Nutanix and Entrust KeyControl

Integration Guide

2025-04-02

Table of Contents

Chapter 1. Introduction

This document describes the integration of Nutanix AHV cluster with the Entrust KeyControl Key Management Solution (KMS). Entrust KeyControl serves as a KMS in Nutanix AHV cluster using the open standard Key Management Interoperability Protocol (KMIP).

1.1. Product configurations

The following versions have been tested for compatibility:

Product	Version
Nutanix AOS	v6.10 and v7.0
Entrust KeyControl	v10.4.3

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

Support for 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

Supported Nutanix Feature	Support
Re-Keying	Yes

1.3. Requirements

To integrate the Entrust KeyControl and the Nutanix AHV cluster you require:

- Access to the Entrust TrustedCare Portal.
- Access to the Nutanix online services and portals.

Familiarize yourself with:

- The Entrust Product Documentation.
- The Entrust DataControl and KeyControl Online Documentation Set.

Chapter 2. Install and configure Entrust KeyControl

A two-node cluster was deployed for this integration. KeyControl can be deployed on AHV using the ISO image. The ISO image is available at Software Downloads. Installation instructions are available at ISO Installation.

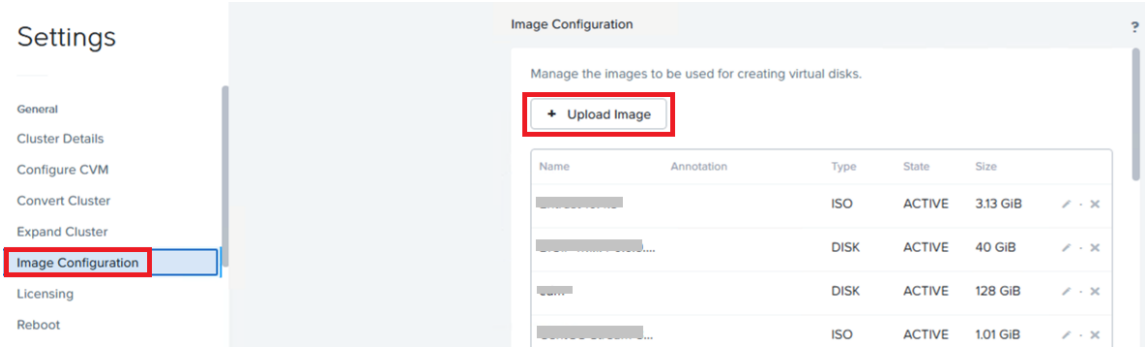
- Upload the KeyControl ISO in AHV
- Deploy an KeyControl node on AHV
- Join the two KeyControl nodes to form a cluster.
- Create a KeyControl vault

2.1. Upload the KeyControl ISO in AHV

For reference see the following Nutanix online documentation:

- Adding an Image.
- Configuring Images.

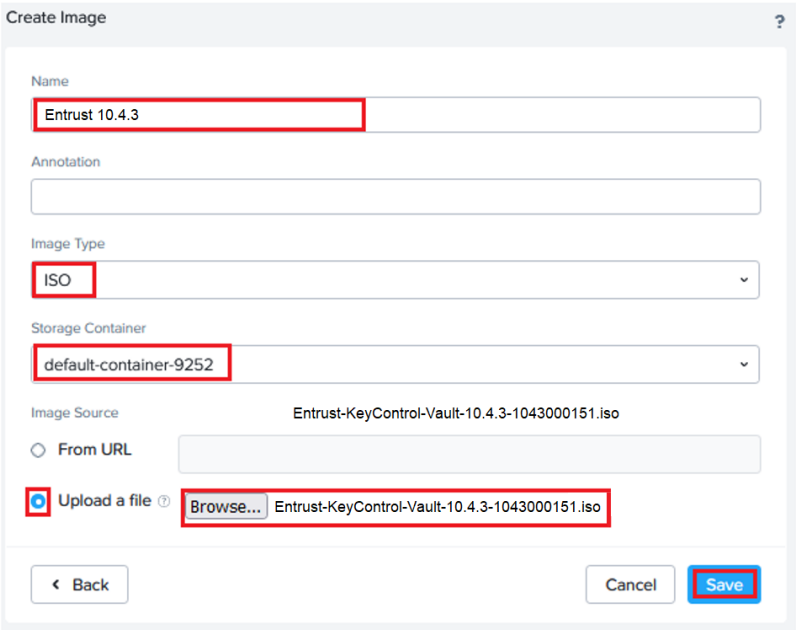
1. Log into the Nutanix Prism Element web UI.
2. Select the **Settings** control on the top tool bar.
3. In the left menu, select **Image Configuration**.



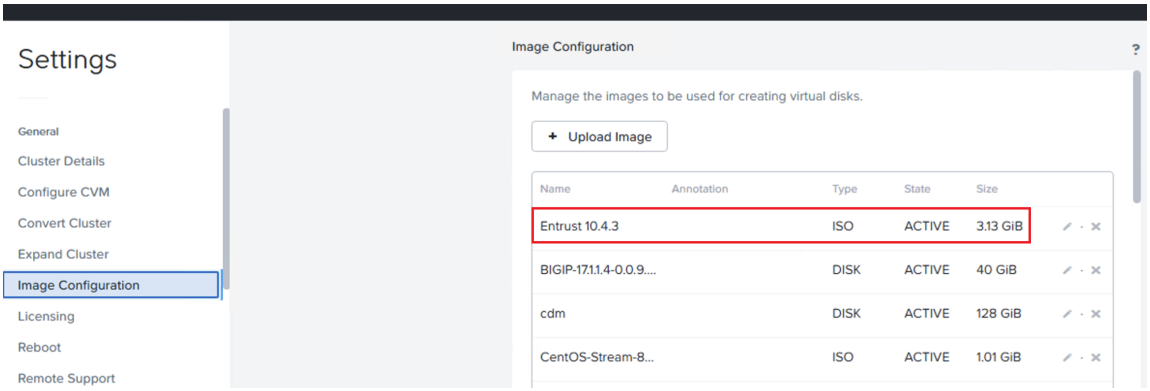
4. Select **Upload Image**.
5. In the **Create Image** window, enter the following: Then select **Save**.

Parameter	Value
Name	Enter a unique name.
Image Type	ISO

Parameter	Value
Storage Container	Select the required container.
Upload a file	Browse to the ISO file and select it.



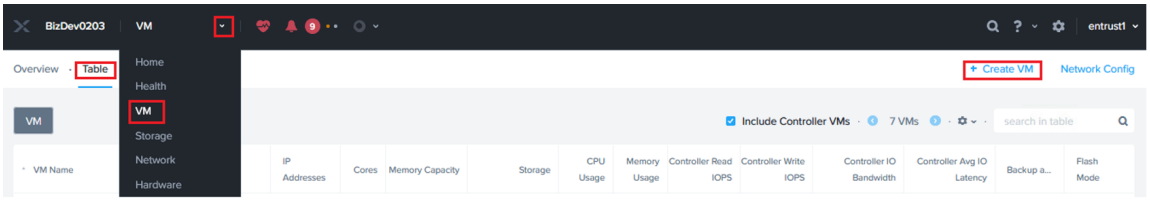
6. In the **Image Configuration** window, confirm that the image is **ACTIVE**.



