



Nutanix and Entrust Cryptographic Security Platform Key Management Vault

Integration Guide

2026-07-10

Table of Contents

1. Introduction	1
1.1. Product configurations.....	1
1.2. Supported features	1
1.3. Requirements	2
2. Install and configure Entrust Cryptographic Security Platform Key Management Vault ..	3
2.1. Upload the Key Management Vault ISO in AHV	3
2.2. Deploy a Key Management Vault node on AHV.....	5
2.3. Initial Configuration of Entrust Key Management Vault and Compliance Manager Nodes.....	9
2.4. Configure the Compliance Manager node	11
2.5. Join the two Key Management Vault nodes to form a cluster.....	11
2.6. Create a KMIP Key Management Vault	11
3. Test the integration by enabling data-at-rest encryption	14
3.1. Select KeyControl as the KMIP Server and generate the certificate requests.....	14
3.2. Create the KMIP client certificate bundles	16
3.3. Add the Entrust Key Management Vault KMIP cluster to the Nutanix AHV cluster.....	18
3.4. Add the Entrust KeyControl KMIP cluster certificates to the Nutanix AHV cluster.....	19
3.5. Enable encryption.....	21
4. Integrating with an HSM.....	22
5. Additional resources and related products.....	23
5.1. nShield as a Service	23
5.2. Entrust CSP Key Manager.....	23
5.3. Entrust products.....	23
5.4. nShield product documentation.....	23

Chapter 1. Introduction

This document describes the integration of a Nutanix AHV cluster with the Entrust Cryptographic Security Platform Key Management Vault (KMS). Entrust Cryptographic Security Platform Key Management Vault serves as the KMS for the Nutanix AHV cluster, communicating over the open-standard Key Management Interoperability Protocol (KMIP).

1.1. Product configurations

The following versions have been tested for compatibility:

Product	Version
Nutanix AOS	v7.5
Entrust Cryptographic Security Platform	1.4
Entrust Key Management Vault	v10.5.3
Entrust Compliance Manager	v10.5.3

1.2. Supported features

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

Entrust KeyControl Feature	Support
Deployment in Nutanix AHV from ISO	Yes
Cluster Mode	Yes
Cluster Expansion	Yes
Node Removal	Yes
Retain Configuration After Total Cluster Power-Down	Yes

The following Nutanix features have been tested in this integration:

Supported Nutanix Feature	Support
Data-at-Rest Encryption	Yes
Cluster Expansion	Yes
Node Removal	Yes
Re-Keying	Yes

1.3. Requirements

To integrate the Entrust Cryptographic Security Platform Key Management Vault and the Nutanix AHV cluster, you must have:

- Access to the [Entrust TrustedCare Portal](#).
- Access to the [Nutanix online services and portals](#).

Familiarize yourself with:

- The [Cryptographic Security Platform Vault v10.5.3 Online Documentation Set](#).

Chapter 2. Install and configure Entrust Cryptographic Security Platform Key Management Vault

A two-node cluster was deployed for this integration. Key Management Vault can be deployed on AHV using the ISO image. The ISO image is available at [Software Downloads](#). Installation instructions are available at [ISO Installation](#).

- [Upload the Key Management Vault ISO in AHV](#)
- [Deploy a Key Management Vault node on AHV](#)
- [Initial Configuration of Entrust Key Management Vault and Compliance Manager Nodes](#)
- [Configure the Compliance Manager node](#)
- [Join the two Key Management Vault nodes to form a cluster](#)
- [Create a KMIP Key Management Vault](#)

2.1. Upload the Key Management Vault ISO in AHV

For reference, see the following Nutanix online documentation:

- [Adding an Image](#).
- [Configuring Images](#).

1. Log in to the Nutanix Prism Central web UI.
2. Select **Prism Center** > **Infrastructure** > **Compute** > **Images**.
3. Select **Add Image**.
4. Under **Image Source**, ensure the **Image File** radio button is selected and then select **Add File**.
5. Locate and add the Entrust ISO file.
6. Enter a **Name**, select the **Image Type**, and enter a **Description**, then select **Next**.

The screenshot shows the 'Select Image' step (1) of a two-step process. The 'Image Source' section has three radio buttons: 'Image File' (selected), 'URL', and 'VM Disk'. Below this is a '+ Add File' button. The 'Source' field displays '[LOCAL]\Entrust-CSP-Vaults-10.5...' with a 'Remove Image' link. The 'General' section contains a 'Name' field with 'Entrust-CSP-Vaults-10.5.3-1053000316...', a 'Type' dropdown set to 'ISO', a 'Description (Optional)' field with 'Test Upload', and a 'Checksum (Optional)' field with a 'SHA-1' dropdown. At the bottom are 'Cancel' and 'Next' buttons.

7. On the next screen, leave the default values selected.

The screenshot shows the 'Select Location' step (2) of a two-step process. The 'Placement Method' section has two radio buttons: 'Place Image directly on clusters' (selected) and 'Place Image using Image Placement policies'. The 'Place Image directly on clusters' option has a description: 'This option is good for smaller environments. The image will be placed on all selected clusters below.' The 'Place Image using Image Placement policies' option has a description: 'This option is good for larger environments. It requires you to first set up Image Placement policies between categories assigned to clusters and categories assigned to images. From there on, you only need to associate a relevant category to an image while uploading it here.' The 'Select Clusters' section has a heading 'Select the set of clusters to use for placement' and a table with two columns: 'Name' and 'Bandwidth Limit'. The table has one row with a checked checkbox, the name 'RNO-NXRDY005', and an empty bandwidth limit field. At the bottom are '< Back', 'Cancel', and 'Save' buttons.

8. Select **Save**. The operation may take close to a minute to complete.

2.2. Deploy a Key Management Vault node on AHV

For more information, refer to [VM Management](#) in the Nutanix online documentation.

1. Log in to the Nutanix Prism Central web UI.
2. Select **Prism Center > Infrastructure > Compute > VM**.
3. Select **Create VM**.
4. Complete the **Create VM** dialog as follows, then select **Next**:
 - a. **Name**: Enter a name for the vault, for example, "entrust-csp-vault-1".
 - b. **Description**: If required, add a description for the VM. This field is optional.
 - c. **Project**: Leave the default value
 - d. **Cluster**: Leave the default value
 - e. **Number of VMs**: 1
 - f. **VM Properties**: 4 CPUs, 2 Cores, 8 GB RAM

The screenshot shows the 'Create VM' dialog in the Nutanix Prism Central web UI, specifically the 'Configuration' tab. The dialog has four tabs: 1 Configuration, 2 Resources, 3 Management, and 4 Review. The 'General' section contains the following fields: 'Name' with the value 'entrust-csp-vault-1', 'Description (Optional)' with the value 'Entrust Vault Server 1', 'Project' set to '_Internal', and 'Cluster' set to 'RNO-NXRDY005'. The 'Number of VMs' field is set to '1'. The 'VM Properties' section shows 'CPUs' set to '4' (with a 'vCPUs' label), 'Cores Per CPU' set to '2' (with a 'Cores' label), and 'Memory' set to '4' (with a 'GB' label). At the bottom right, there are 'Cancel' and 'Next' buttons.

