In the **Key Management Server** section, click the **Add New Key Management Server** button.

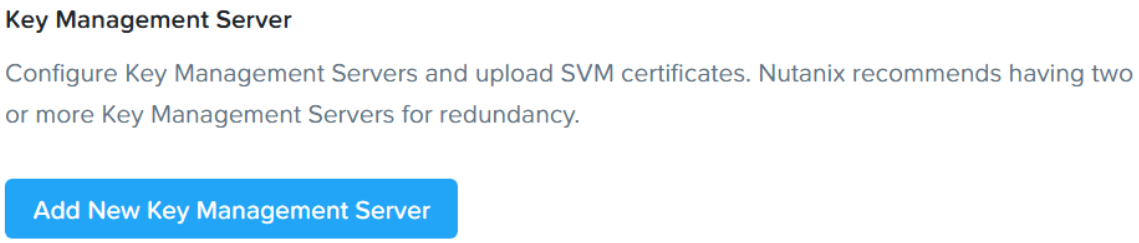


Figure 16 : Add New Key Management Server

7. In the **Add a New Key Management Server** screen, enter the ESKM's **Name**, **IP address**, and **Port Number** in the appropriate fields.

Figure 17 : Add Address

The port is where the key management server is configured to listen for the KMIP protocol. The default port number is 5696.

8. If you have configured multiple key management servers in cluster mode, click the **Add Address** button to provide the addresses for each ESKM device in the cluster.
9. Click **Save**.

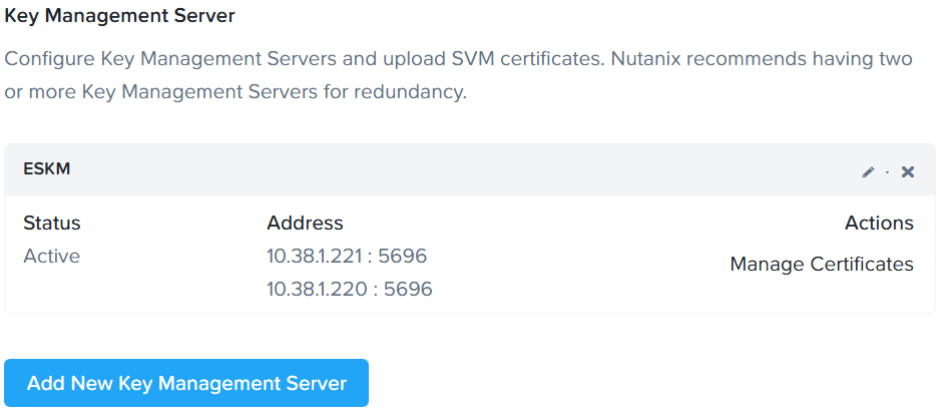


Figure 18 : Manage Certificates

10. In the **KMS CA Certificates**, click **Add New Certificate Authority**.

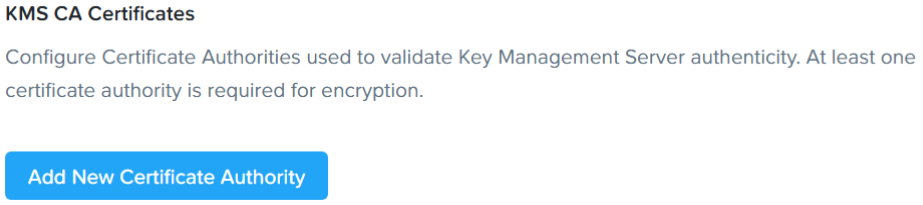


Figure 19 : Add New Certificate Authority

11. In the **Add a New Certificate Authority** section, click **Upload CA Certificate** button to upload the CA Certificate. Upload the **ESKMCA,** which is used to sign the KMIP server and the client certificate.