2.2. Deploy an KeyControl node on AHV

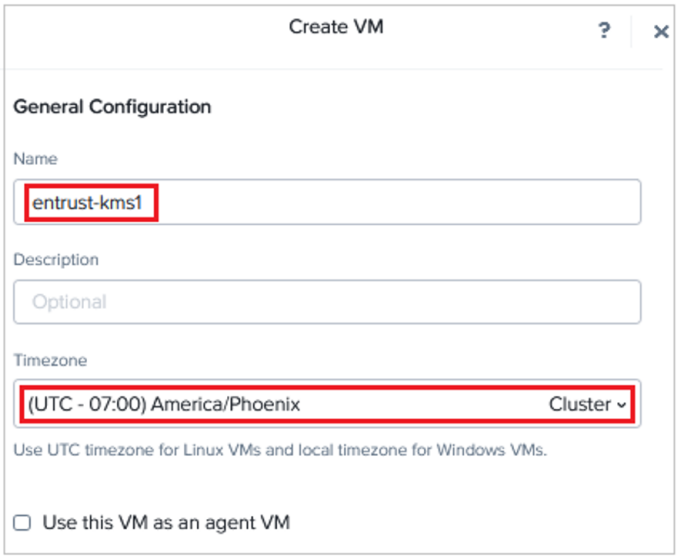
For reference see VM Management in the Nutanix online documentation.

1. Log in to the Nutanix Prism Element webUI.
2. Select **VM** from the pull-down menu on the top tool bar.



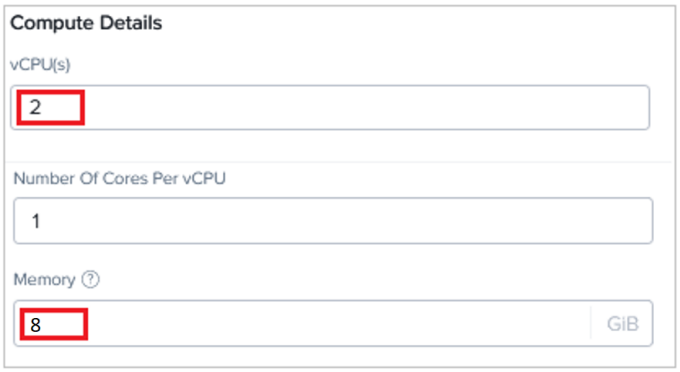
3. Select the **Table** tab.
4. Select **Create VM**.
5. In the **General Configuration** window, enter the following:

Parameter	Value
Name	Enter a unique name for the VM.
Timezone	Select your timezone.
Use this VM as an agent VM	Un-check



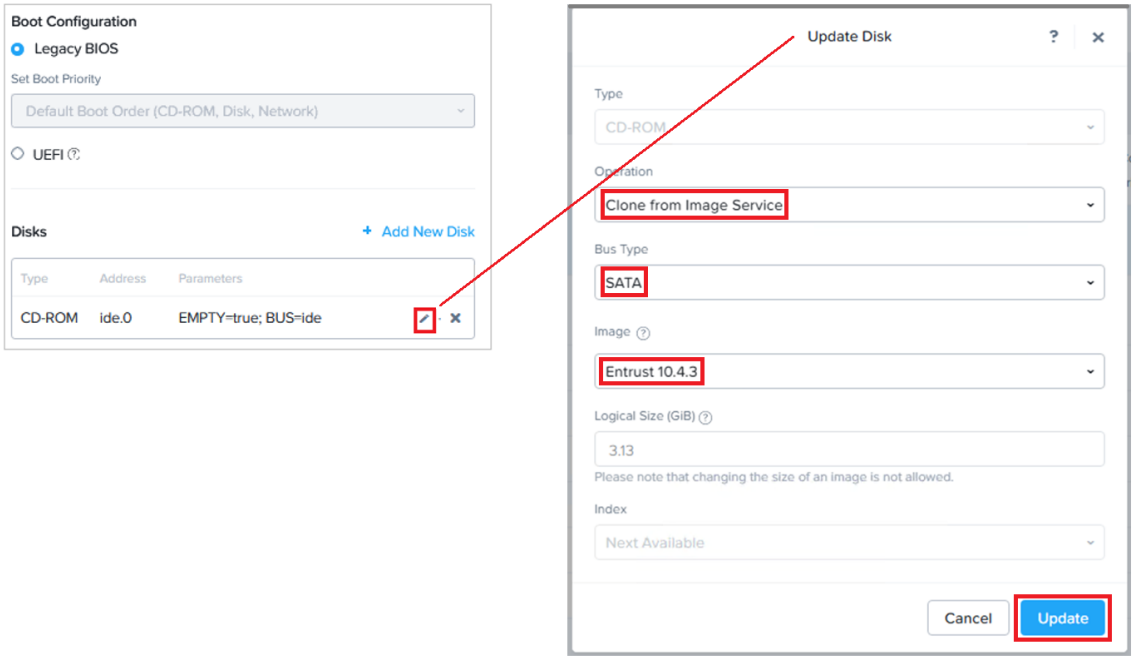
6. In the **Compute Details** window, enter the following:

Parameter	Value
vCPUs	2 (Number of cores per vCPU =1)
Memory	8



7. In the **Boot Configuration**, enter the following:
   - Select **Legacy BIOS**.
   - Under **Disks**, select the edit button for the **CD-ROM** entry.
8. In the **Update Disk** window, enter the following. Then select **Update**.

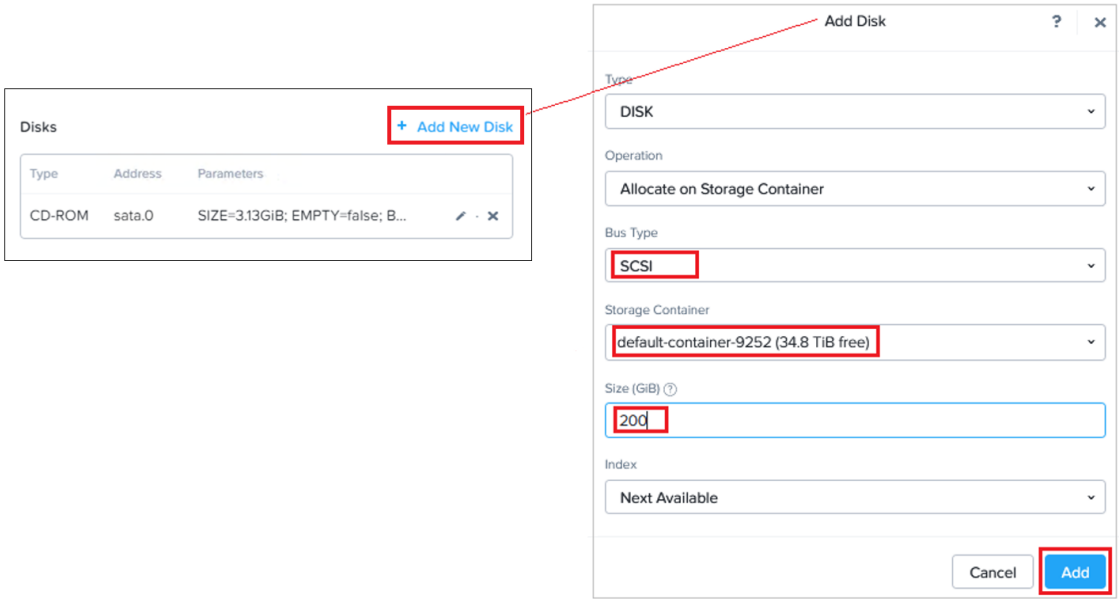
Parameter	Value
Operation	Clone from Image Service
Bus Type	SATA
Image	Enter the image file name.