5. Attach the **CD-ROM**: Under **Disks**, select **Attach Disk**.
6. Complete the **Attach Disk** window as follows, then select **Save**:
 - a. **Type**: Select **CD-ROM**.

- b. **Operation:** Select **Clone from Image**
- c. **Image:** Select the image you created earlier.
- d. **Bus Type:** Select **SATA**.
- e. Leave the other fields set to the default values.

Attach Disk [X]

Type
CD-ROM [v]

Operation
Clone from Image [v]

Disk Placement
☒ Same cluster ☐ Other cluster

To place disks on other clusters, you need atleast two HCI clusters running on AHV, with AOS version 7.5 or higher. [X]

Image
Entrust-CSP-10.5.3-1053000316.iso [v]

Storage Cluster
RNO-NXRDY005 [v]

Used to place VM Disks.

Once the first disk is created using storage from a specific cluster, all successive disks will use the same cluster for storage.

Cancel Save

- 7. Attach another **Disk**: Under **Disks**, select **Attach Disk**.
- 8. Complete the **Attach Disk** window as follows, then select **Save**.
 - a. **Type**: Select **Disk**.
 - b. **Operation**: Select **Allocate on Storage Container**.
 - c. **Capacity**: 80 GB.



For the Compliance Manager VM, the minimum requirement is 250 GB.

- d. **Bus Type**: Select **SATA**.
- e. Leave the other fields set to the default values.

Attach Disk

×

Type

Disk

Operation

Allocate on Storage Container

Disk Placement

☒ Same cluster
☐ Other cluster

i To place disks on other clusters, you need atleast two HCI clusters running on AHV, with AOS version 7.5 or higher.

×

Storage Container

default-container-64793673060108

i VM disks can only be created on cluster - RNO-NXRDY005.

Capacity

1

GiB

Bus Type

SCSI

Cancel

Save

9. Attach a Subnet: Under **Network**, select **Attach to Subnet**.
10. Complete the **Attach to subnet** window as follows, then select **Save**:
 - a. **Subnet**: Select the Subnet.
 - b. **Assignment Type**: Select **Assign Static IP**.
 - c. **IP Address**: Enter the IP address.
 - d. Leave the other fields set to the default values.

Subnet Attachment

Subnet

VLAN-1123-RNO-NXRDY005

VLAN ID

1123

IPAM

Managed

Network Connection State

Connected

Private IP Assignment

Network Address / Prefix	Free IPs (In Subnet)	Free IPs (In Pool)
	163	41

Assignment Type ?

IP Address

Assign Static IP

NIC Configuration

Cancel

Save

11. In the **Boot Configuration**, select **Legacy BIOS**, then select **Next**.
12. Set the **Timezone**, then select **Next**.
13. Select **Create VM**.

You can track the progress of the VM creation process:

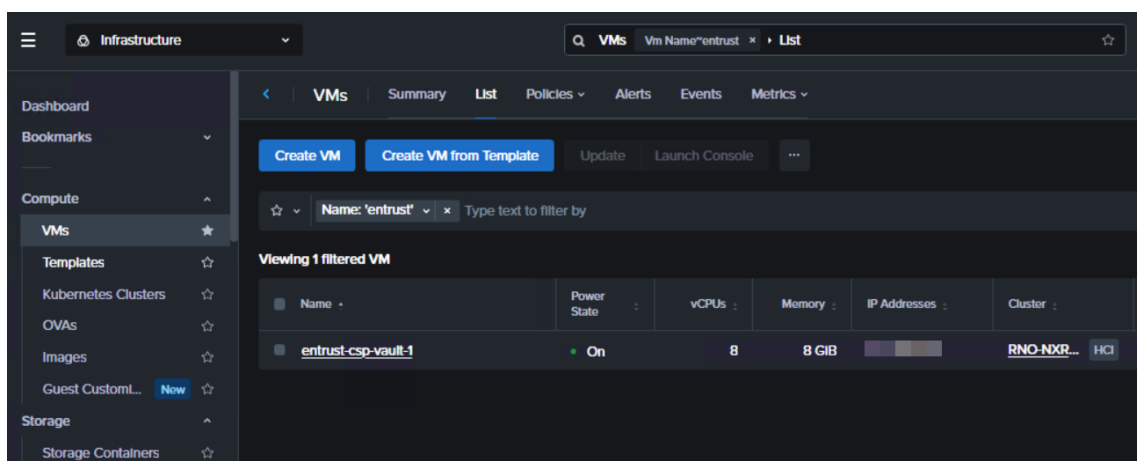


14. Repeat all steps to create a second Entrust Key Management Vault node and a Compliance Manager node.

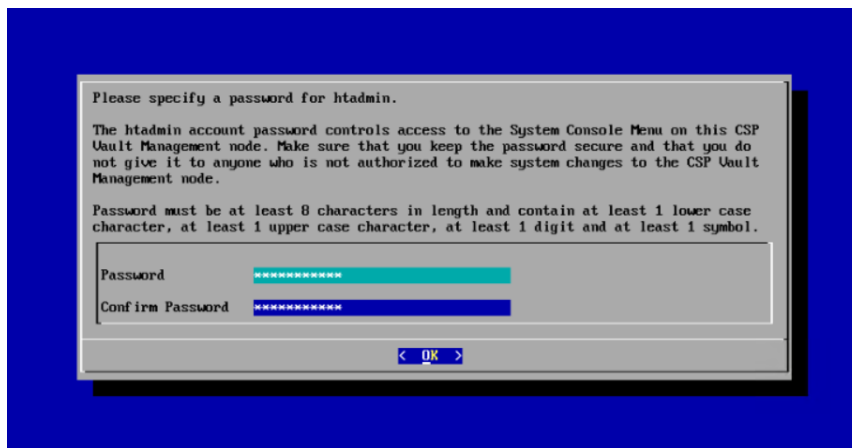
2.3. Initial Configuration of Entrust Key Management Vault and Compliance Manager Nodes