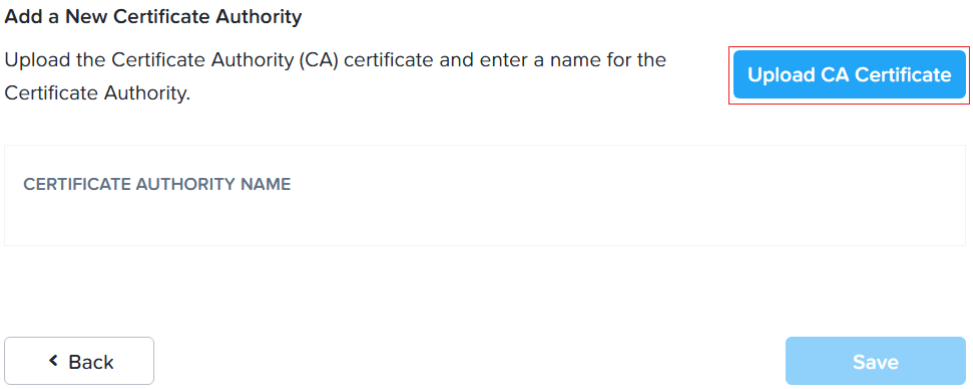


Figure 20 : Upload CA Certificates

12. Enter **Certificate Authority Name**.

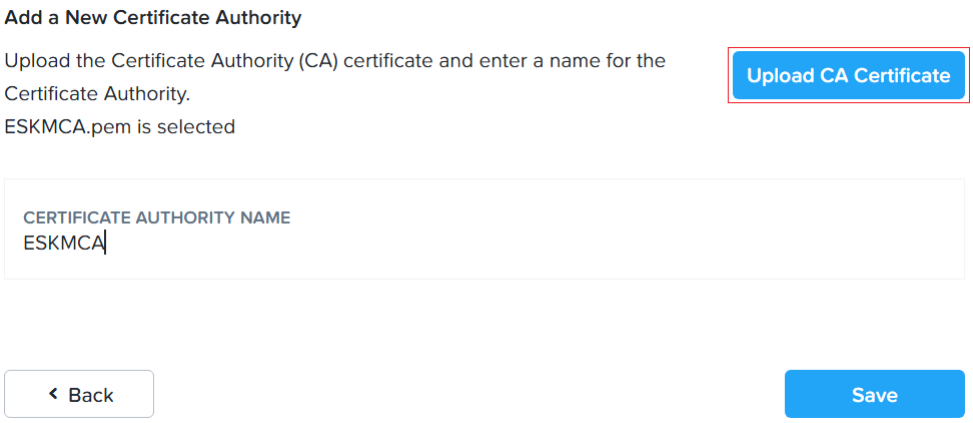


Figure 21 : Certificate Authority Name

13. Click **Save**.

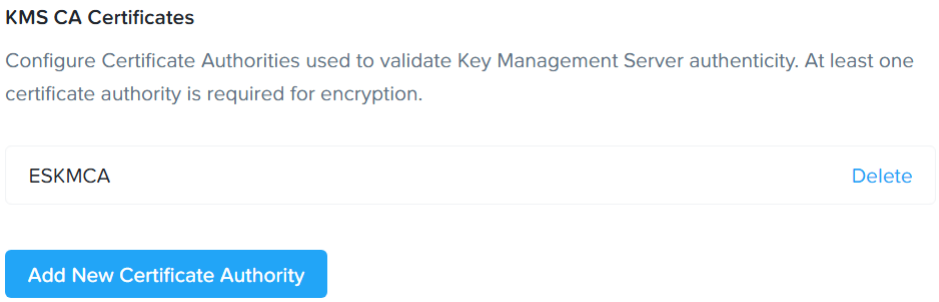


Figure 22 : Certificate Authority Name

14. Go to the **Key Management Server** section. Click the **Manage Certificates** button.
15. In the **Manage Signed Certificates** screen, click **Upload Files** to upload all the signed certificates in one step.

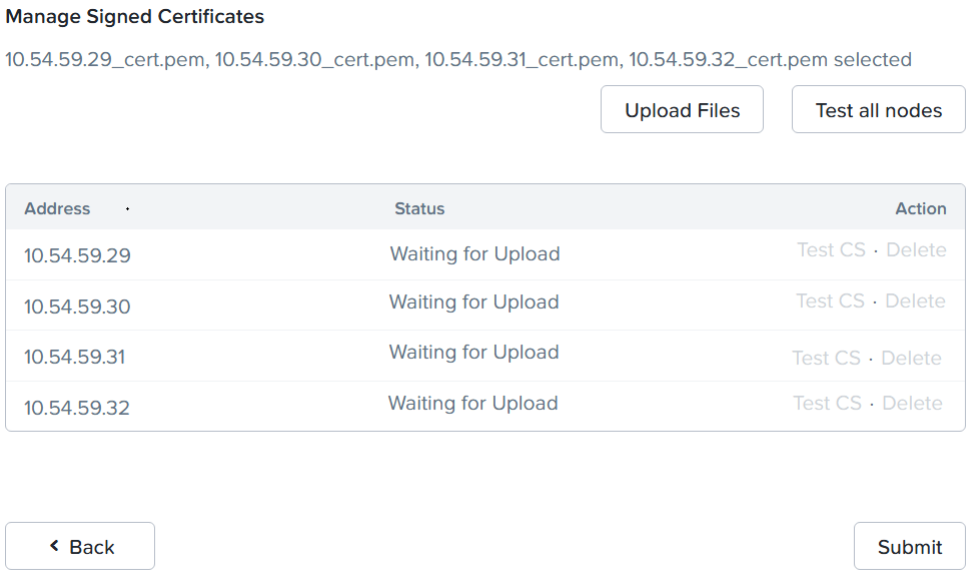


Figure 23 : Managed Signed Certificates

16. Click **Test all nodes** button to test the certificates for all nodes in one step. A status of Verified indicates the test was successful for that node.

If the status shows "**unverified**," that means there is a connectivity or certificate issue with the Key Management Server. Make sure all nodes show "**Verified**" before you enable encryption.