9. Select **Add New Disk**.

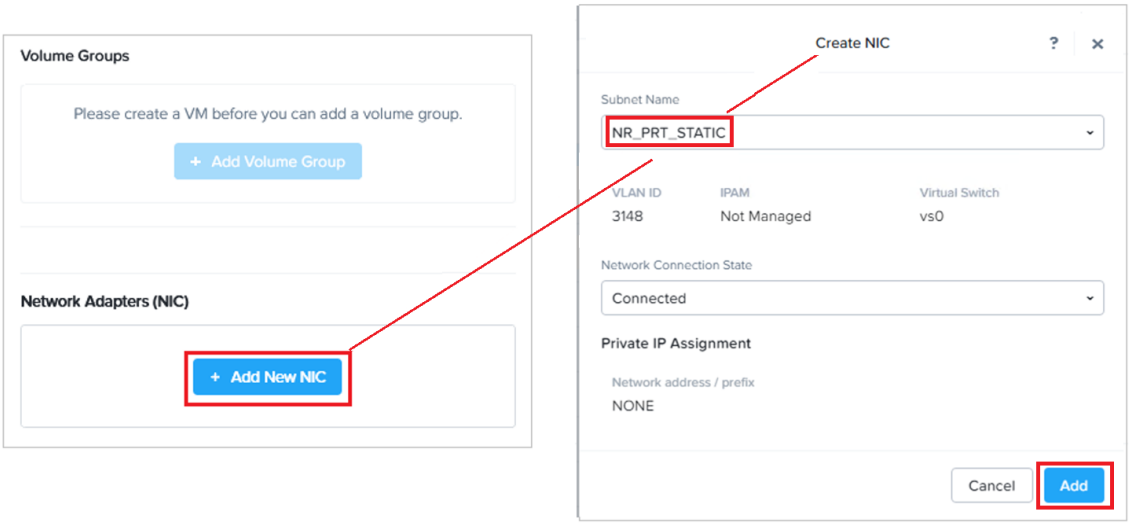
10. In the **Add Disk** window, enter the following. Then select **Add**.

Parameter	Value
Operation	Allocate on Storage Container
Bus Type	SCSI
Storage Container	Select the required service container.
Size	200
Index	Next Available

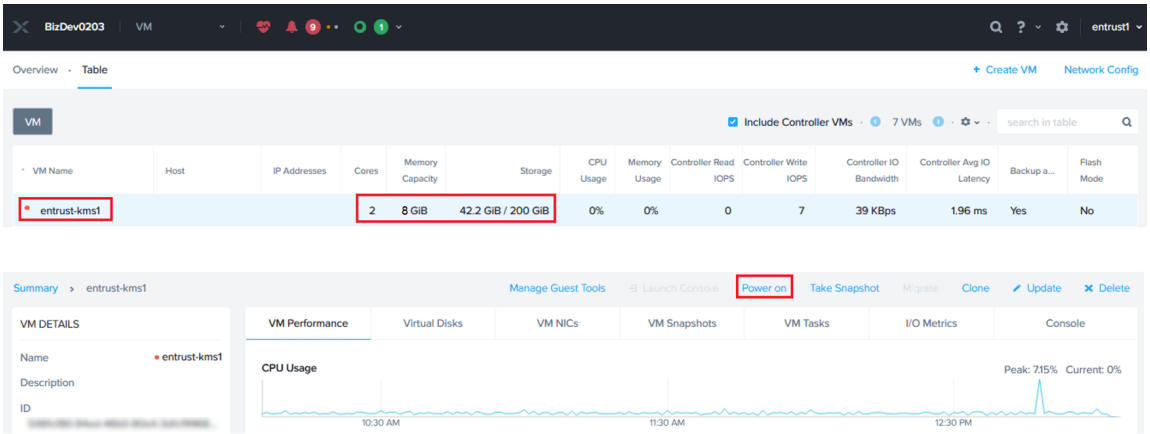


11. Under **Network Adapters (NIC)**, select **Add New NIC**.
12. In the **Create NIC** window, select your **Subnet Name**. Then select **Add**.

> Select a static network as DHCP network deployment is not supported.



13. At the bottom of the **Create VM** window, select **Save**.
14. On the **VM** page, confirm the VM was created.



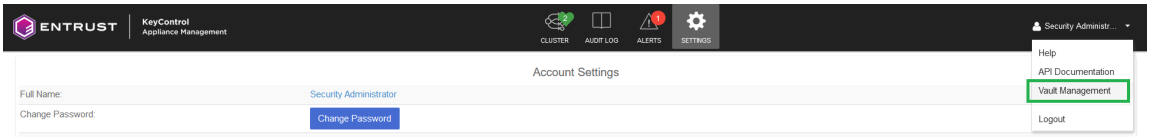
15. Select **Power on** to start the VM.
16. Repeat all steps to create a second Entrust KeyControl node.

2.3. Join the two KeyControl nodes to form a cluster.

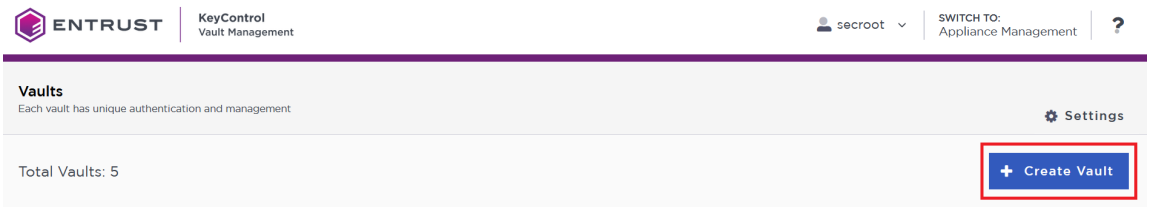
Join the two KeyControl nodes in a high availability cluster following the instructions in Installing a New KeyControl Vault Cluster Additional information can be found at Entrust Documentation (search for the **KeyControl**).