Perform the following steps for each of the VMs you have created:

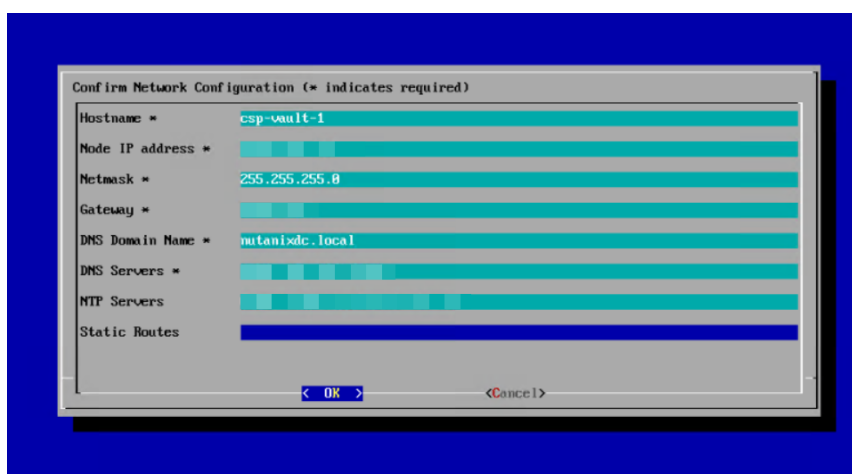
1. Log in to the Nutanix Prism Central web UI.
2. Select **Prism Center** > **Infrastructure** > **Compute** > **VM**.
3. Search for and select the required VM.



4. Under **Power Operations**, select **Power On**.
5. Select **Launch Console**.
6. After the installer finishes, when prompted for a password for the **htadmin** account, set the password and select **OK**.



7. Enter the network information.



8. Verify the network information and select **Yes**.
9. Select **OK** once setup is complete.
10. In a browser, go to the URL (<https://Node IP address>) and log in with the default secroot credentials.

The default secroot password is **secroot**.

11. Accept the license agreement.
12. Select **Continue as a Standalone Node**.
13. Enter a new password for the secroot user and select **Update Password**.
14. Configure the email settings then select **Continue**.

-
15. Select **Download** and save the admin key.
 16. Select **Continue**.

2.4. Configure the Compliance Manager node

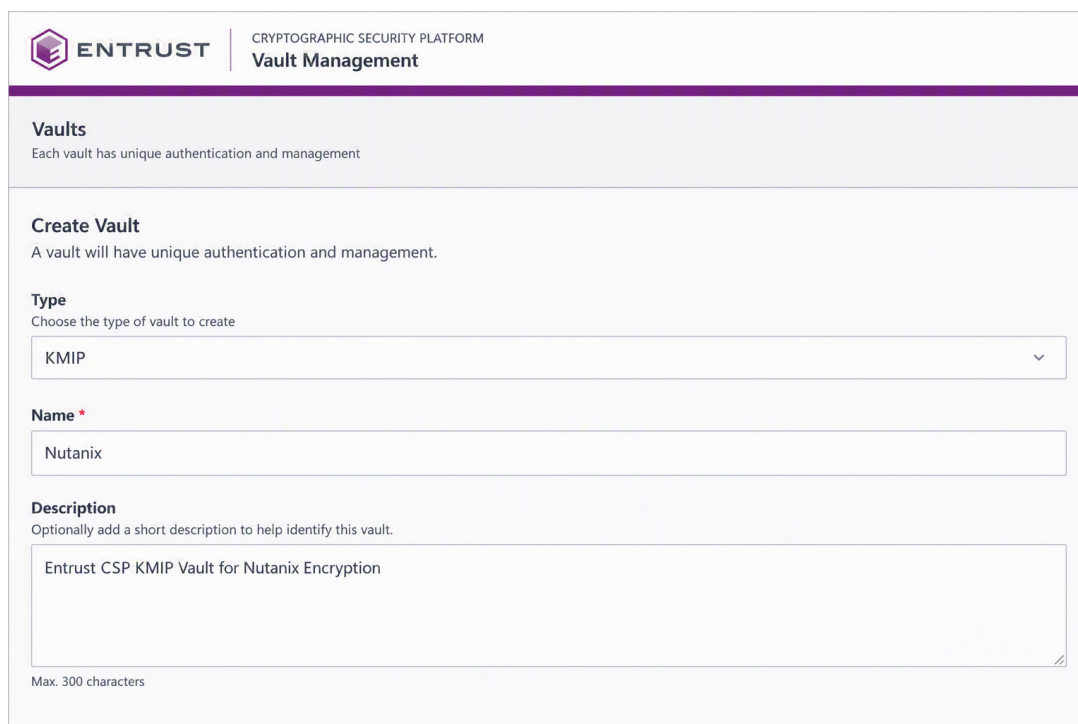
Configure the Compliance Manager to establish an initial Appliance Cluster connection with the first Key Management Vault node. For more information, refer to [Creating an Appliance Cluster Connection](#).

2.5. Join the two Key Management Vault nodes to form a cluster

Join the two Key Management Vault nodes in a high-availability cluster following the instructions in [Installing an Additional CSP Vault Cluster Node on a VM from an ISO Image](#).

2.6. Create a KMIP Key Management Vault

1. Sign in to the KeyControl Appliance Manager.
2. If it loads in the **Appliance Management** view, select **SWITCH TO: Manage Vaults** in the toolbar at the top of the window.
3. On the **Vault Management** home page, select **Create Vault**. The **Create Vault** dialog appears.
4. Complete the **Create Vault** dialog as follows, then select **Create Vault**:
 - a. **Type**: Select **KMIP**.
 - b. **Name**: Enter a name for the vault.
 - c. **Description**: Enter a description.
 - d. **Email Notifications**: Leave it **Off** unless you configured email when you set up the CSP Vault node.
 - e. **Administrator**: Enter **Administrator**.
 - f. **Admin Email**: Enter your company email.



ENTRUST CRYPTOGRAPHIC SECURITY PLATFORM
Vault Management

Vaults

Each vault has unique authentication and management

Create Vault

A vault will have unique authentication and management.

