



Nutanix and Entrust KeyControl

Integration Guide

2025-02-20

Table of Contents

1. Introduction	1
1.1. Documents to read first	1
1.2. Product configurations	1
1.3. Supported features	1
1.4. Requirements	2
2. Install and configure Entrust KeyControl	3
2.1. Upload the KeyControl ISO in AHV	3
2.2. Deploy an KeyControl node on AHV	4
2.3. Join the two KeyControl nodes to form a cluster	7
2.4. Create an KeyControl vault	7
3. Test the integration by enabling data-at-rest encryption	10
3.1. Select KeyControl as the KMIP Server and generate the certificate requests	10
3.2. Create the KMIP client certificate bundles	11
3.3. Add the Entrust KeyControl KMIP cluster to the Nutanix AHV cluster	13
3.4. Add the Entrust KeyControl KMIP cluster certificates to the Nutanix AHV cluster	14
3.5. Enable encryption	16
4. Integrating with an HSM	18
5. Additional resources and related products	19
5.1. nShield Connect	19
5.2. nShield as a Service	19
5.3. KeyControl	19
5.4. Entrust products	19
5.5. nShield product documentation	19

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. Documents to read first

This guide describes how to configure the Entrust KeyControl server as a KMS in Nutanix AHV cluster.

To install and configure the Entrust KeyControl server as a KMIP server, see the [Entrust DataControl and KeyControl Online Documentation Set](#), located in the [Entrust Product Documentation](#).

For more information related to either product refer to [Entrust TrustedCare](#) and the [Nutanix online services and portals](#).

1.2. Product configurations

The following versions have been tested for compatibility:

Product	Version
Nutanix AOS	6.5.3.7+ AHV 20220304.242
Entrust KeyControl	v10.1.1

1.3. Supported features

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

Entrust KeyControl Feature	Support
Deployment in Nutanix AHV from ISO	Yes
Cluster Mode	Yes
Cluster Expansion	Yes

Entrust KeyControl Feature	Support
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
Re-Keying	Yes

1.4. Requirements

Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

Chapter 2. Install and configure Entrust KeyControl

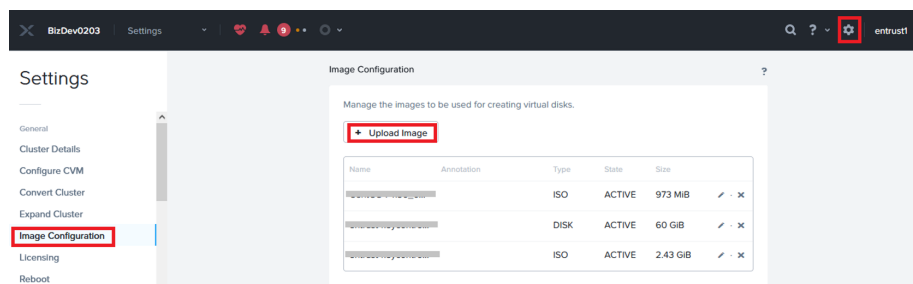
A two-node cluster was deployed for this integration.

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](#)

2.1. Upload the KeyControl ISO in AHV

For reference, see [Create a VM](#) in the Nutanix online documentation.

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. Enter **Create Image** information:
 - For **Name**, enter a unique name. For example, **ISO-Entrust-KeyControl-10.1.1**.
 - For **Image Type**, select **ISO**.
 - For **Storage Container**, select the required container.
 - Select **Upload a file**, browse to the ISO file and select it for use.

Create Image

Name:

Annotation:

Image Type:

Storage Container:

Image Source:

☐ From URL

☒ Upload a file

6. Select **Save**.

7. On the **Image Configuration** page, confirm that the image is **ACTIVE**.

Image Configuration

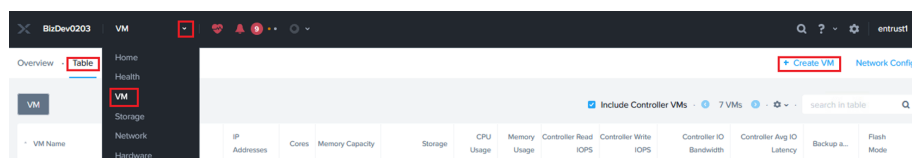
Manage the images to be used for creating virtual disks.