2.4. Create a KeyControl vault

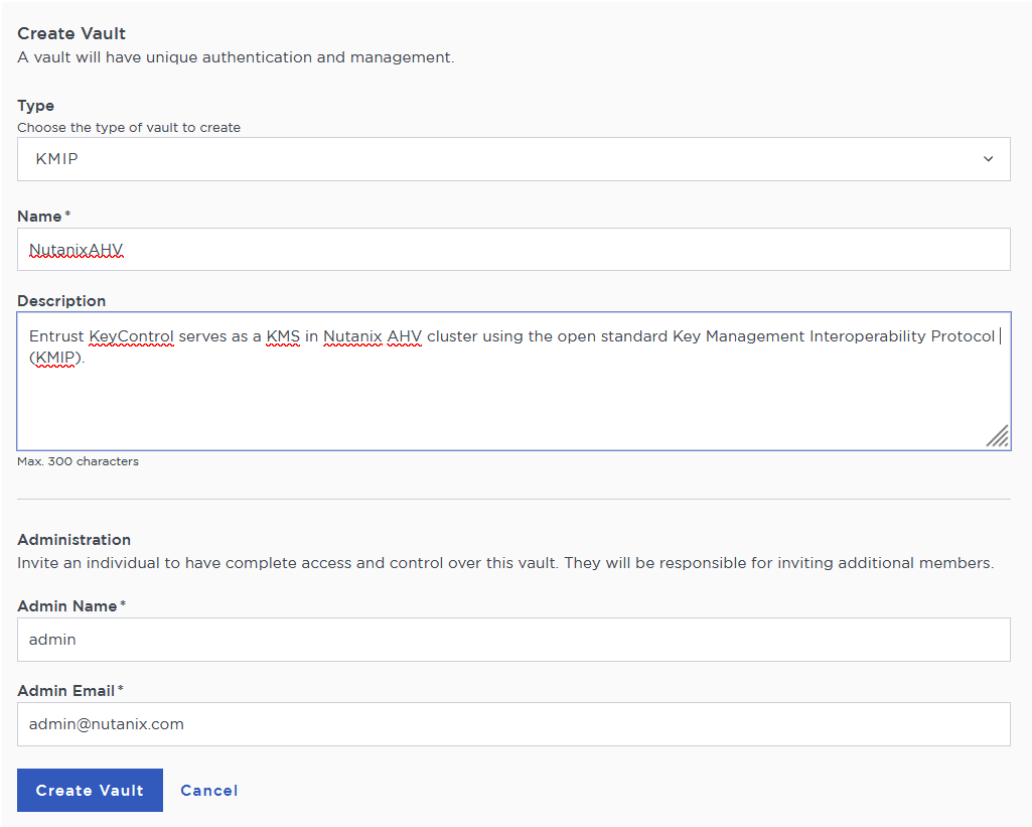
1. Sign in to the KeyControl Appliance Manager.
2. In the **Appliance Management** home page select **Vault Management**.



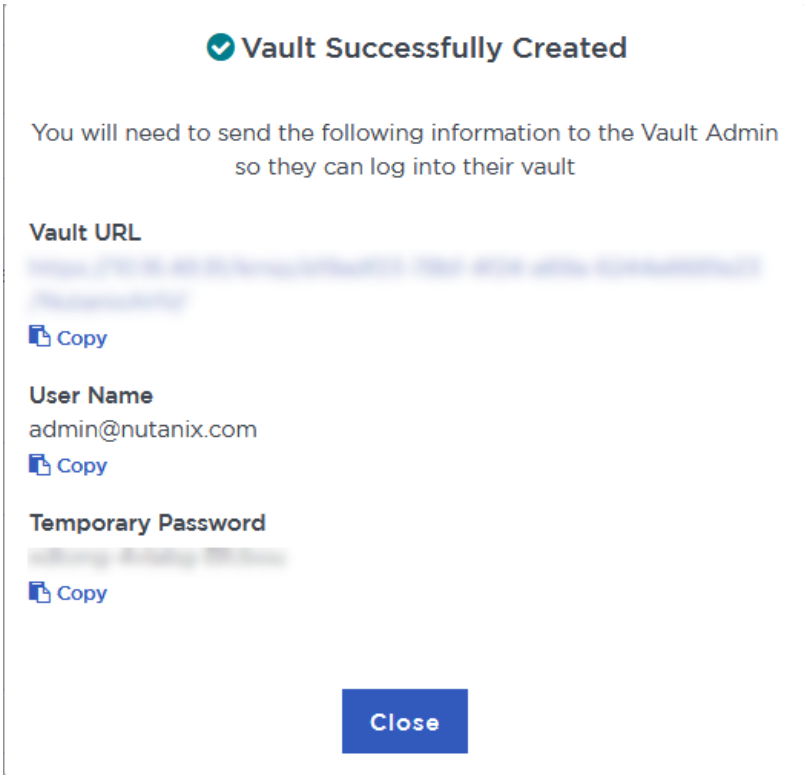
3. In the **Vault Management** home page, select **Create Vault**. The **Create Vault** dialog appears.



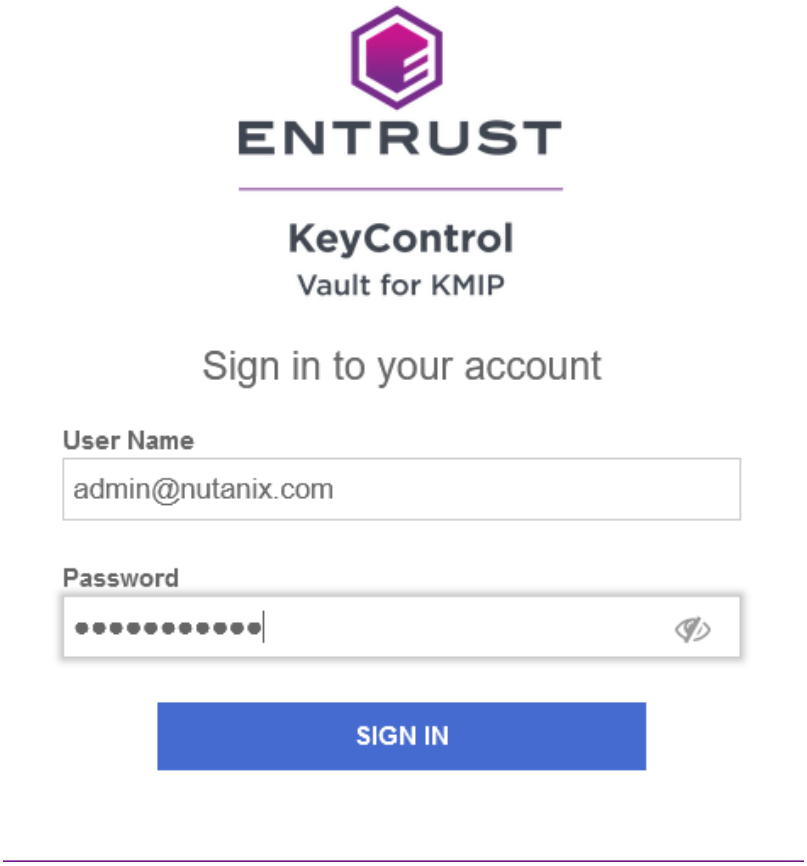
4. In the **Type** drop-down box, select **KMIP**. Enter the required information, then select **Create Vault**.



5. Bookmark the following URL and save the credentials. You will receive an email with the above information if the SMTP was set.