17. Click **Submit**. The following window displays.

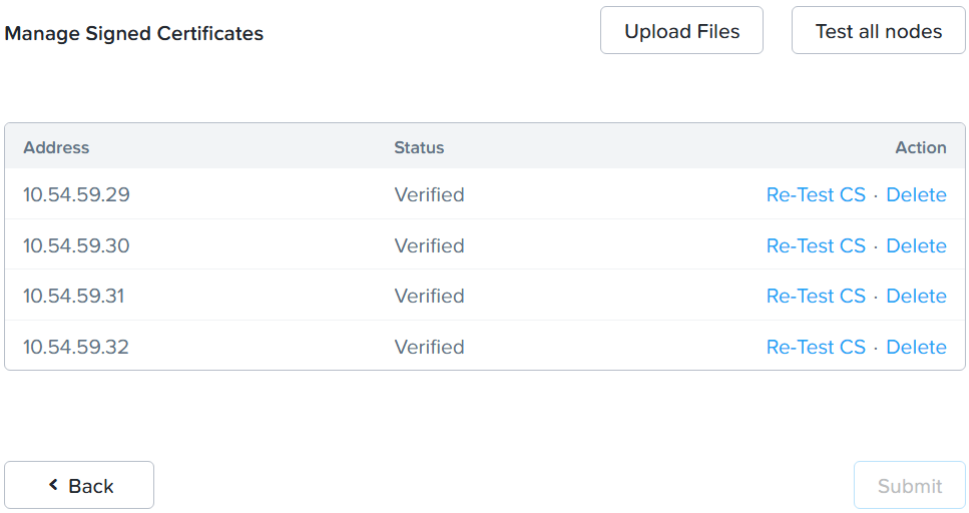


Figure 24 : Uploaded Signed Certificates

18. When the configuration is complete, click the **Enable Encryption** button.

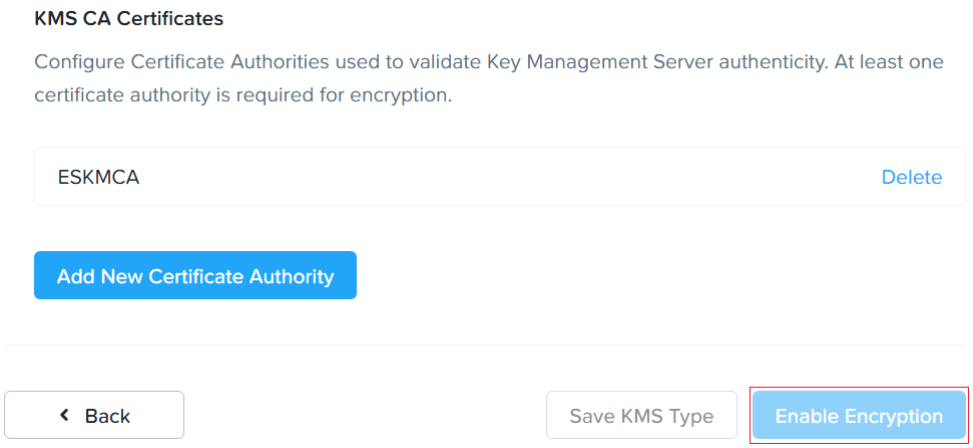


Figure 25 : Enable Encryption

19. **Enable Encryption** window is displayed.

Figure 26 : Data-at-Rest Encryption Screen

To help ensure your data's security, you cannot disable software-only data-at-rest encryption once it is enabled. Nutanix recommends regularly backing up your data, encryption keys, and key management server.

- Type **ENCRYPT** and click **Encrypt** button. The data-at-rest encryption is enabled. To view the status of the encrypted cluster or container, go to **Data at Rest Encryption** in the **Settings** menu.

When you enable encryption, a low-priority background task runs to encrypt all the unencrypted data. This task is designed to take advantage of any available CPU space to encrypt the unencrypted data within a reasonable time. If the system is occupied with other workloads, the background task consumes less CPU space. Depending on the amount of data in the cluster, the background task can take 24 to 36 hours to complete.

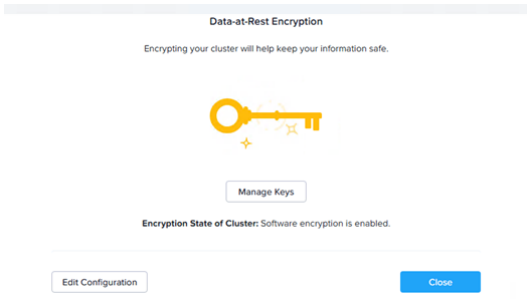


Figure 27 : Data-at-Rest Encryption Screen - Encrpyting Cluster

Once the task to encrypt a cluster begins, you cannot cancel the operation. Even if you stop and restart the cluster, the system resumes the operation.

For changing the Key Encryption Keys, see https://portal.nutanix.com/page/documents/details?targetId=Nutanix-Security-Guide-v6_10:wc-security-data-encryption-passwords-wc-aos-t.html#ntask_gjp_mks_gq.

7 Verification and Testing

7.1 Logs and Validation Steps

7.1.1 KEK Retrieval after Full Cluster Restart

1. Shutdown VMs in the Nutanix cluster.
2. Stop Nutanix Cluster Services.
3. Shutdown CVMs and Nutanix Hosts in the cluster, wait for 3 minutes to power drain and verify shutdown status.
4. Shut down both Active nodes of KMS Server.
5. Power on Hosts and verify status(CVMs power on automatically).
6. Start Nutanix Cluster Services.
7. Power on the VMs to test the KEK(Key Encryption Key) is not retrieved from the KMS, and the DEK(Data Encryption Key) cannot successfully unlock the Drives to boot the VMs.
8. Power on and start services for the First Active KMS Nod,e and attempt to boot the Nutanix VMs and record behavior.