Type
Choose the type of vault to create

KMIP

Name *

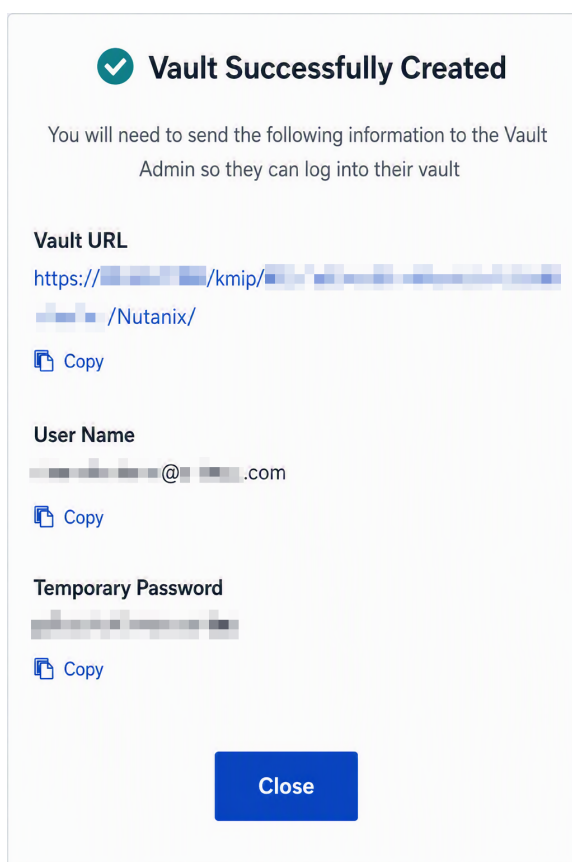
Nutanix

Description
Optionally add a short description to help identify this vault.

Entrust CSP KMIP Vault for Nutanix Encryption

Max. 300 characters

5. Bookmark the URL and save the credentials displayed in the confirmation dialog.



✓ **Vault Successfully Created**

You will need to send the following information to the Vault Admin so they can log into their vault

Vault URL
https://[redacted]/kmip/[redacted]
[redacted]/Nutanix/
Copy

User Name
[redacted]@[redacted].com
Copy

Temporary Password
[redacted]
Copy

Close

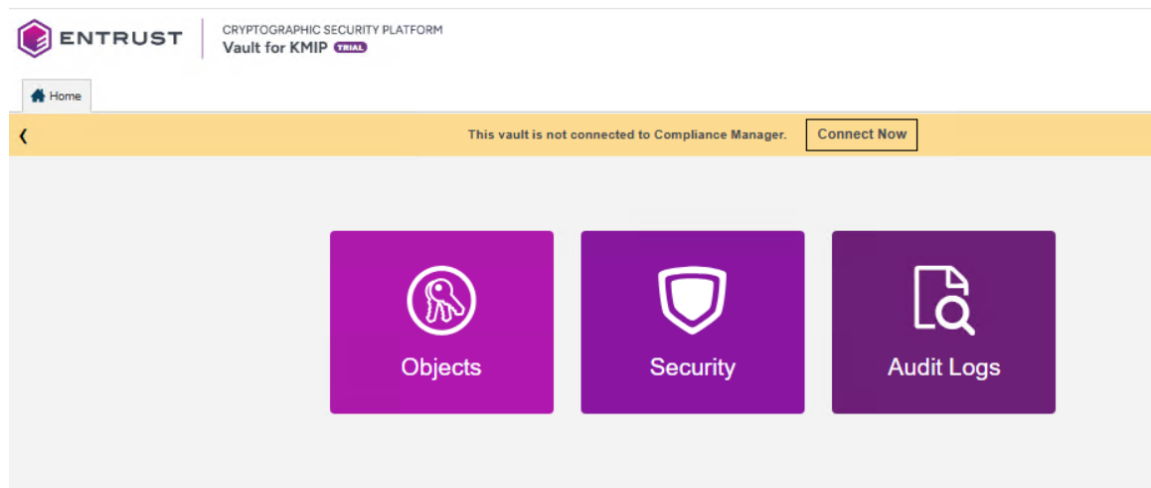
6. In a web browser, navigate to the vault URL.

Sign in to the Vault with the user name and the temporary password that you saved in the

previous step.

+ The user name should be the email address that you specified when you created the vault.

