Nutanix and Entrust KeyControl

Integration Guide

2024-02-12

© 2024 Entrust Corporation. All rights reserved.

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. 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

The following steps summarize the deployment of the Entrust KeyControl in cluster mode in Nutanix:

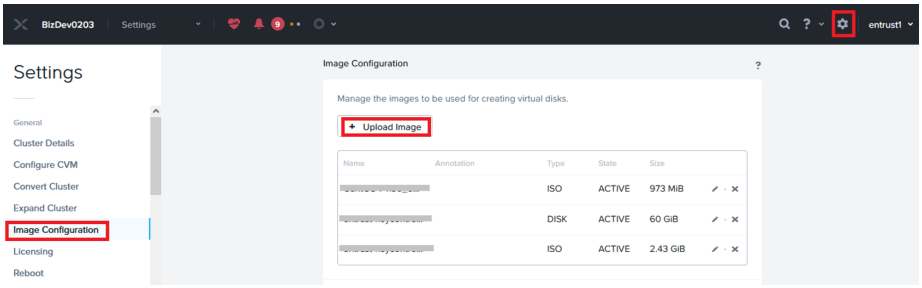
1. Upload the Entrust KeyControl ISO in AHV
2. Deploy an Entrust KeyControl node on AHV
3. Join the two Entrust KeyControl nodes to form a cluster.
4. Create an Entrust KeyControl vault

A two-node cluster was deployed for this integration. Refer to the following link for Online Documentation Set.

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 Entrust KeyControl ISO in AHV

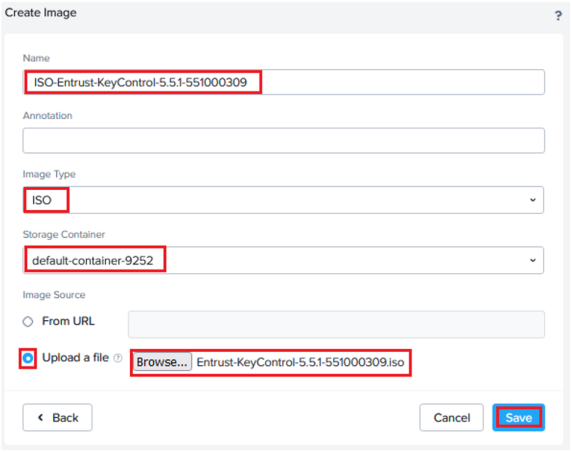
1. Log into the Nutanix Prism Element web UI.
2. Select the **Settings** control on the top tool bar.
3. In the left menu, select **Image Configuration**. The **Image Configuration** page appears. For example:



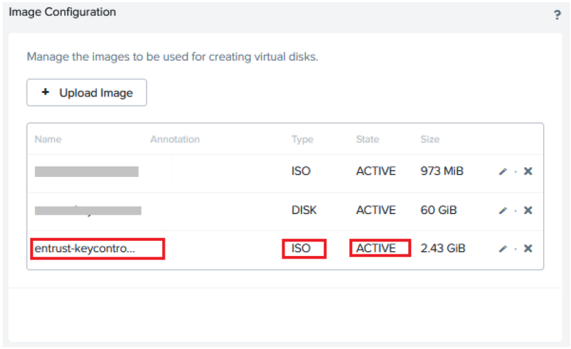
4. Select **Upload Image**. The **Create Image** dialog appears.
5. Enter **Create Image** information:
    - For **Name**, enter a unique name. For example, **ISO-Entrust-KeyControl-10.1.1**.
    - For **Image Type**, select **ISO**.
    - For **Storage Container**, select the required container.

- Select **Upload a file**, browse to the ISO file and select it for use.

For example:



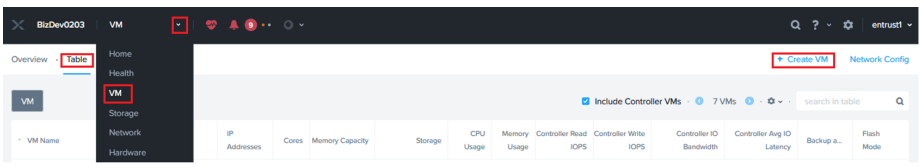
6. Select **Save**.
7. On the **Image Configuration** page, confirm that the image is **ACTIVE**. For example:



For reference, see Configuring Images in the Nutanix online documentation.