Name	Annotation	Type	State	Size
		ISO	ACTIVE	973 MiB
		DISK	ACTIVE	60 GiB
entrust-keycontro...		ISO	ACTIVE	2.43 GiB

For reference, see [Configuring Images](#) in the Nutanix online documentation.

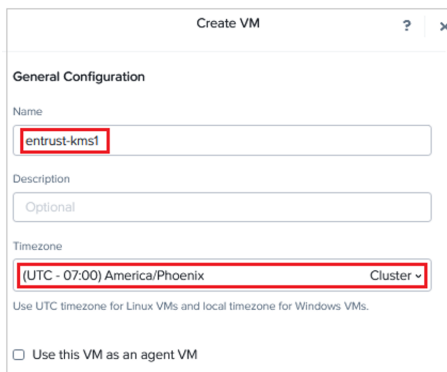
2.2. Deploy an KeyControl node on AHV

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. Under **General Configuration** information:
 - For **Name**, enter a unique name for the VM.
 - For **Timezone**, select your timezone.

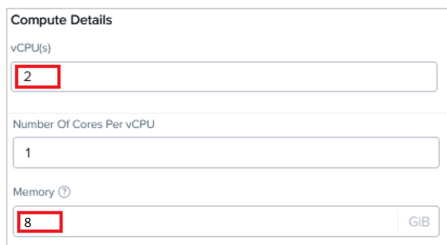
- Clear **Use this VM as an agent VM**.



The screenshot shows the 'Create VM' dialog box with the 'General Configuration' tab selected. The 'Name' field contains 'entrust-kms1'. The 'Description' field is empty. The 'Timezone' dropdown is set to '(UTC - 07:00) America/Phoenix'. Below the dropdown, there is a note: 'Use UTC timezone for Linux VMs and local timezone for Windows VMs.' At the bottom, there is a checkbox labeled 'Use this VM as an agent VM' which is currently unchecked.

6. Under **Compute Details** information:

- For **vCPUs**, enter **2**.
- For **Memory**, select **8**.



The screenshot shows the 'Compute Details' dialog box. The 'vCPU(s)' field is set to '2'. The 'Number Of Cores Per vCPU' field is set to '1'. The 'Memory' field is set to '8' GiB.

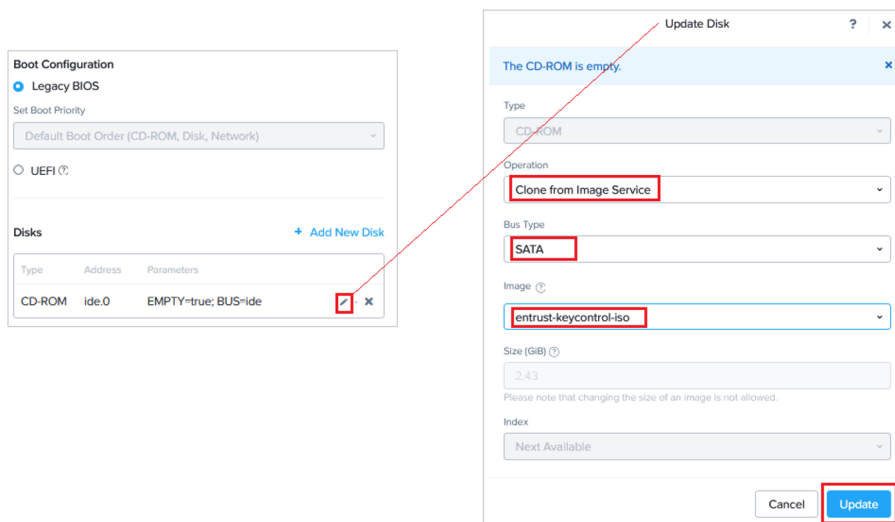
7. Under **Boot Configuration** information:

- Select **Legacy BIOS**.
- Under **Disks**, select the edit button for the **CD-ROM** entry.

8. In the **Update Disk** dialog:

- For **Operation**, select **Clone from Image Service**.
- For **Bus Type**, select **SATA**.
- For **Image**, enter the ISO file name.