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



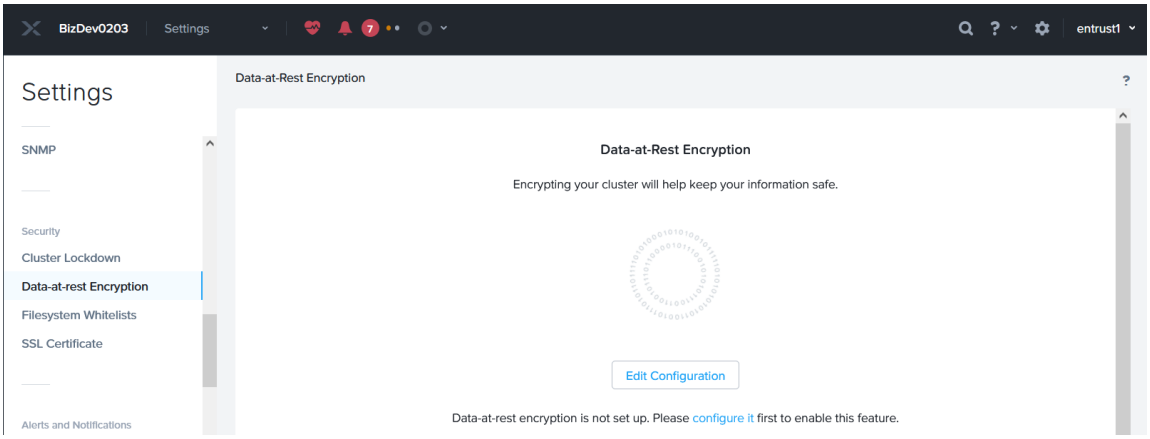
7. Notice the new vault.

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

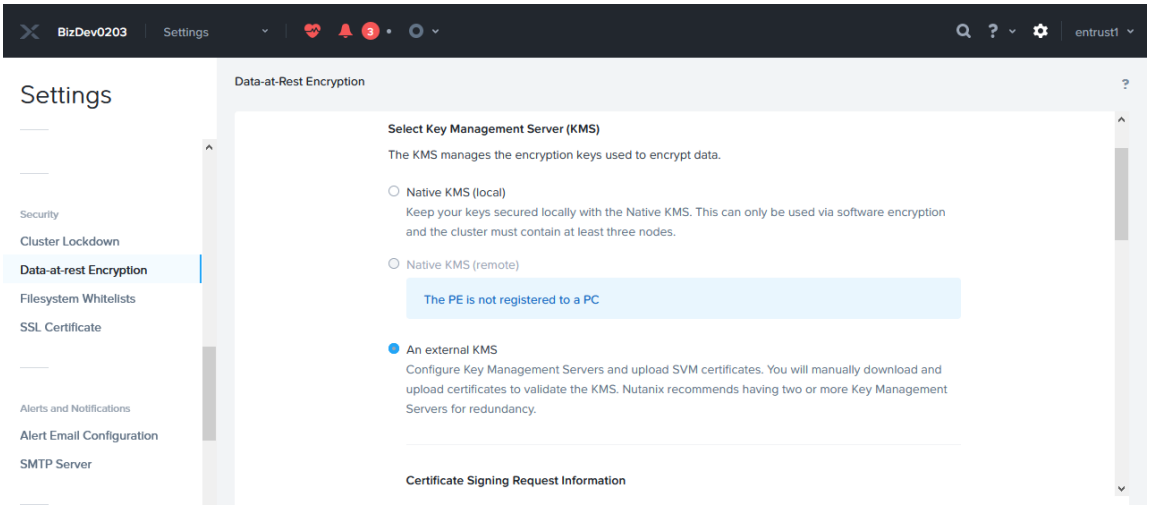
- Select KeyControl as the KMIP Server and generate the certificate requests
- Create the KMIP client certificate bundles
- Add the Entrust KeyControl KMIP cluster to the Nutanix AHV cluster
- Add the Entrust KeyControl KMIP cluster certificates to the Nutanix AHV cluster
- Enable encryption

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

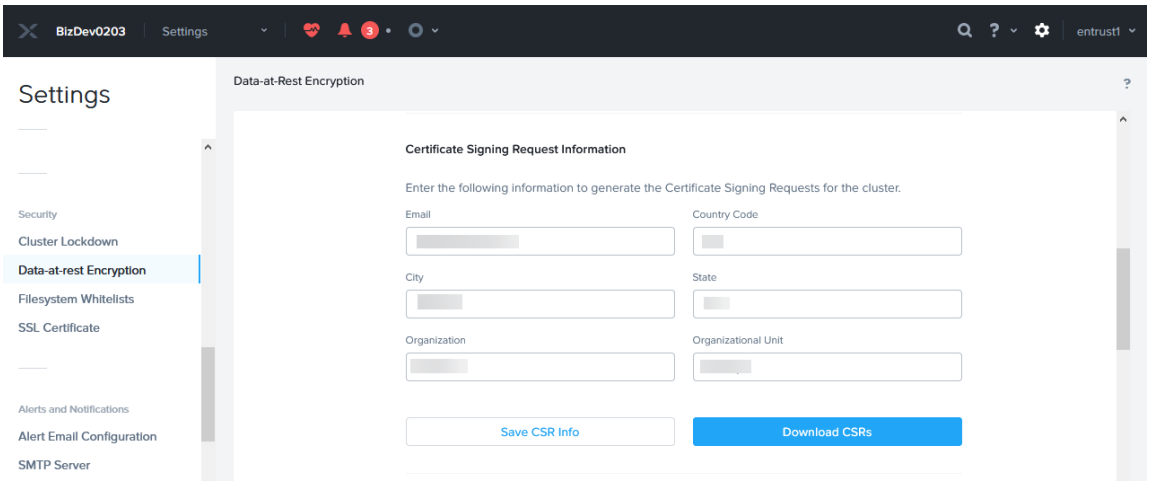
1. Log into the Nutanix Prism Element web UI.
2. Select the **Settings** pull-down menu in the toolbar, scroll down, and select **Settings** again. The **Gear** icon in the top right of the toolbar does the same operation.
3. Select **Data-at-rest Encryption** under **Security** on the **Settings** left pane. Then select **Edit Configuration** or **Continue Configuration**.



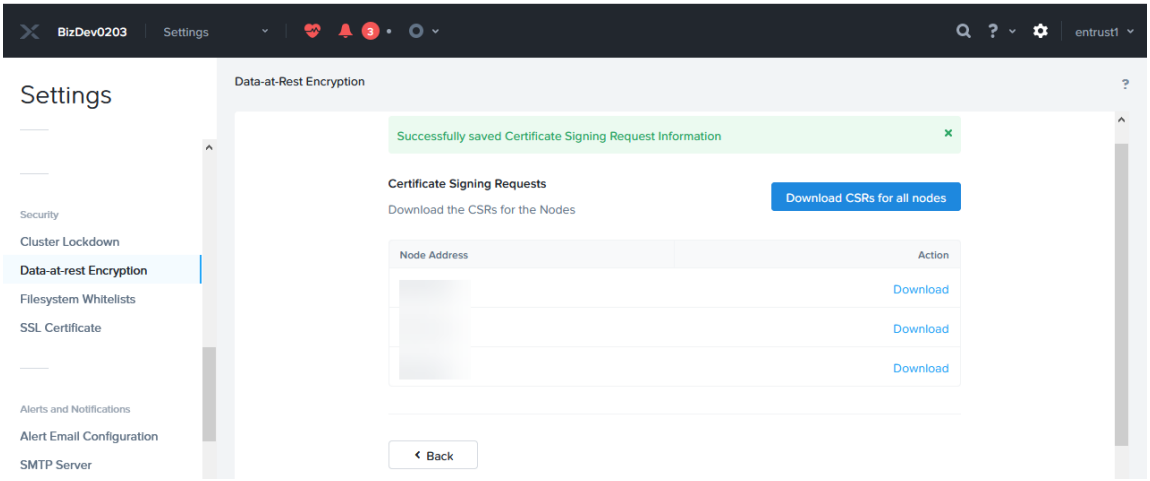
4. Select **An external KMS**.