2.2. Deploy an Entrust KeyControl node on AHV

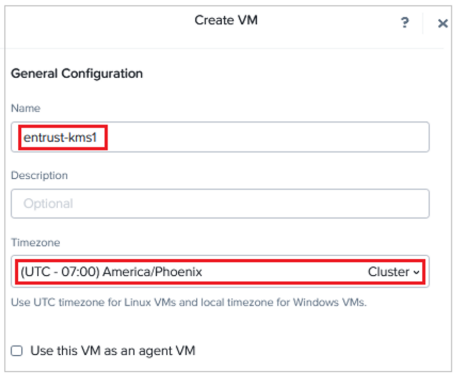
1. Log into the Nutanix Prism Element web UI.
2. Select **VM** from the pull-down menu on the top tool bar. The **VM** page appears. For example:



3. Select the **Table** tab.

4. Select **Create VM**. The **Create VM** dialog appears.
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**.

    For example:

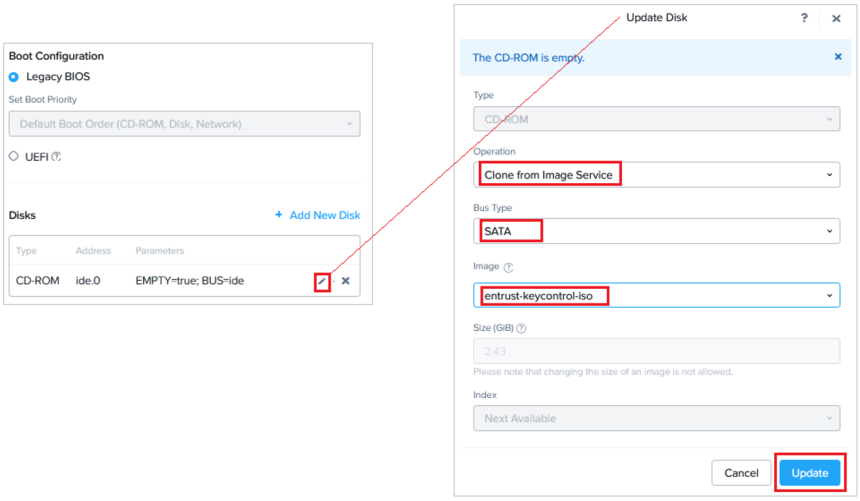


6. Under **Compute Details** information:
    - For **vCPUs**, enter **2**.
    - For **Memory**, select **60**.

    For example:

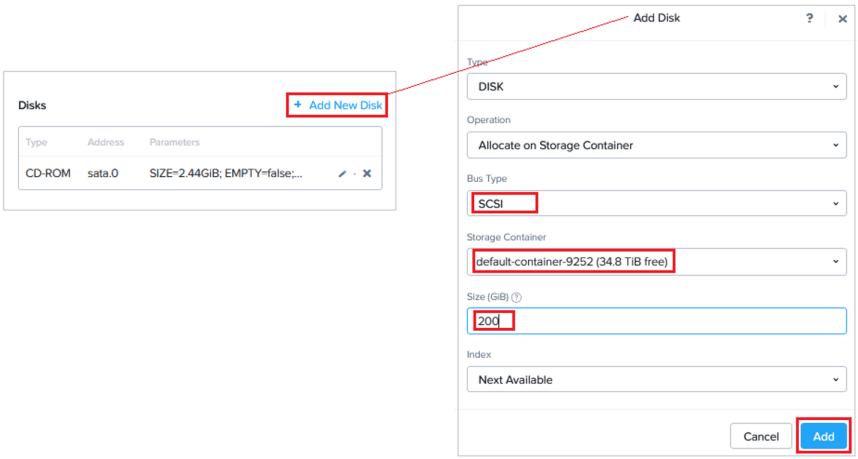
7. Under **Boot Configuration** information:
    - Select **Legacy BIOS**.
    - Under **Disks**, select the edit button for the **CD-ROM** entry. The **Update Disk** dialog appears.
    - In the **Update Disk** dialog:
        - For **Operation**, select **Clone from Image Service**.
        - For **Bus Type**, select **SATA**.
        - For **Image**, enter the ISO file name.
        - Select **Update**.