9. Select **Update**.

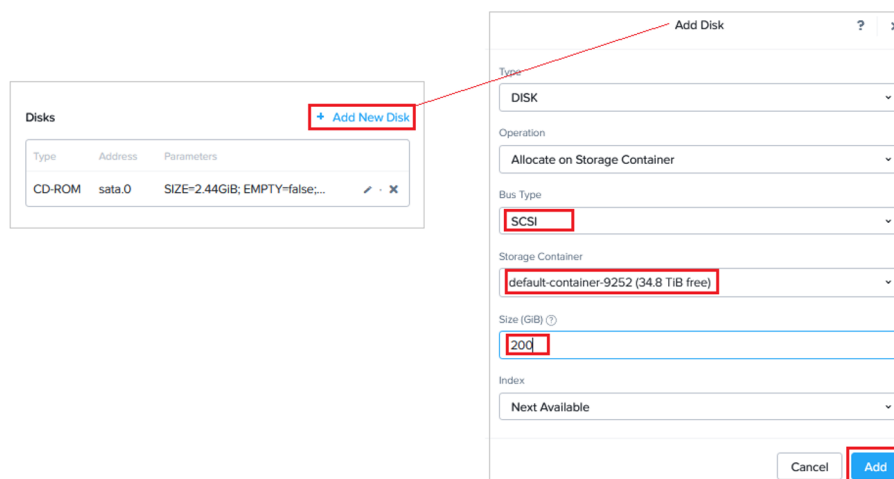


10. Select **Add New Disk**.

11. In the **Add Disk** dialog:

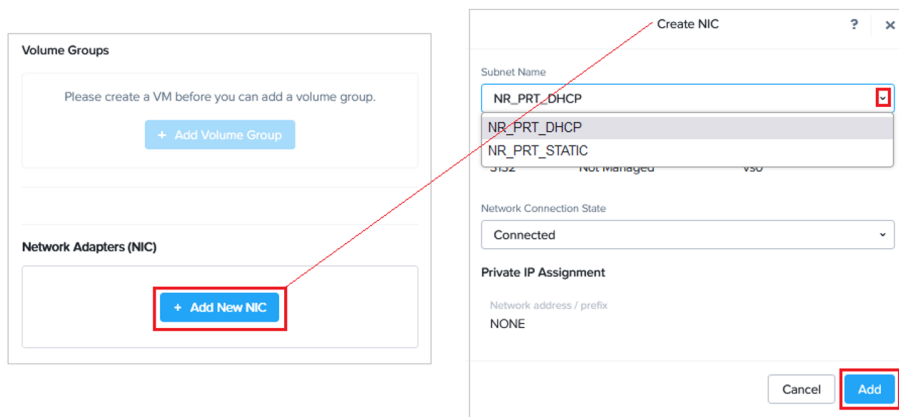
- For **Operation**, select **Allocate on Storage Container**.
- For **Bus Type**, select **SCSI**.
- For **Storage Container**, select the required service container.
- For **Size**, select **200**.
- For **Index**, select **Next Available**.

12. Select **Add**.

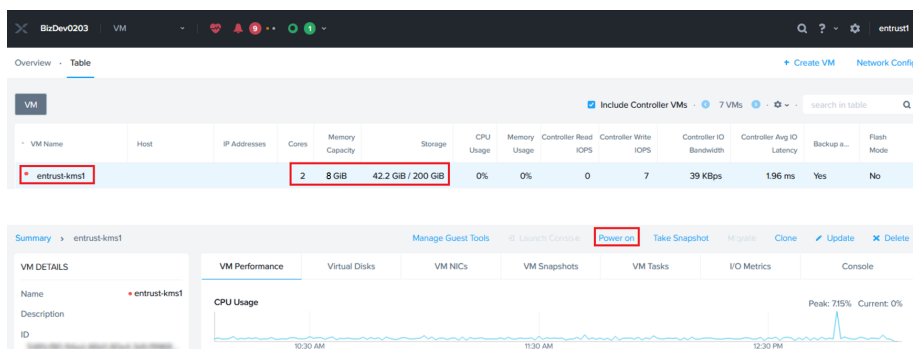


13. Under **Network Adapters (NIC)**, select **Add New NIC**.

14. In the **Create NIC** dialog, select your **Subnet Name** and select **Add**.



15. At the bottom of the **Create VM** dialog, select **Save** to save the VM.
16. On the **VM** page, confirm that the VM is created.