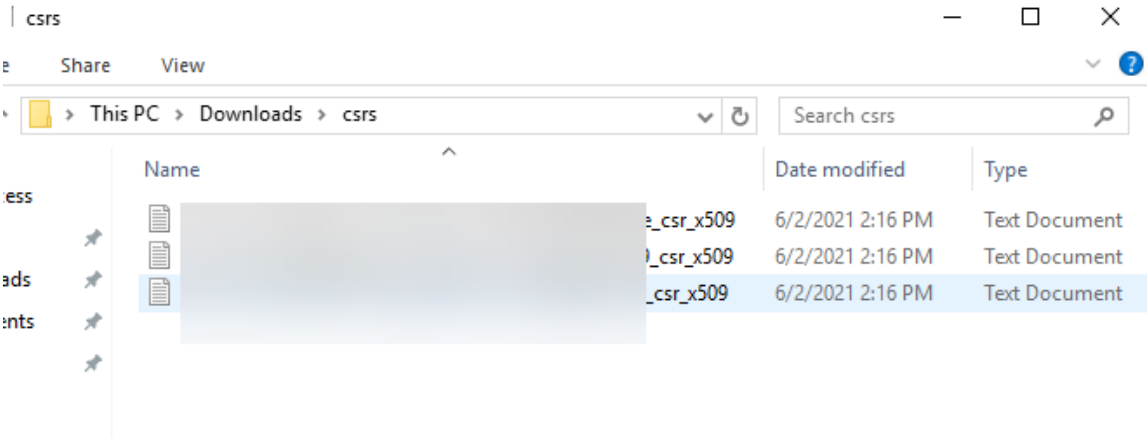
5. Scroll down to **Certificate Signing Request Information**. Fill the request form, then select **Save CSR Info**.



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



7. The compressed `csrs.zip` file is created. Save the file locally. Extract the files. Notice that a certificate request was created for each node in the Nutanix AHV cluster.

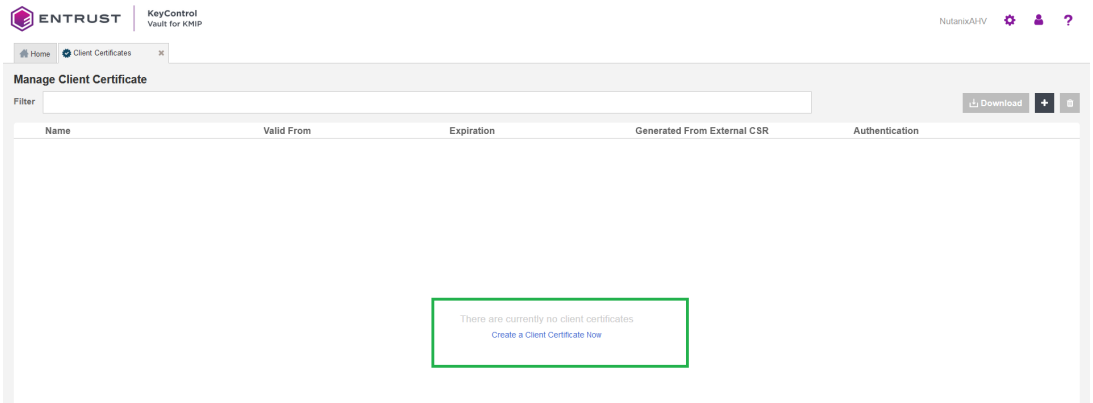


8. Change the file extension of the above certificates from `.txt` to `.csr`.

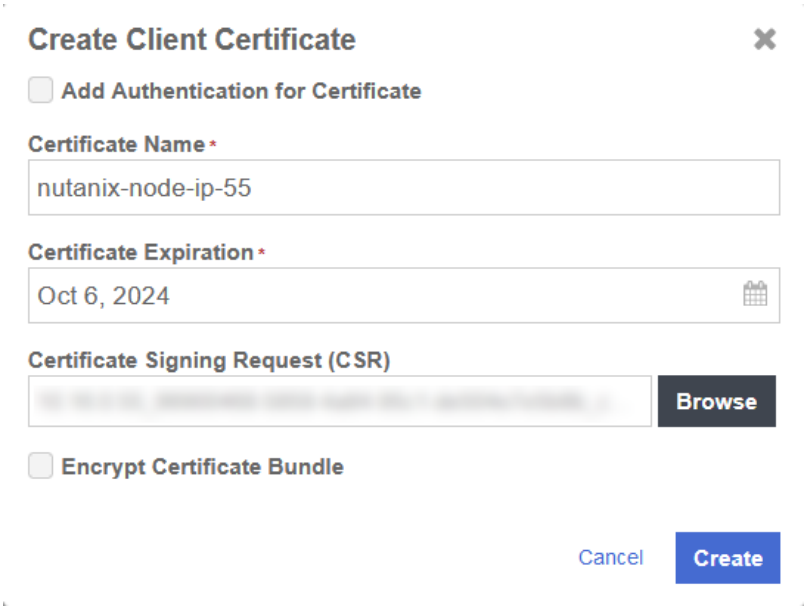
3.2. Create the KMIP client certificate bundles

1. Log into the Entrust KeyControl vault created in Install and configure Entrust KeyControl.
2. Select the **Security** icon, and then the **Client Certificates** icon.

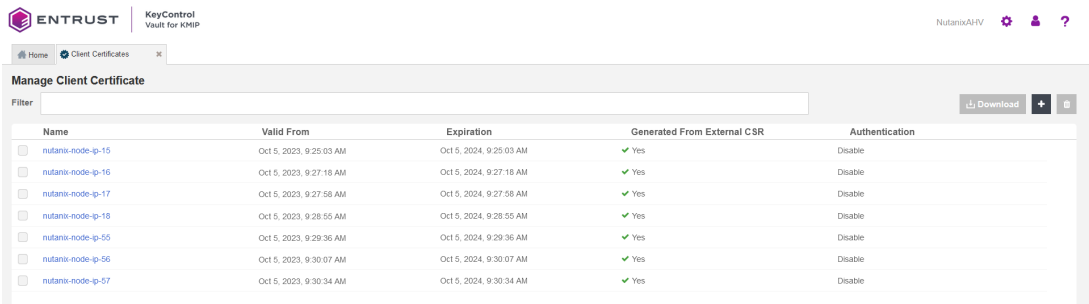
3. Select **Create a Client Certificate Now**.



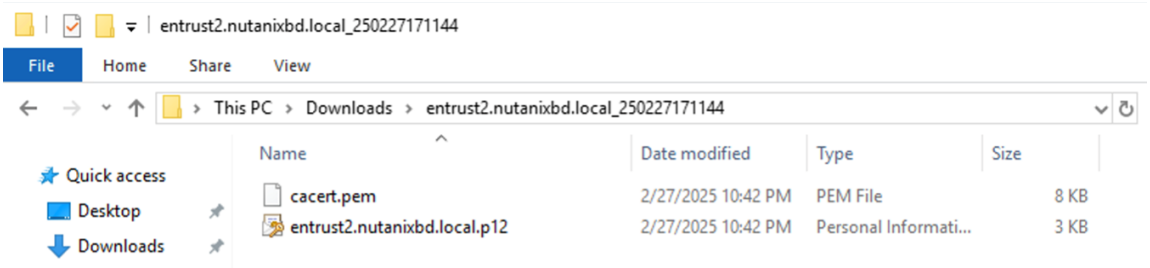
4. Enter the **Certificate Name** in the text box. Choose a name unique per a given node in the Nutanix cluster, for example the last octet of the node's IP address as part of the name.
5. Select **Load File** and choose the certificate request from section Select KeyControl as the KMIP Server and generate the certificate requests corresponding to the given node. Change the file extension of these certificates from `.txt` to `.csr` if not done before. You may need to allow **All** file types for them to show in the file manager window. Then select **Create**.