1. Change the initial password when prompted.
2. Sign in again to verify the new credentials.

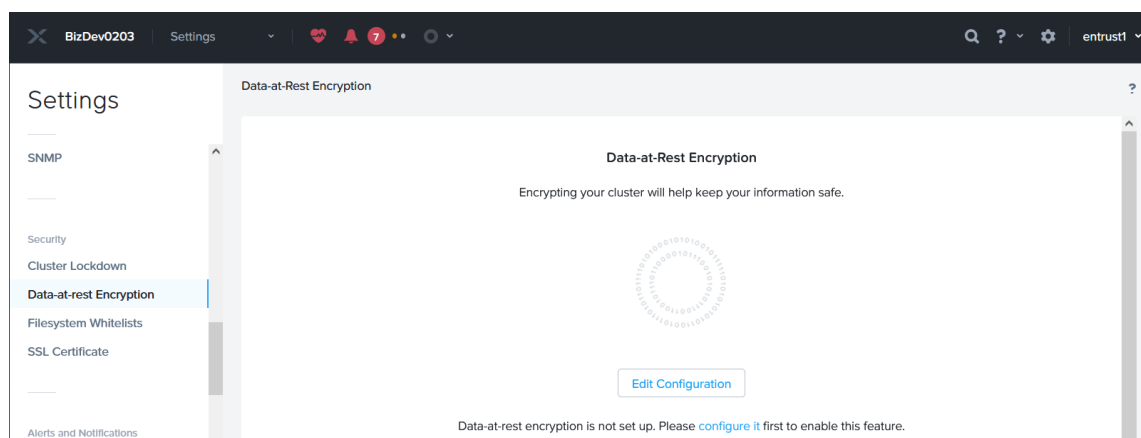


Chapter 3. Test the integration by enabling data-at-rest encryption

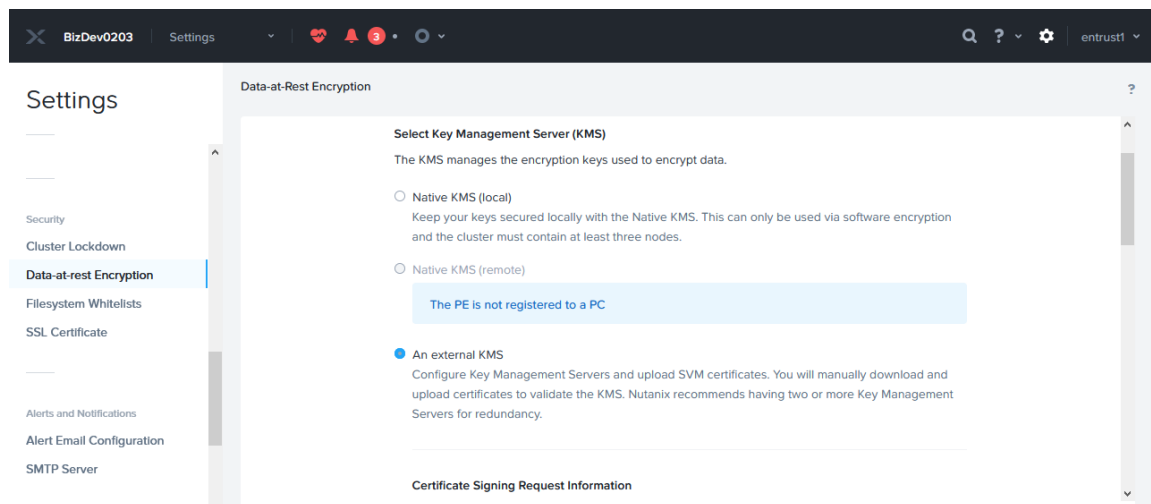
- Select KeyControl as the KMIP Server and generate the certificate requests
- Create the KMIP client certificate bundles
- Add the Entrust Key Management Vault KMIP cluster to the Nutanix AHV cluster
- Add the Entrust KeyControl KMIP cluster certificates to the Nutanix AHV cluster
- Enable encryption

3.1. Select KeyControl as the KMIP Server and generate the certificate requests

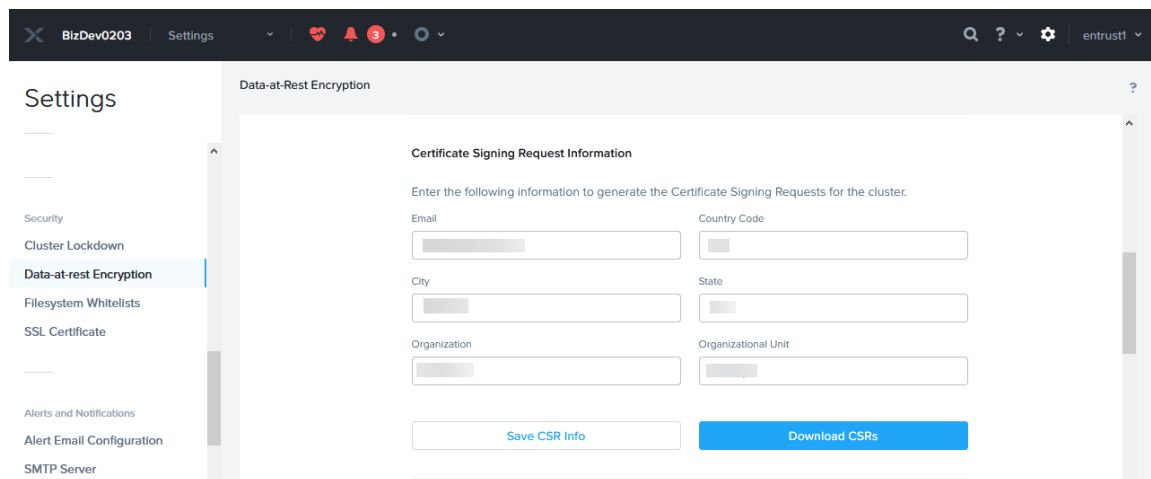
1. Log in to the Nutanix Prism Element web UI.
2. In the toolbar, on the right-hand side, select the gear icon to display the **Settings** menu.
3. Select **Data-at-rest Encryption** under **Security** on the **Settings** left pane, then select **Edit Configuration** or **Continue Configuration**.



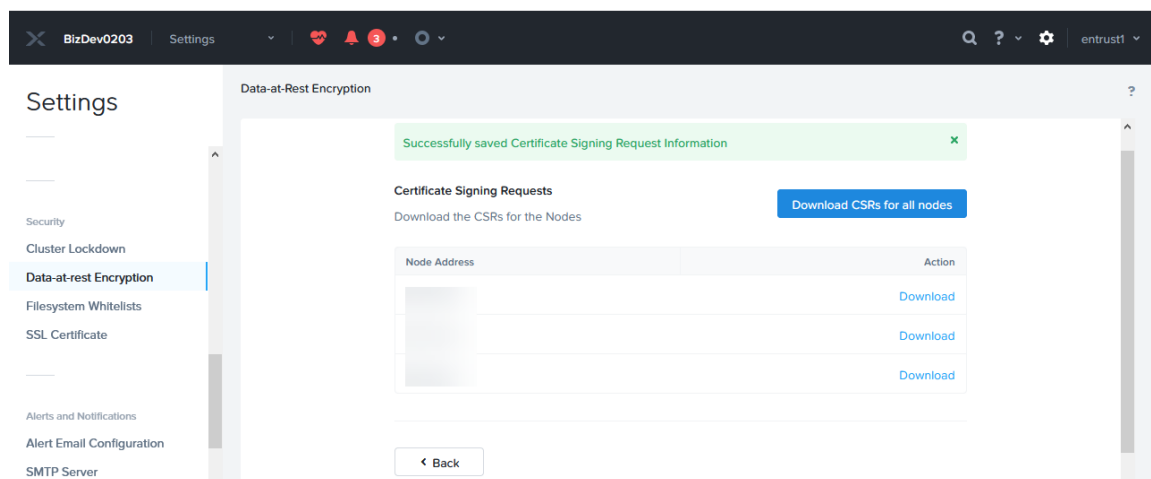
4. Select **An external KMS**.



5. Scroll down to **Certificate Signing Request Information**. Complete the request form, then select **Save CSR Info**.



6. Select **Download CSRs**.
7. When the **Certificate Signing Request** form appears, select **Download CSRs for all nodes**.



This creates a compressed **csrs.zip** file.

8. Save the **csrs.zip** file locally and extract the files.

A certificate request file is created for each node in the Nutanix AHV cluster.