Expected Results

- When both Active-Active KMS nodes are down, the cluster fails to retrieve the Key from KMS and decrypt the container. As a result, the test-VM using the disk from the container can read the disk but fails to boot.

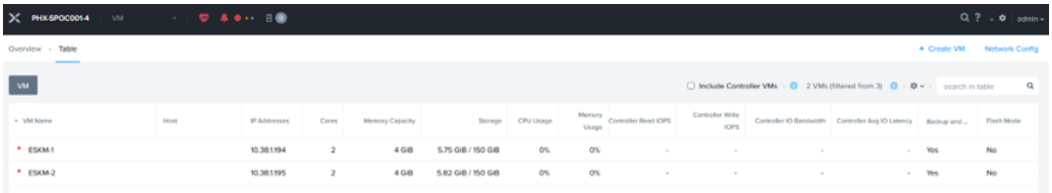


Figure 28 : Active - Active KMS

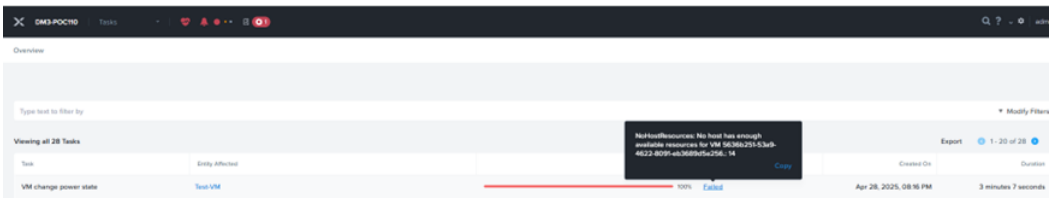


Figure 29 : Failed to Boot

- When ESKM-1 is DOWN and ESKM-2 is UP in the Active-Active cluster, the cluster retrieves the Key from ESKM-2 and decrypts the container. As a result, the test-VM using the disk from the container reads the disk and the VM-boots successfully.

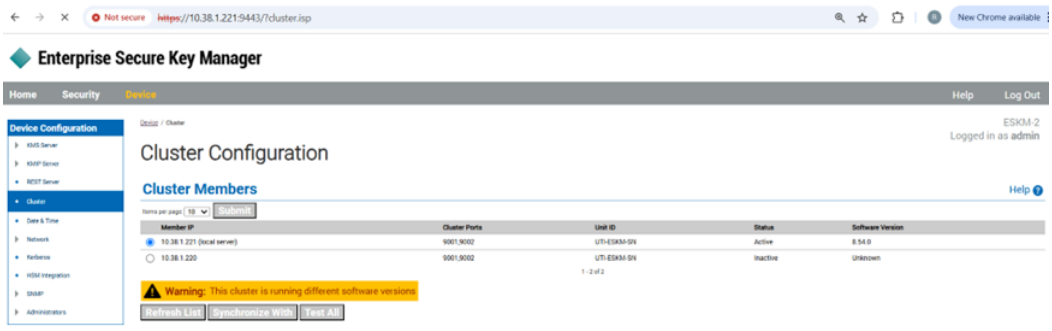


Figure 30 : Cluster Configuration

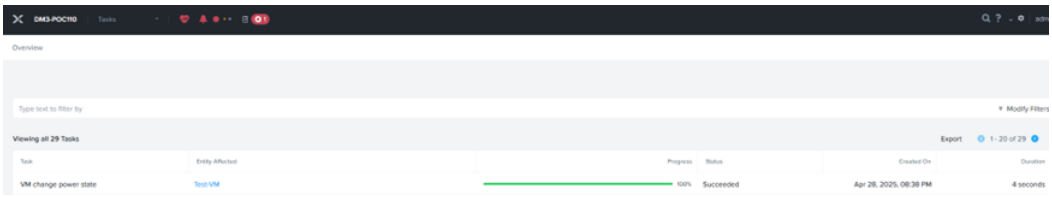


Figure 31 : VM Boot Success

Figure 32 : Test- VM

- When ESKM-2 is DOWN and ESKM-1 is UP in the Active-Active cluster, the cluster retrieves the Key from ESKM-1 and decrypts the container. As a result, the test-VM using the disk from the container reads the disk and the VM-boots successfully.