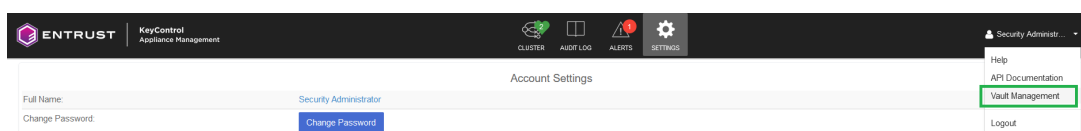
17. Select **Power on** to start the VM.
18. Repeat all steps to create a second node.

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

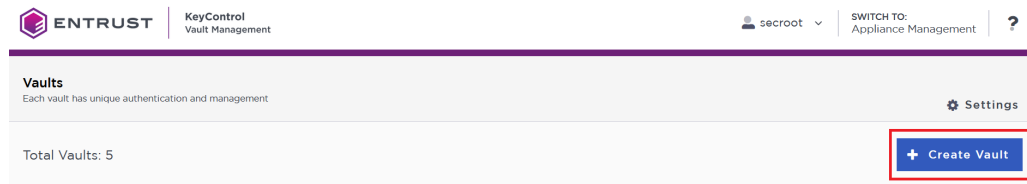
Join the two KeyControl nodes in a high availability cluster following the instructions [Installing a New KeyControl Vault Cluster](#). Additional information can be found at [Entrust Documentation](#) (search for the **KeyControl**).