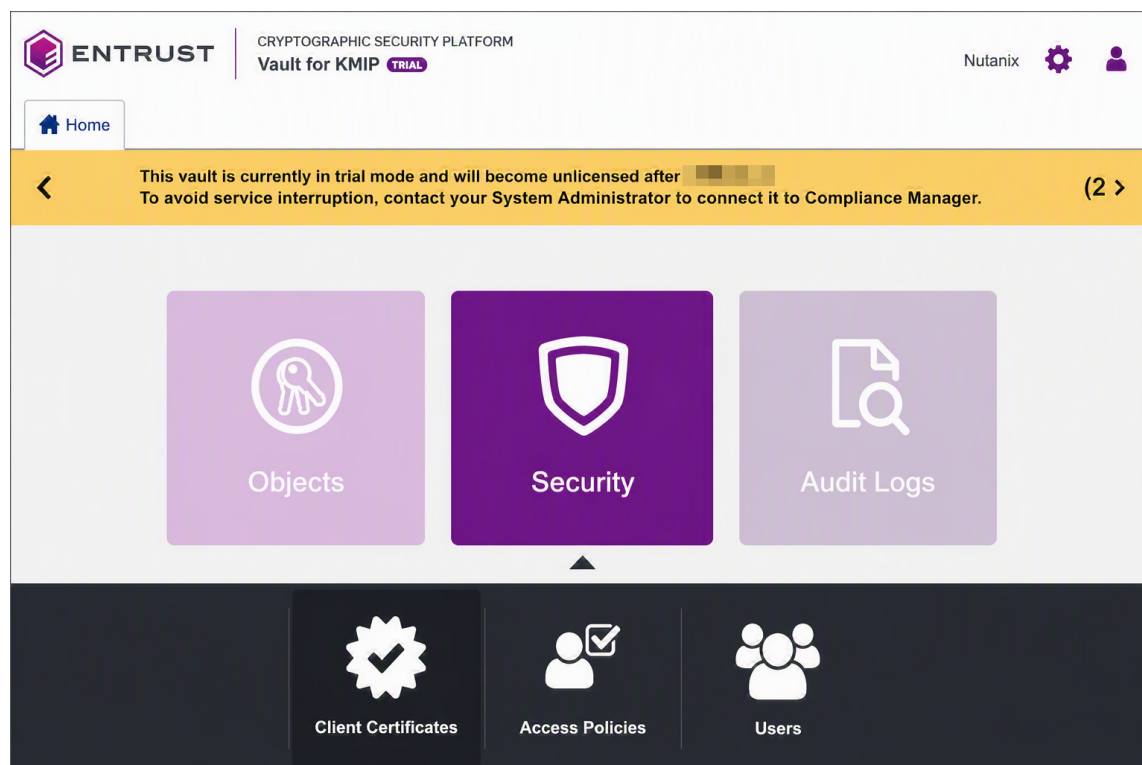
```
Directory: C:\Users\RNO-NXRDY005-User08\Downloads\csrs
```

Mode	LastWriteTime	Length	Name
-a---	7/8/2026 10:32 AM	1813	10.8.60.29_13caa80d-8f2b-4177-a4dc-7d8b0945837e_csr_x509.txt
-a---	7/8/2026 10:32 AM	1813	10.8.60.30_8db05d92-3dcf-4874-ab93-93a8df853d2d_csr_x509.txt
-a---	7/8/2026 10:32 AM	1813	10.8.60.31_ea8dee92-fdff-4720-ba3e-e4c78d8e501d_csr_x509.txt

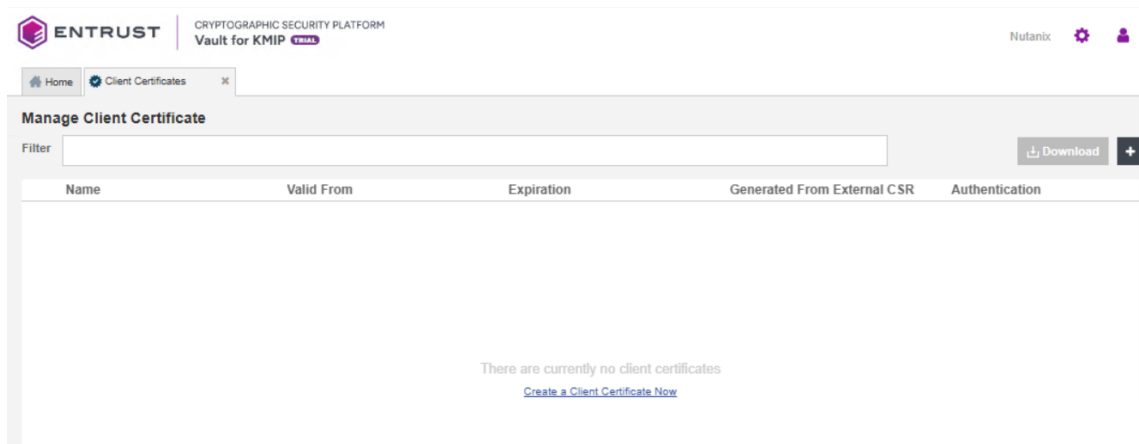
9. Change the file extension of the above certificates from **.txt** to **.csr**.

3.2. Create the KMIP client certificate bundles

1. Log in to the Entrust Key Management Vault created in [Install and configure Entrust Cryptographic Security Platform Key Management Vault](#).
2. Select the **Security** icon, and then the **Client Certificates** icon.



3. Select **Create a Client Certificate Now**.



4. In the **Create Client Certificate** dialog:

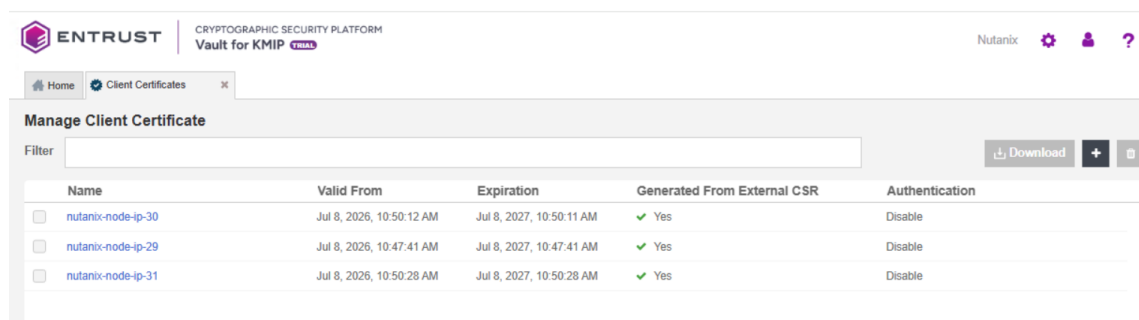
- a. Enter the **Certificate Name**. Choose a name unique to a given node in the Nutanix cluster, for example, the last octet of the node's IP address.
- b. For the **Certificate Signing Request (CSR)**, select **Browse** and choose the certificate request corresponding to the given node.



Change the file extension of these certificates from **.txt** to **.csr** if not done before.