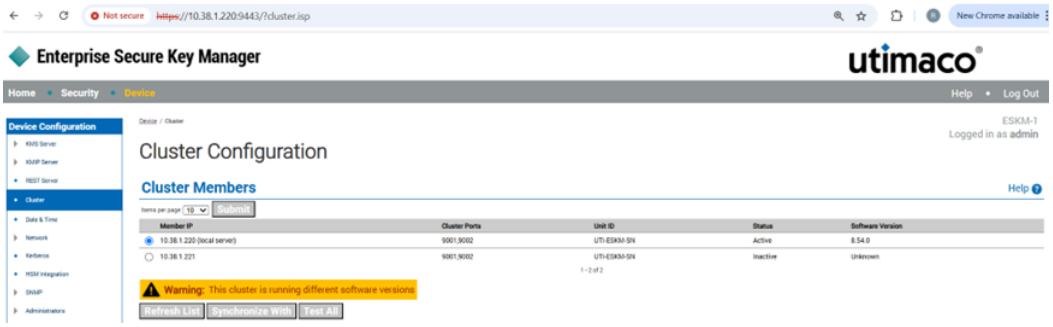


Figure 33 : Cluster Configuration

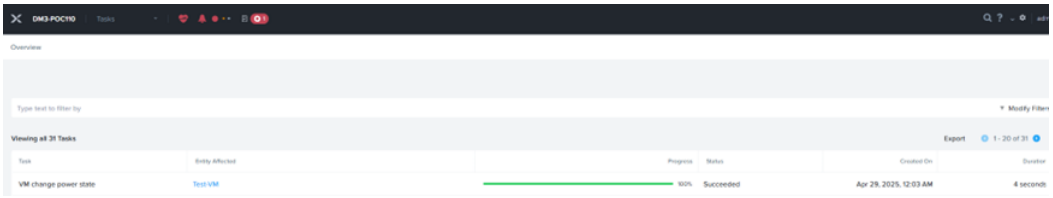


Figure 34 : VM Boot Success

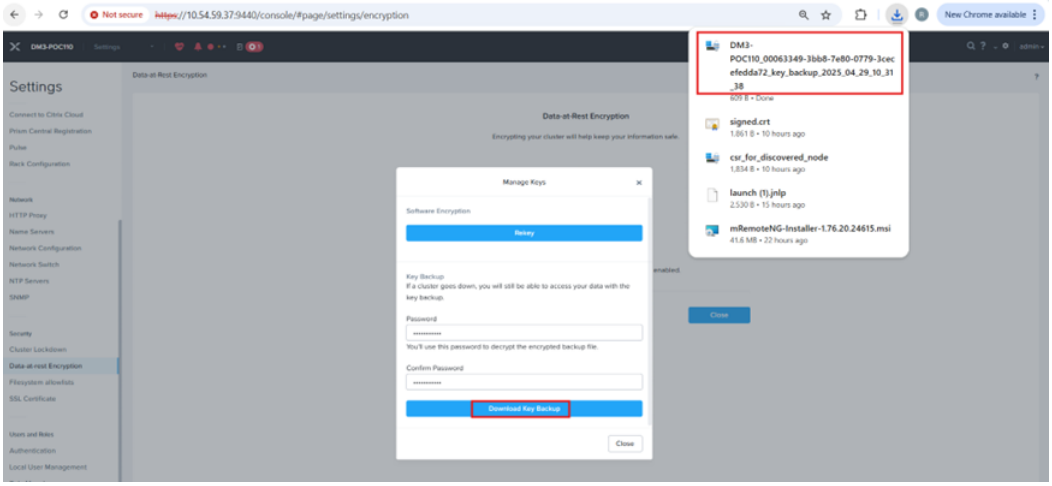
Figure 35 : Test-VM

7.1.2 Backing up Keys

1. Log in to Nutanix Prism Element as an administrator.
2. Select **Data at Rest Encryption** in the **Settings** page.
3. In the Cluster Encryption page, select **Manage Keys**.

4. Enter and confirm the password.
5. Click the **Download Key Backup** button.

   The backup file is saved in the default download location on your local machine.



Verify that the download of the “Key” file is successful and saved in the default download location.

For more information on backing up Keys, see https://portal.nutanix.com/page/documents/details?targetId=Nutanix-Security-Guide-v6_8:wc-security-data-encryption-export-key-t.html#ntask_vlq_v5g_mbb

7.1.3 Validating with Re-keys

1. Log in to Nutanix Prism Element as an administrator.
2. Select **Data at Rest Encryption** in the **Settings** page.
3. In the **Cluster Encryption** page, select **Manage Keys** and click the **Rekey** button under **Software Encryption**. For more information on validating with Re-keys, see https://portal.nutanix.com/page/documents/details?targetId=Nutanix-Security-Guide-v6_7:wc-security-data-encryption-passwords-wc-aos-t.html.