2.4. Create an 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.

Vault Successfully Created

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

Vault URL

Copy

User Name
admin@nutanix.com

Copy

Temporary Password

Copy

Close

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

ENTRUST

KeyControl
Vault for KMIP

Sign in to your account

User Name

Password

SIGN IN

7. Notice the new vault.

ENTRUST

KeyControl
Vault for KMIP

NutanixAHV

Home

Objects

Security

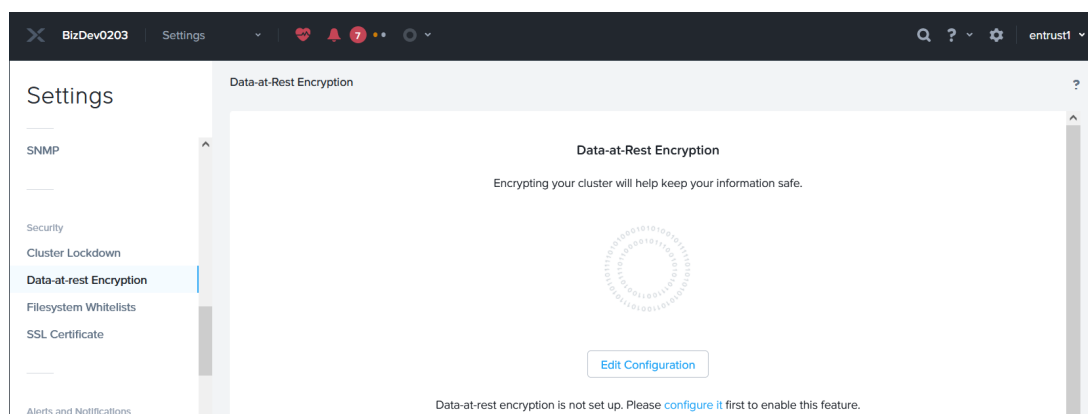
Audit Logs

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

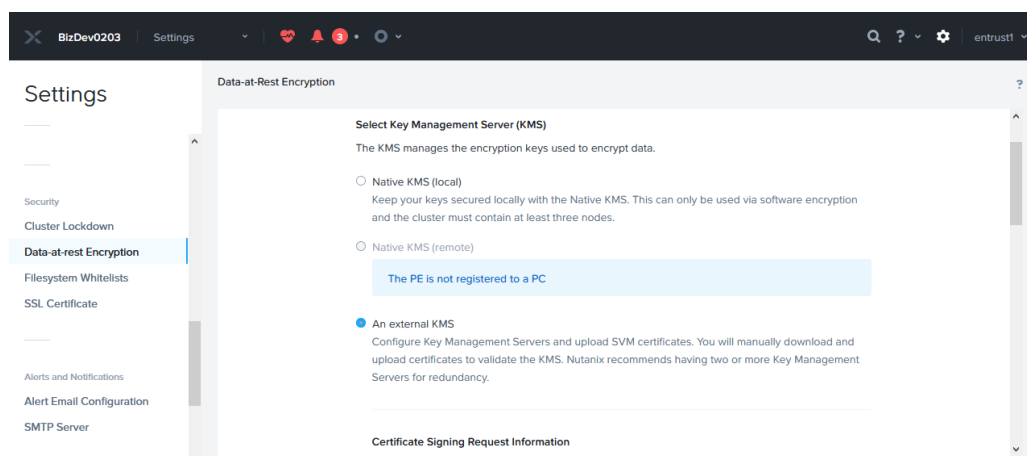
These instructions are performed on a different AHV cluster, not on the one that was used in [Install and configure Entrust KeyControl](#).

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**.

Settings

Data-at-Rest Encryption

Certificate Signing Request Information

Enter the following information to generate the Certificate Signing Requests for the cluster.

Email: Country Code:

City: State:

Organization: Organizational Unit:

[Save CSR Info](#) [Download CSRs](#)

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

Settings

Data-at-Rest Encryption

Successfully saved Certificate Signing Request Information

Certificate Signing Requests

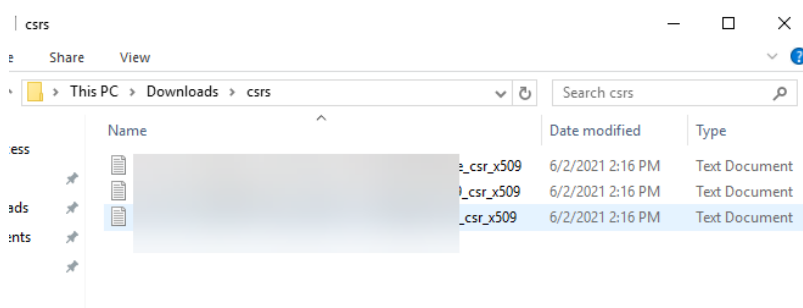
Download the CSRs for the Nodes

[Download CSRs for all nodes](#)

Node Address	Action
<input type="text"/>	Download
<input type="text"/>	Download
<input type="text"/>	Download

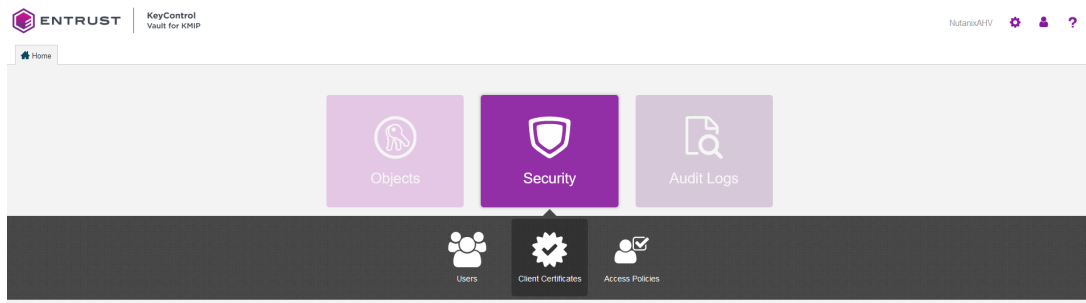
[Back](#)

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.