- c. Select **Create**.

5. Create certificates for the other nodes.



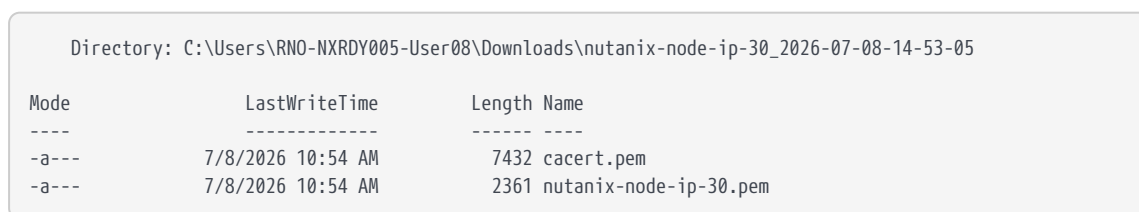
6. Select the required certificate and then select **Download**.

The download file name is in the following format:

<certificatename_datetimestamp>.zip.

7. Unzip the file.

It contains a user certificate/key file called **certificatename.pem** and a server certificate file called **cacert.pem**.



8. Repeat the step above for the other certificates.

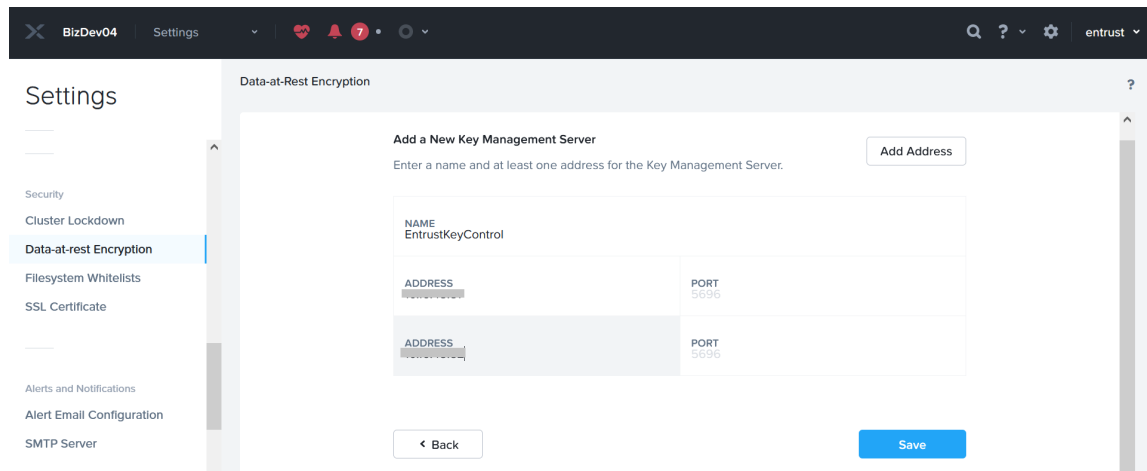


The **cacert.pem** files are identical across all nodes. The **certificatename.pem** files are unique to each node.

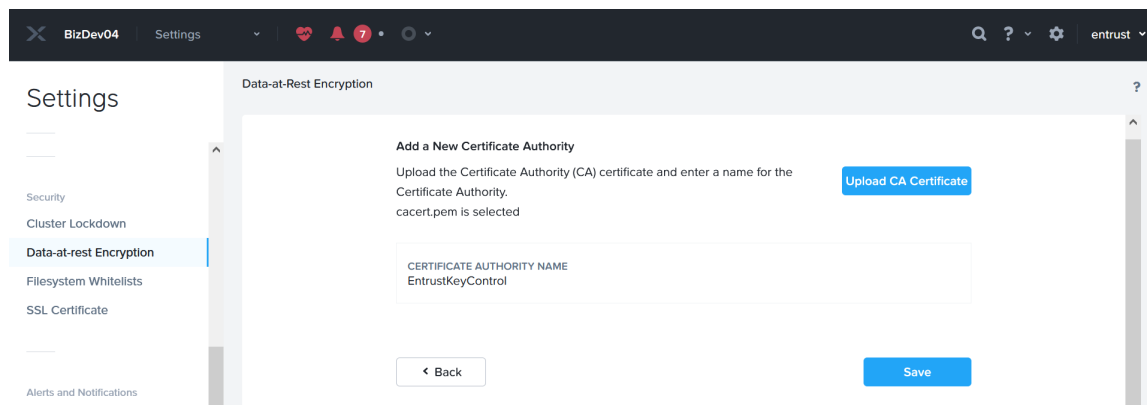
3.3. Add the Entrust Key Management Vault KMIP cluster to the Nutanix AHV cluster

1. Log in to the Nutanix Prism Element web UI.
2. In the toolbar, on the right-hand side, select the gear icon to display the **Settings** menu.
3. Select **Data-at-rest Encryption** under **Security** on the **Settings** left pane.
4. Select **Continue Configuration**, then scroll down and select **Add New Key Management Server**.
5. Enter a name for the Entrust Key Management Vault cluster and the IP addresses of all the nodes in the cluster, and then select **Save**.

The default port is 5696.



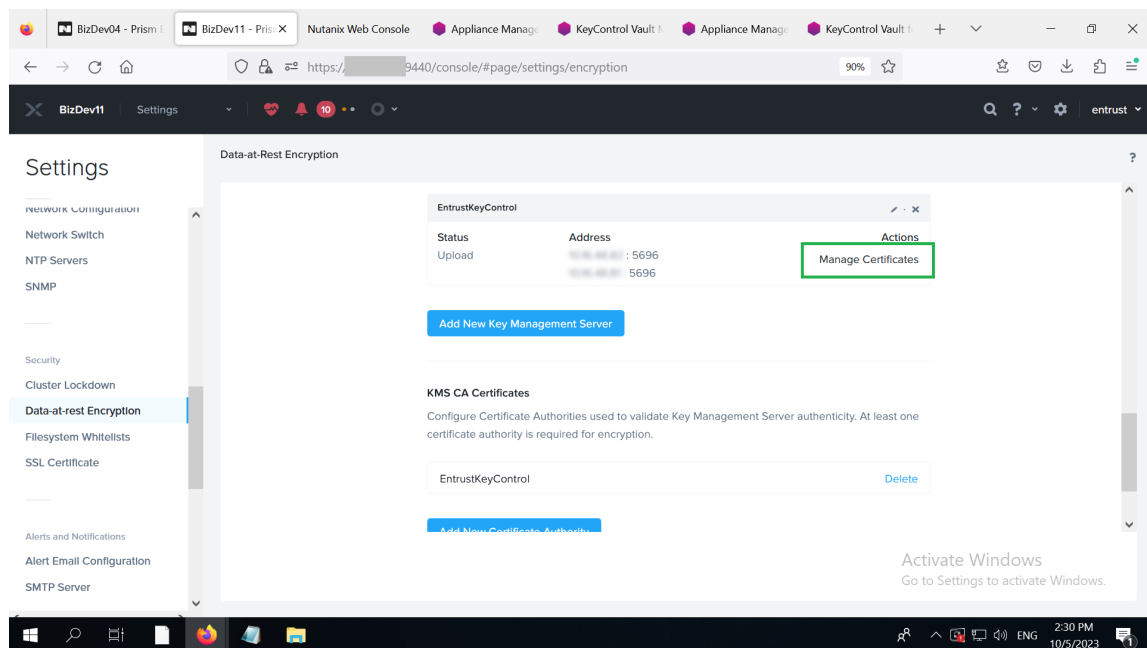
6. Select **Add New Certificate Authority** further down. Name the CA, then select **Upload CA Certificate**, and choose one of the **cacert.pem** files created above. All **cacert.pem** files are identical.