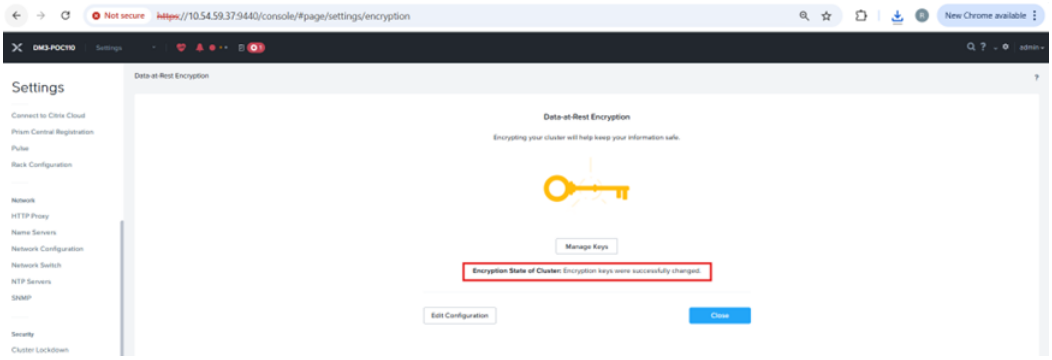


Figure 36 : Re-key

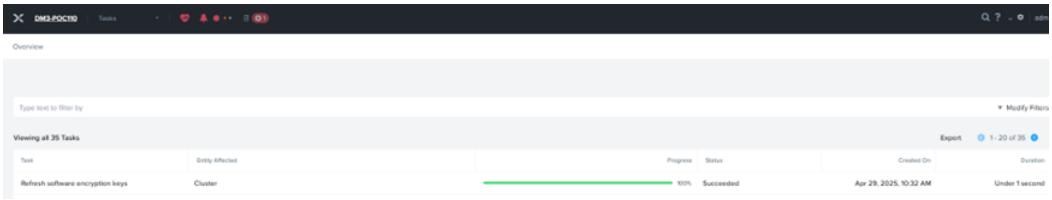


Figure 37 : Re-key Success

4. Shut down VMs in the Nutanix cluster.
5. Stop Nutanix Cluster Services.
6. Shut down CVMs and Nutanix Hosts in the cluster, wait for 3 minutes for the power to drain, and verify the shutdown status.
7. Shut down both nodes of KMS Server.
8. Power on Hosts and verify status(CVMs power on automatically).
9. Start Nutanix Cluster Services.
10. Power on the VMs to test the KEK (Key Encryption Key) is not retrieved from the KMS, and the DEK (Data Encryption Key) cannot successfully unlock the Drives to boot the VMs.
11. Power on and start services for the Active KMS Node and attempt to boot the Nutanix VMs and record behavior.

Verify the events/logs of the KMS cluster to see if the keys are fetched successfully from the new active KMS server.

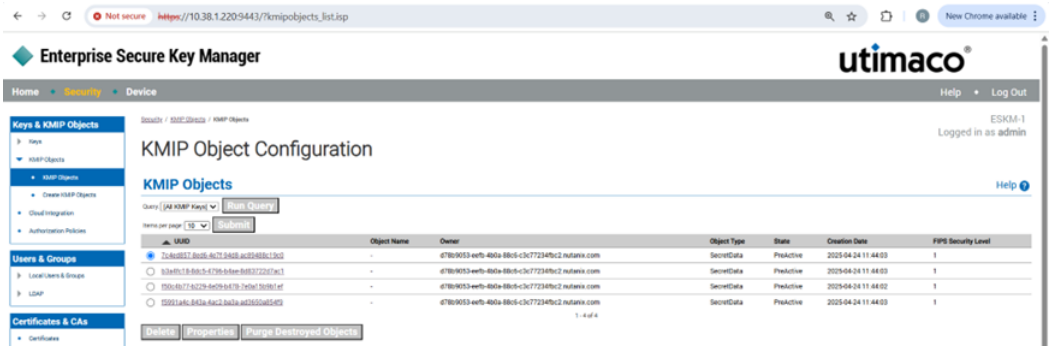


Figure 38 : Before Re-key

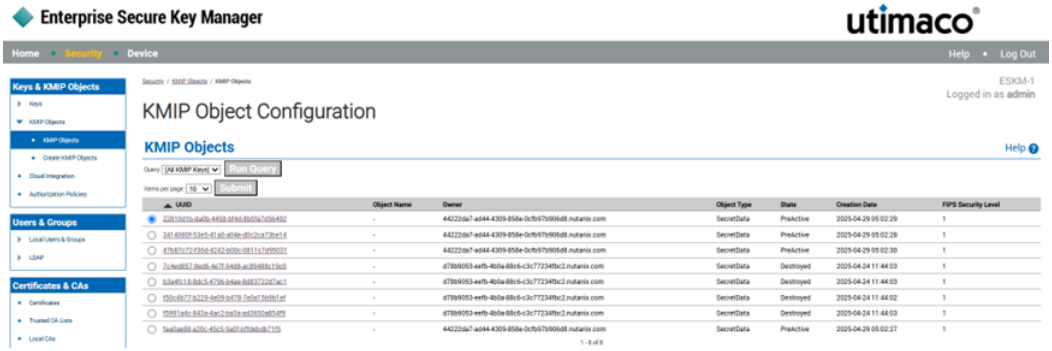


Figure 39 : After Re-Key

7.1.4 Validate Encryption on Cluster Expansion

1. Log in to the Nutanix Prism Element web console.
2. Do one of the following:
   - Select **Expand Cluster** in the **Settings** page. (or)
   - Go to the **Hardware** dashboard and click the **Expand Cluster** button.

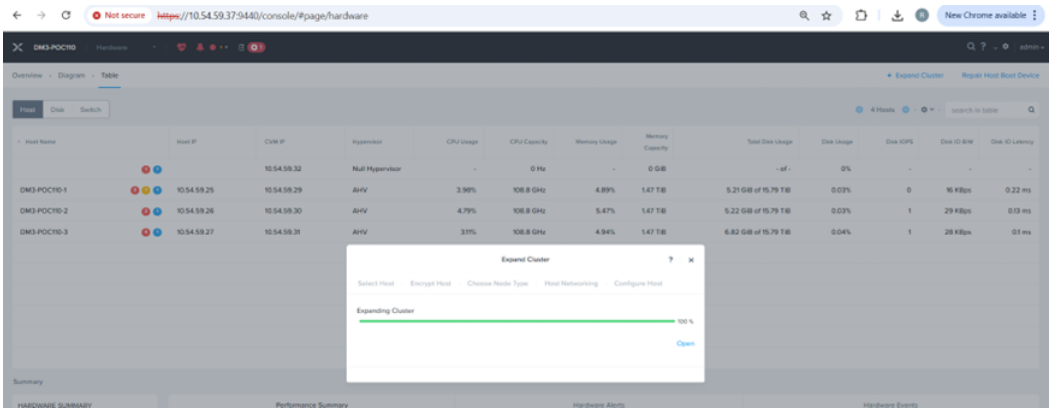


Figure 40 : Expand Cluster

3. In the **Expand Cluster** window, select (click the radio button for) the desired option and then click the **Next** button:

    - Select **Expand Cluster** to begin the expansion immediately (after you complete the remaining configuration steps).