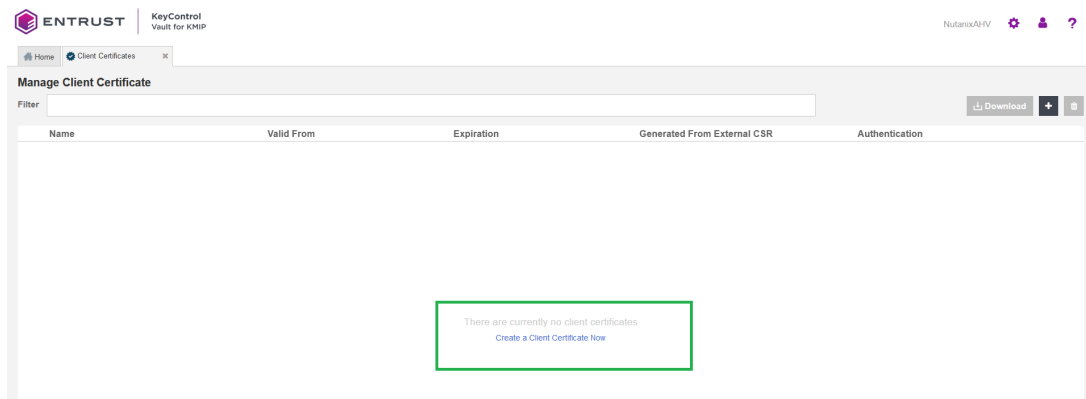


3.2. Create the KMIP client certificate bundles

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. These certificates are not **.csr** type. You may need to allow **All** file types for them to show in the file manager window. Then select **Create**.

Create Client Certificate

×

☐ Add Authentication for Certificate

Certificate Name *

Certificate Expiration *

📅

Certificate Signing Request (CSR)

Browse

☐ Encrypt Certificate Bundle

Cancel

Create

6. Create certificates for the other nodes.

ENTRUST

KeyControl
Vault for KMIP

NutanixAHV ⚙️ 👤 ?

Home Client Certificates X

Manage Client Certificate

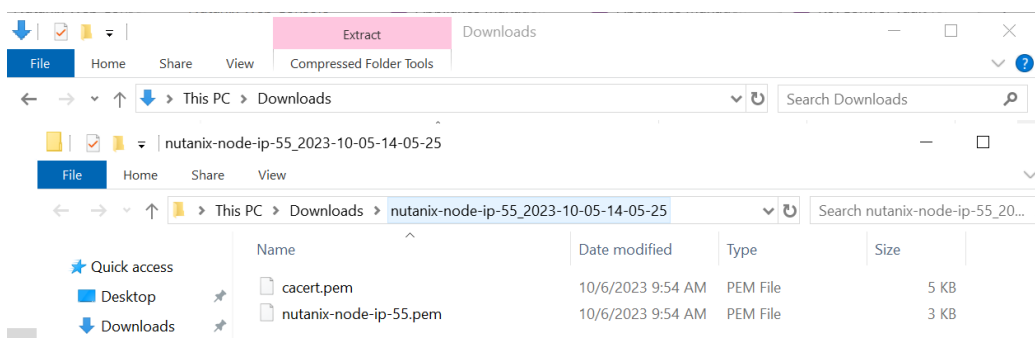
Filter

Download +

Name	Valid From	Expiration	Generated From External CSR	Authentication
<input type="checkbox"/> nutanix-node-ip-15	Oct 5, 2023, 9:25:03 AM	Oct 5, 2024, 9:25:03 AM	✓ Yes	Disable
<input type="checkbox"/> nutanix-node-ip-16	Oct 5, 2023, 9:27:18 AM	Oct 5, 2024, 9:27:18 AM	✓ Yes	Disable
<input type="checkbox"/> nutanix-node-ip-17	Oct 5, 2023, 9:27:58 AM	Oct 5, 2024, 9:27:58 AM	✓ Yes	Disable
<input type="checkbox"/> nutanix-node-ip-18	Oct 5, 2023, 9:28:55 AM	Oct 5, 2024, 9:28:55 AM	✓ Yes	Disable
<input type="checkbox"/> nutanix-node-ip-55	Oct 5, 2023, 9:29:36 AM	Oct 5, 2024, 9:29:36 AM	✓ Yes	Disable
<input type="checkbox"/> nutanix-node-ip-56	Oct 5, 2023, 9:30:07 AM	Oct 5, 2024, 9:30:07 AM	✓ Yes	Disable
<input type="checkbox"/> nutanix-node-ip-57	Oct 5, 2023, 9:30:34 AM	Oct 5, 2024, 9:30:34 AM	✓ Yes	Disable

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**.

The screenshot shows the 'Data-at-Rest Encryption' settings page. On the left, the 'Data-at-rest Encryption' menu item is selected under the 'Security' category. The main content area is titled 'Add a New Key Management Server'. It includes a sub-header 'Enter a name and at least one address for the Key Management Server.' and an 'Add Address' button. Below this is a table with two rows of input fields:

NAME	ADDRESS	PORT
EntrustKeyControl	10.16.48.81	5696
	10.16.48.82	5696

At the bottom of the form are a '< Back' button and a 'Save' button.