6. Create certificates for the other nodes.



7. Select one of the certificates created above. Then select **Download**.
8. Notice the download file name `<username_datetimestamp>.zip`. Unzip the file. It contains a user certification/key file called `username.pem` and a server certification file called `cacert.pem`.

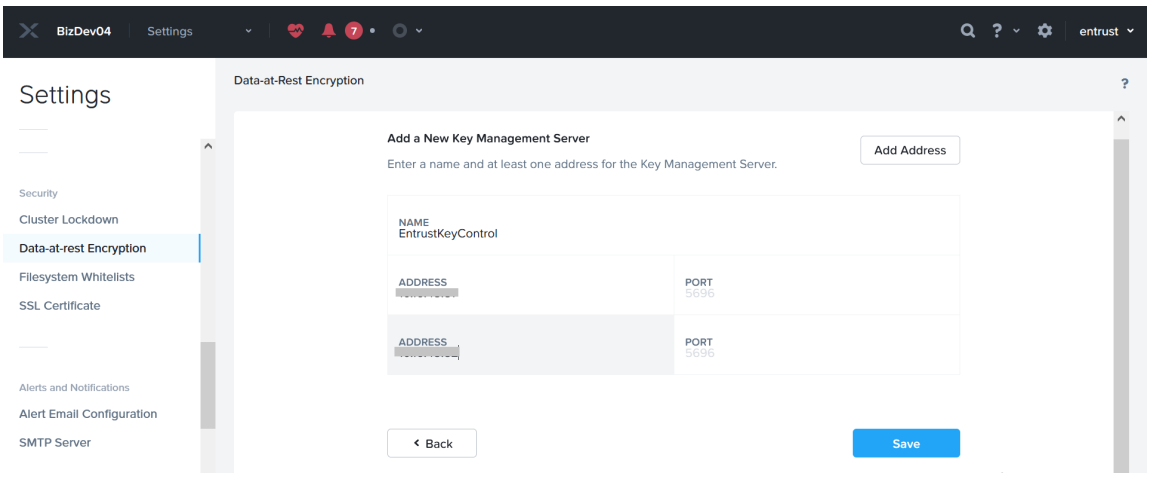


9. Repeat the step above for the other certificates.

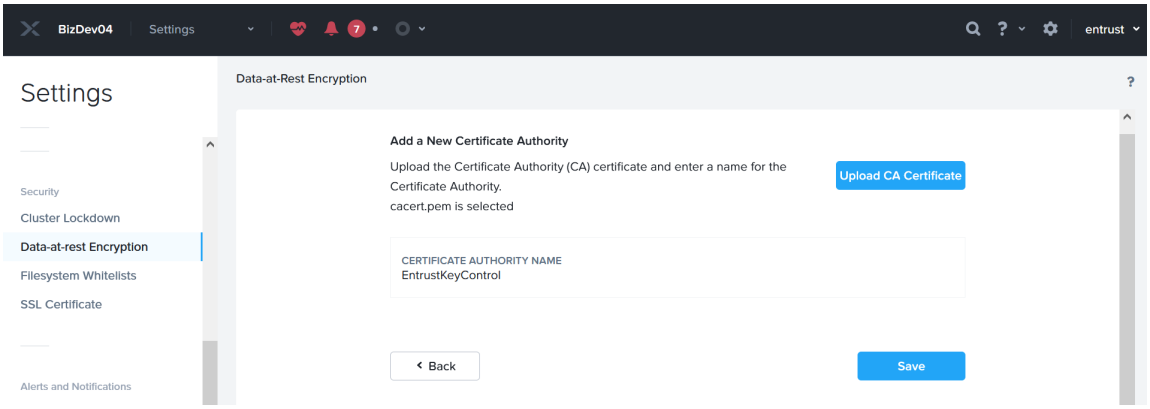
> The `cacert.pem` file for each node above are identical. The `username.pem` files are unique for each node.

3.3. Add the Entrust KeyControl KMIP cluster to the Nutanix AHV cluster

1. Log into 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 and select **Add New Key Management Server**.
5. Enter a name for the Entrust KeyControl cluster, and the IP address of all the nodes in the cluster. The default port is 5696. Then select **Save**.

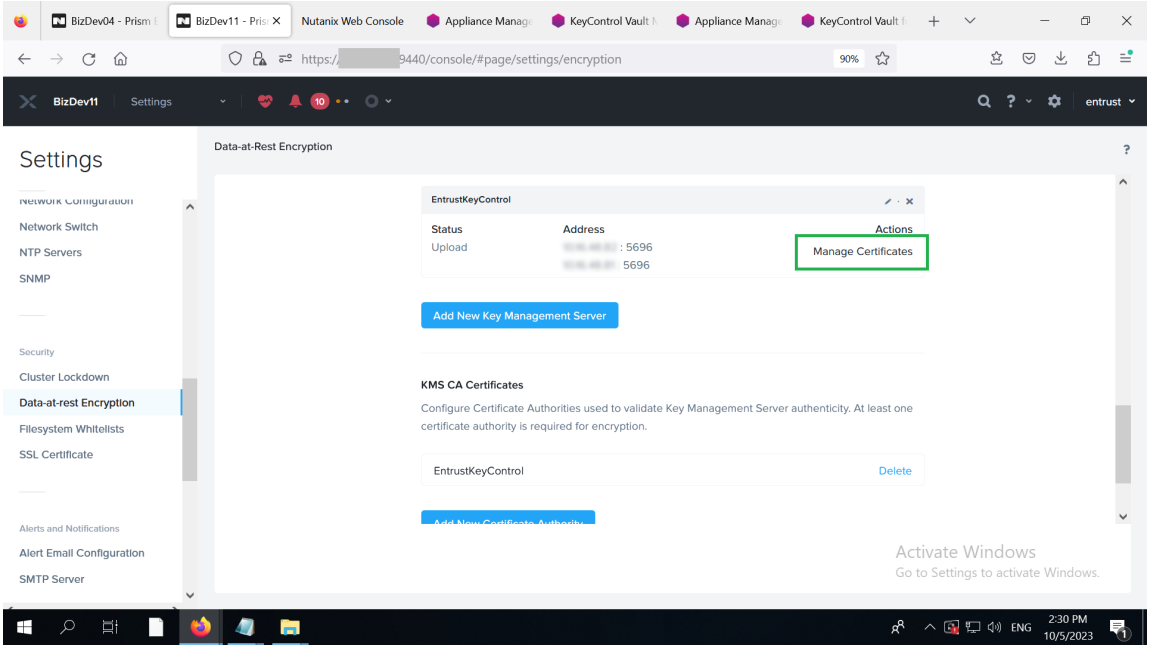


6. Select **Add New Certificate Authority** further down. Name the CA, then select **Upload CA Certificate**, and choose one of the `cacert.pem` files created above. All `cacert.pem` files are identical. Then select **Save**.