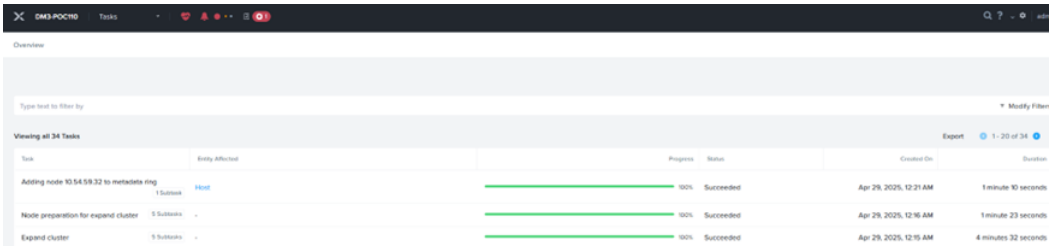


Figure 41 : Expand Cluster - Success

Select **Prepare Now and Expand Later** to prepare the nodes now but delay adding them to the cluster until a later time. Preparing the nodes includes imaging the hypervisor (if needed), upgrading the AOS version (if needed), and preparing a new node network configuration (if needed). For more information on expanding the cluster, see https://portal.nutanix.com/page/documents/details?targetId=Web-Console-Guide-Prism-v6_7:wc-cluster-expand-wc-t.html.

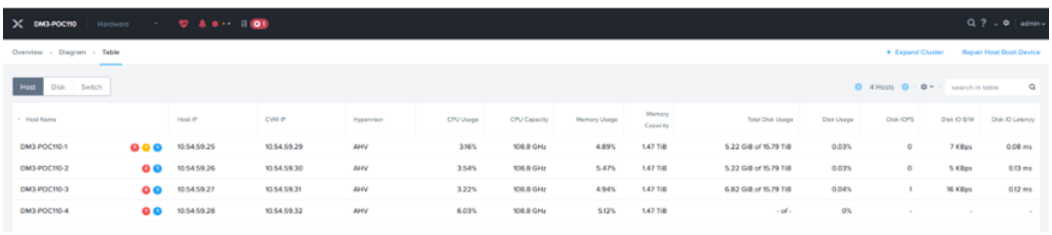


Figure 42 : Expanded Cluster

Ensure that factory-prepared node(s) are imaged with the same AOS/AHV version of the cluster. Re-imaging is not possible during expansion.

4. In Nutanix Prism Settings, expand the cluster and check if the node(s) appear in the discovered list.
5. Select the node(s) and add them to the cluster.
6. Enter the details for the Host Name, Controller VM, Hypervisor, and IPMI IP.
7. In the Encrypt Host, click "Generate and download CSR".
8. Get the CSRs signed by a certificate authority (CA).
9. Upload a signed certificate in order for the nodes to connect to the KMS server.
10. Choose the Node type as "HCI Node".
11. Choose the uplink for Host Networking.
12. Click "**Run Checks**" to verify that the nodes are ready.
13. Complete the cluster expansion.

Verify that the node is successfully added to the cluster and test the connectivity to the KMS servers.

7.1.5 Validate Encryption After Node Removal

1. Log in to the Nutanix Prism Element web console.
2. Select the node you want to remove in one of the following ways:

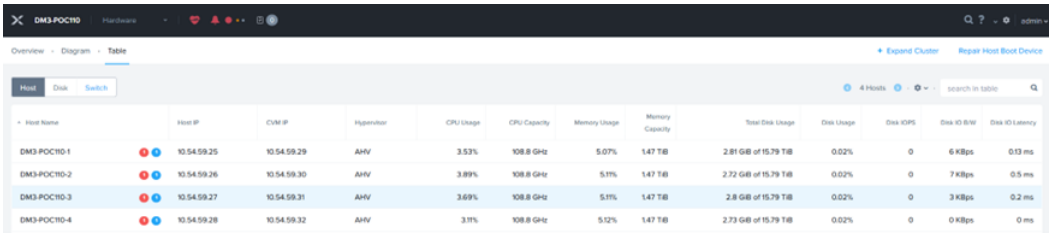


Figure 43 : Before Removing Node

3. On the diagram page, select the target node (host). (Or)
   In the **Table** page, click the **Host** tab and select the node (host).
4. Click the **Remove Host** link on the right of the **Summary** line.