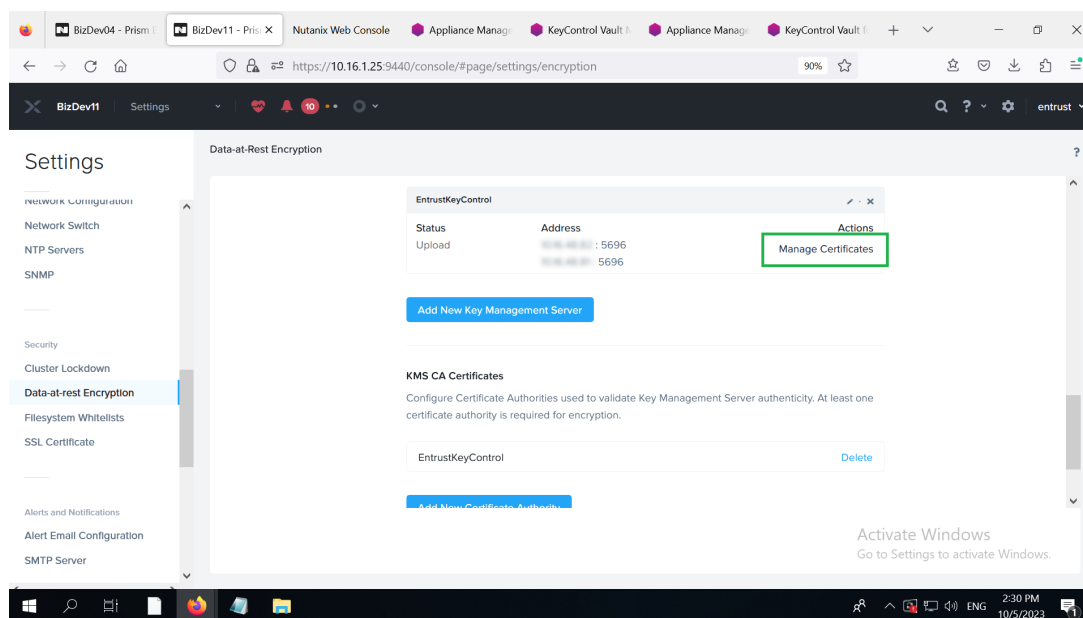
6. Select **Add New Certificate Authority** further down. Name the CA, then select **Upload CA Certificate**, and choose one of the **cacert.pem** files created above. All **cacert.pem** files are identical. Then select **Save**.

The screenshot shows the 'Data-at-Rest Encryption' settings page, specifically the 'Add a New Certificate Authority' section. It includes a sub-header 'Upload the Certificate Authority (CA) certificate and enter a name for the Certificate Authority. cacert.pem is selected' and an 'Upload CA Certificate' button. Below this is a text input field for the 'CERTIFICATE AUTHORITY NAME' with the value 'EntrustKeyControl'. At the bottom of the form are a '< Back' button and a 'Save' button.

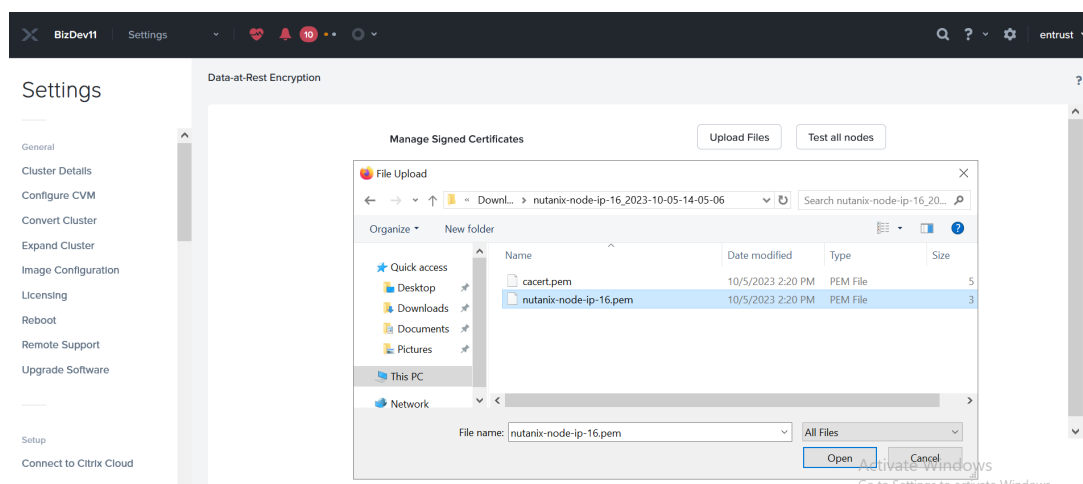
3.4. Add the Entrust KeyControl KMIP cluster certificates to the Nutanix AHV cluster