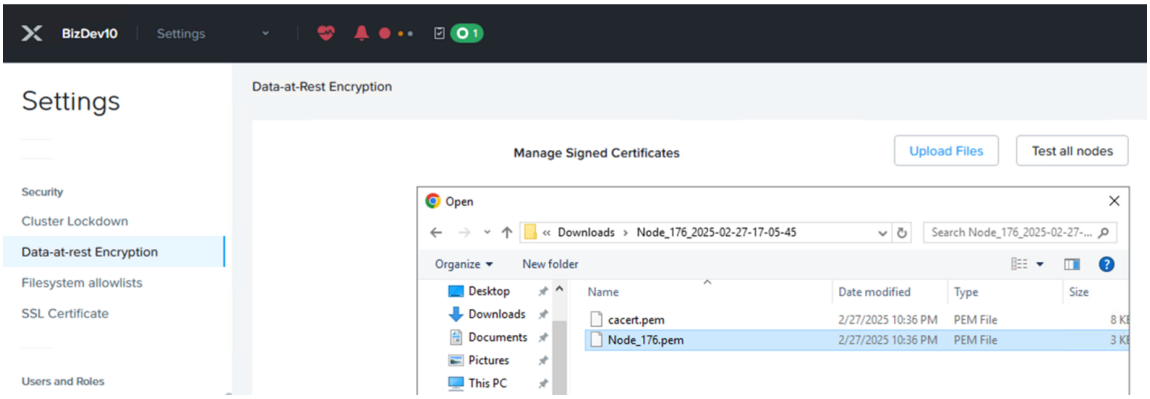


3.4. Add the Entrust KeyControl KMIP cluster certificates to the Nutanix AHV cluster

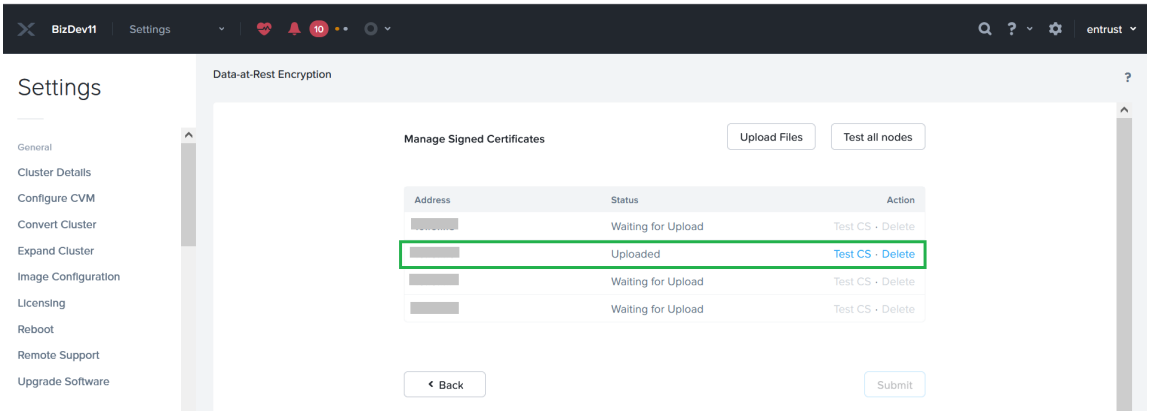
1. Log into the Nutanix Prism Element web UI.
2. Select the **Settings** icon to the right of the toolbar to bring up the **Settings** menu.
3. Select **Data-at-rest Encryption** under **Security** on the **Settings** left pane.
4. Select **Continue Configuration**. Then scroll down to the **Key Management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



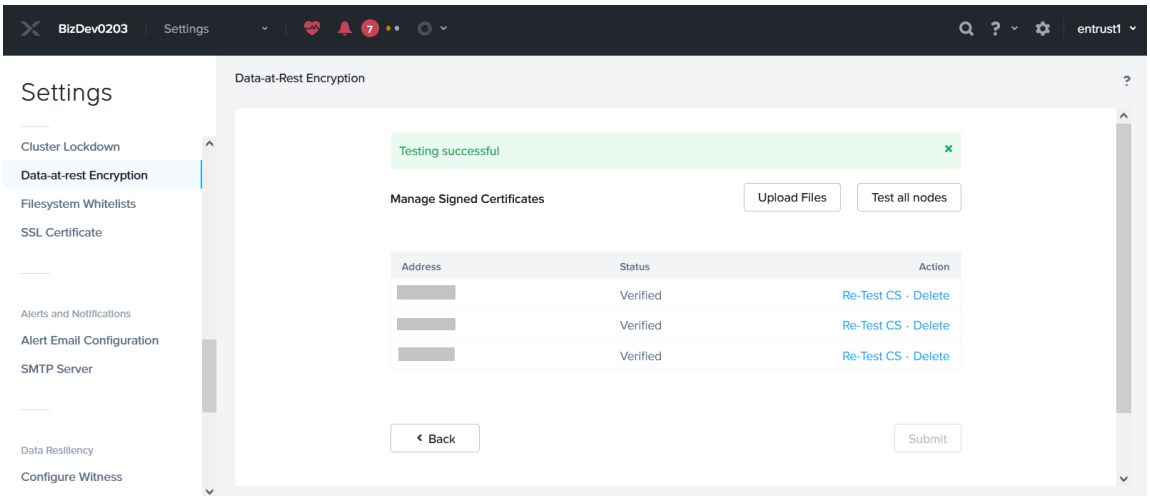
6. Select **Upload Files**, and choose a `username.pem` created above, then select **Submit**.



7. Notice the status for the node corresponding to the selected certificate displaying **Uploaded**. Select **Test CS** and the status changes to **Verified**.



8. Repeat the above for the other nodes.

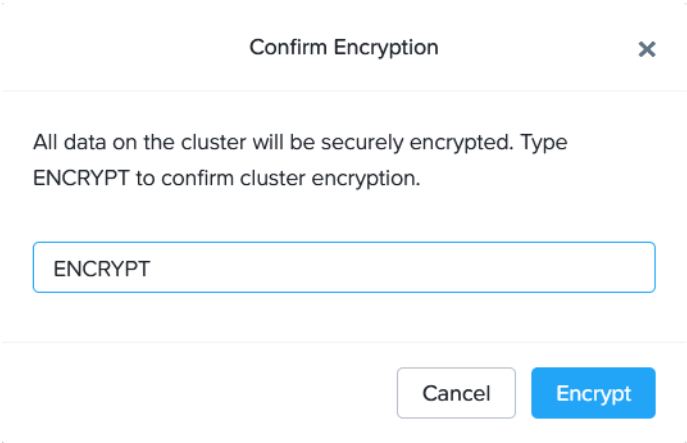


3.5. Enable encryption

1. Log into 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. Then select **Encrypt**.



The display confirms that the cluster is now encrypted.

Chapter 4. Integrating with an HSM

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

Chapter 5. Additional resources and related products

5.1. nShield Connect

5.2. nShield as a Service

5.3. KeyControl

5.4. Entrust products

5.5. nShield product documentation