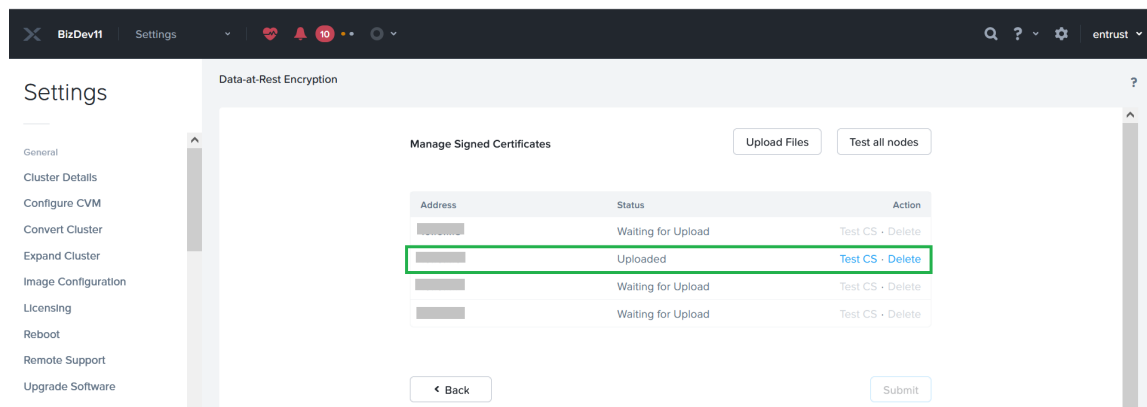
7. Select **Save**.

3.4. Add the Entrust KeyControl KMIP cluster certificates to the Nutanix AHV cluster

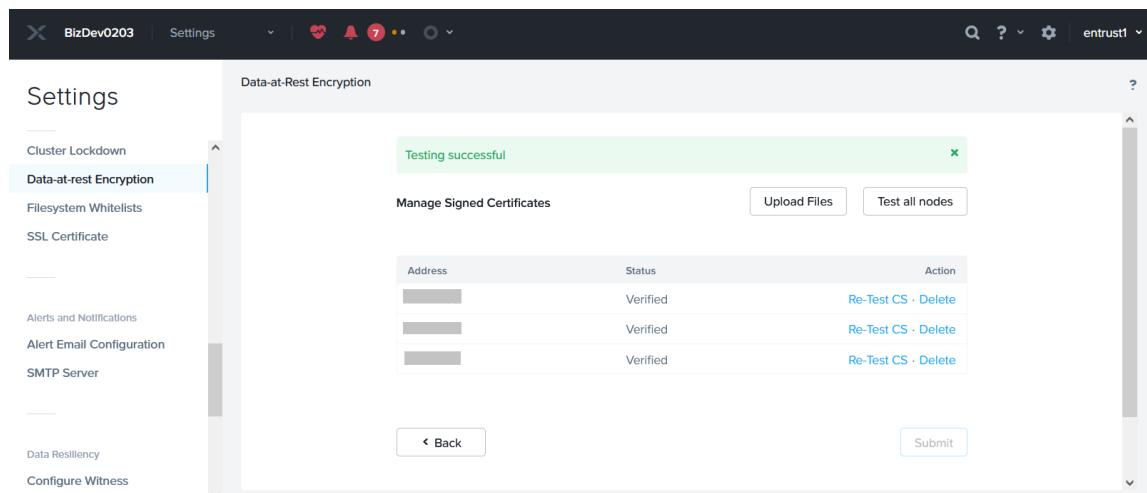
1. Log in to the Nutanix Prism Element web UI.
2. Select the **Settings** icon to the right of the toolbar to bring up the **Settings** menu.
3. Select **Data-at-rest Encryption** under **Security** on the **Settings** left pane.
4. Select **Continue Configuration**, then scroll down to the **Key Management Server** section.
5. Select the **Manage Certificates** hyperlink of the **EntrustKeyControl** cluster. This hyperlink is below **Actions**.



6. Select **Upload Files**, choose the relevant **certificatename.pem** file, then select **Submit**.
7. The status for the node corresponding to the selected certificate displays **Uploaded**. Select **Test CS** and the status changes to **Verified**.



8. Repeat the above for the other nodes.



3.5. Enable encryption

1. Log in to the Nutanix Prism Element web UI.
2. Select the **Settings** icon to the right of the toolbar to bring up the **Settings** menu.
3. Select **Data-at-rest Encryption** under **Security** on the **Settings** left pane.
4. Select **Enable Encryption**.
5. Enter the word **ENCRYPT** to confirm encryption in the pop-up window.
6. Select **Encrypt**.

Confirm Encryption

✕

All data on the cluster will be securely encrypted. Type ENCRYPT to confirm cluster encryption.

ENCRYPT

Cancel

Encrypt

The display confirms that the cluster is now encrypted.

Chapter 4. Integrating with an HSM

For guidance on integrating the Entrust Key Management Vault with a Hardware Security Module (HSM), consult your HSM vendor. If you are using an Entrust nShield HSM, refer to the [Entrust Cryptographic Security Platform Key Management Vault: nShield® HSM Integration Guide](#).

Chapter 5. Additional resources and related products

5.1. nShield as a Service

5.2. Entrust CSP Key Manager

5.3. Entrust products

5.4. nShield product documentation