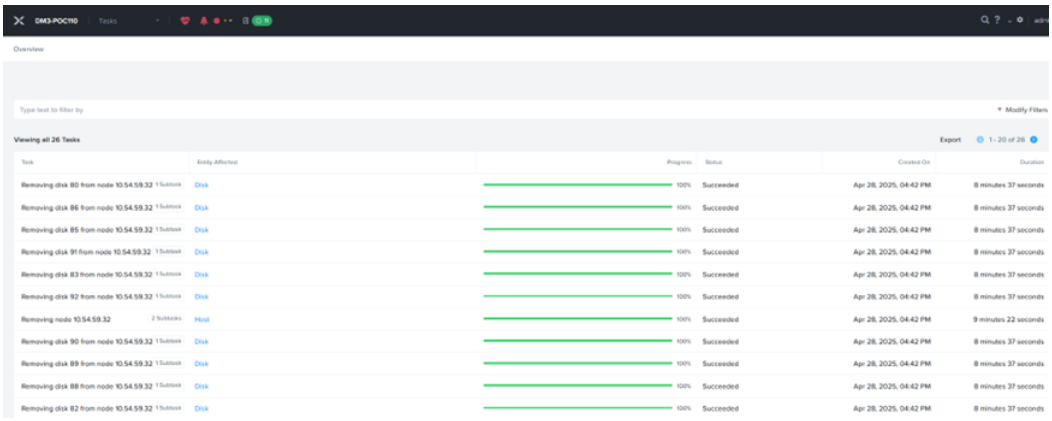


Figure 44 : Removing Nodes

5. Click the **OK** button in the confirmation dialog box.

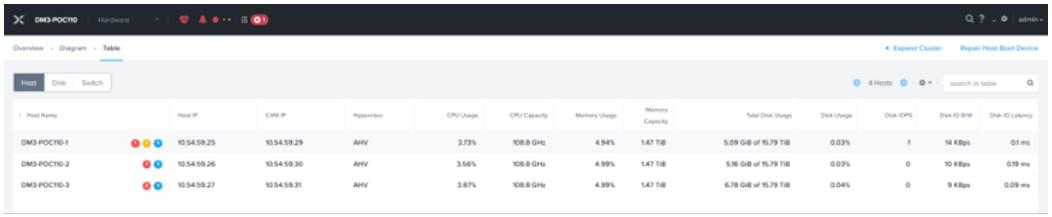


Figure 45 : After Removing Nodes

For more information on removing a node from a cluster, see https://portal.nutanix.com/page/documents/details?targetId=Web-Console-Guide-Prism-v6_7:wc-removing-node-pc-c.html.

Verify that the node has been removed from the Prism—Hardware page and from the 'KMS server—Managed Signed Certificate list.'

7.1.6 Perform a Crypto-Erase

Data on the AOS cluster is always encrypted, and the data encryption key (DEK) used to read the encrypted data is known only to the AOS. All data on the drive can effectively be destroyed (that is, become permanently unreadable) by deleting the container or cluster. This is known as a crypto-erase.

1. Log in to any CVM in the cluster using SSH.
2. Power off all the VMs that are running on the hosts in the cluster.
   `nutanix@cvm$ acli vm.off *`
3. Stop the Nutanix cluster.
   `nutanix@cvm$ cluster stop`
4. Destroy the cluster.
   `nutanix@cvm$ cluster destroy`

For more information on destroying a cluster, see https://portal.nutanix.com/page/documents/details?targetId=Nutanix-Security-Guide-v6_8:wc-security-data-encryption-destroy-wc-aos-t.html.

8 Troubleshooting

8.1 Log Location and Interpretations

Verify the logs on the Utimaco ESKM by following the below steps:

1. In the ESKM Management Console, click Device tab.
2. Click on Log Viewer under the Logs & Statistics.
3. Click on KMIP under the Log Viewer.

8.2 Contact for Support

8.2.1 Utimaco Technical Support

For technical questions, contact Utimaco Technical Support:

- E-mail: support-atalla@utimaco.com
- Telephone: 800-500-7858 (U.S.A.) +1-916-414-0216 (International)
- Website: https://support.utimaco.com/

Before contacting Utimaco with your questions, collect the following information:

- Product model names and numbers
- Technical support registration number or NonStop system number (if applicable)
- Service Agreement ID number (SAID)
- Product serial numbers
- Error messages
- Software version number

8.2.2 24-hour support

24-hour emergency support is available to those customers who have valid service contracts. Use this service for product and system emergencies that occur after normal working hours or

on weekends and U.S. holidays. Questions about product installation and setup are supported during normal working hours.

For 24-hour emergency support call: 800-500-7858 (U.S.A.) +1-916-414-0216 (International).

9 Appendices

9.1 References

Title	Description	Document/Link
Enterprise Secure Key Manager v8.54.0 Installation and Replacement Guide	Setup and configuration steps for Utimaco ESKM	ESKM_Installation and Replacement_Guide.pdf
Enterprise Secure Key Manager v8.54.0 Release Notes.	New features, enhancements and fixes related to Utimaco ESKM.	ESKM_Release_Notes.pdf
Enterprise Secure Key Manager v8.54.0 User Guide	Provide detailed instructions for managing the Utimaco ESKM.	ESKM_User_Guide.pdf
OASIS Websites	OASIS websites for more information on the Key Management Interoperability Protocol (KMIP) specification, usage guides and profiles	https://www.oasis-open.org/standards https://wiki.oasis-open.org/kmip/KnownKMIPImplementations

Table 6: References