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.

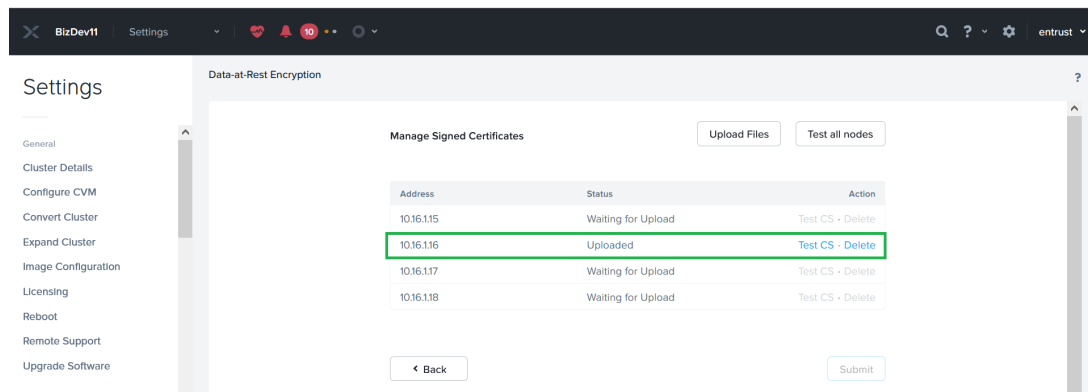
3. Select **Data-at-rest Encryption** under **Security** on the **Settings** left pane.
4. Select **Continue Configuration**. Then scroll down to the **Key Management Server** section.
5. Select the **Manage Certificates** hyperlink of the **EntrustKeyControl** cluster. This hyperlink is below **Actions**.



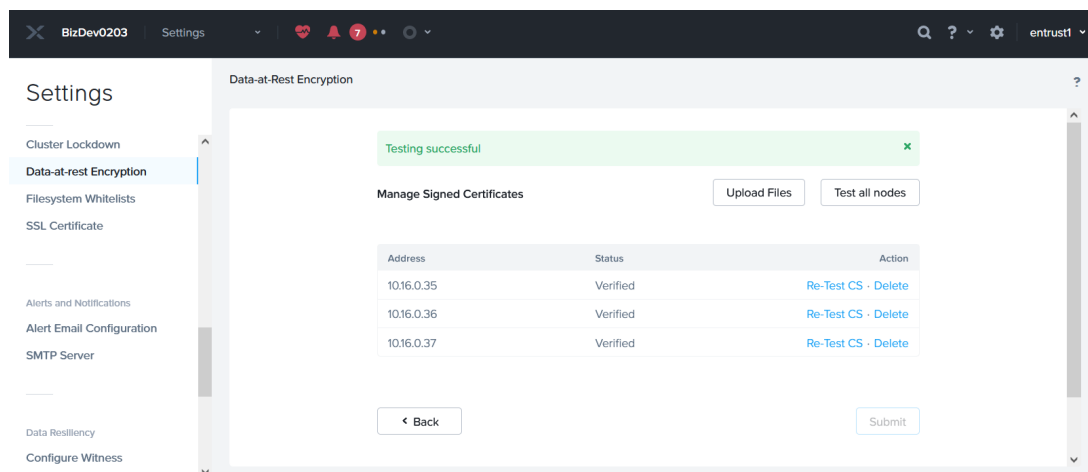
6. Select **Upload Files**, and choose a **username.pem** created above, then select **Submit**.



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

To 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**.

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 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 nShield HSM Integration Guide](#) available at [Entrust documentation library](#).

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