For example:

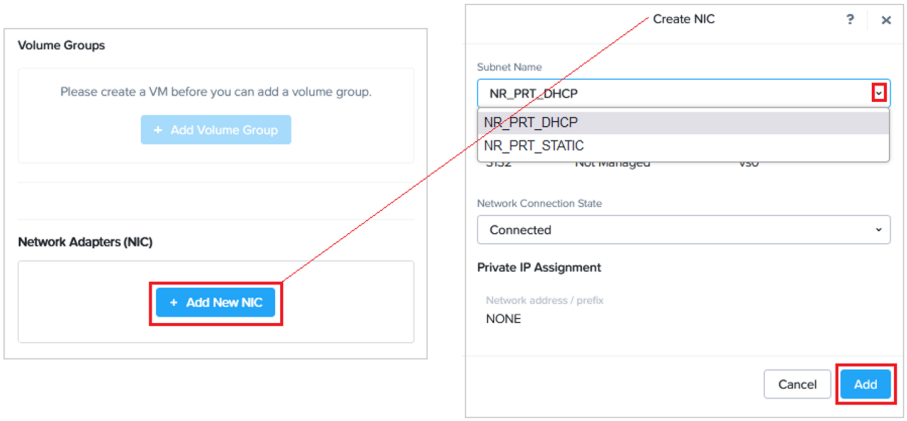


- Select **Add New Disk**. The **Add Disk** dialog appears.
- In the **Add Disk** dialog:
  - For **Operation**, select **Allocate on Storage Container**.
  - For **Bus Type**, select **SCSI**.
  - For **Storage Container**, select the required service container.
  - For **Size**, select **200**.
  - For **Index**, select **Next Available**.
  - Select **Add**.

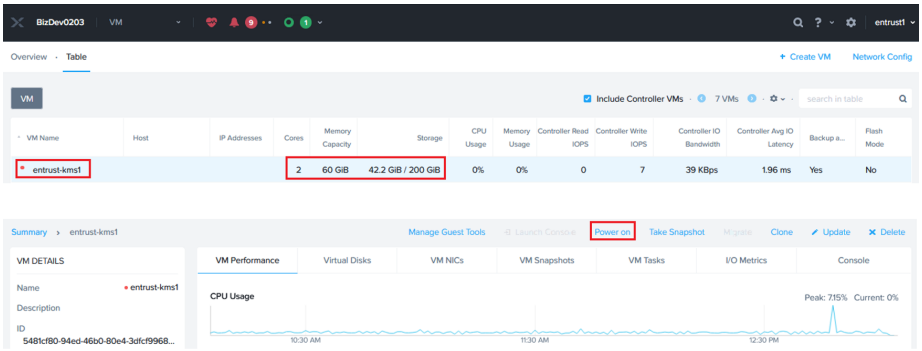
For example:



8. Under **Network Adapters (NIC)**, select **Add New NIC**. The **Create NIC** dialog appears.
9. In the **Create NIC** dialog, select your **Subnet Name** and select **Add**. For example:



10. At the bottom of the **Create VM** dialog, select **Save** to save the VM.
11. On the **VM** page, confirm that the VM is created. For example:



12. Select **Power on** to start the VM.

For reference, see Create a VM in the Nutanix online documentation.

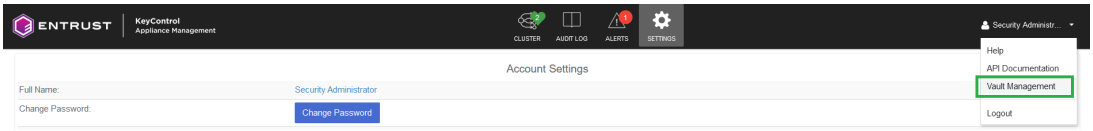
1. Repeat the above to create a second node.

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

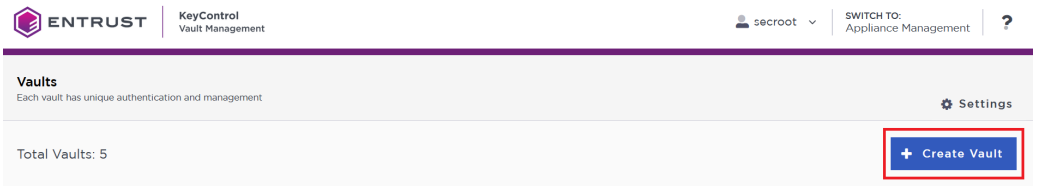
Join the two Entrust KeyControl nodes in a high availability cluster following the instructions Installing a New KeyControl Vault Cluster Additional information can be found at Entrust Dcoumentation. Search for the **KeyControl**.

2.4. Create an Entrust KeyControl vault

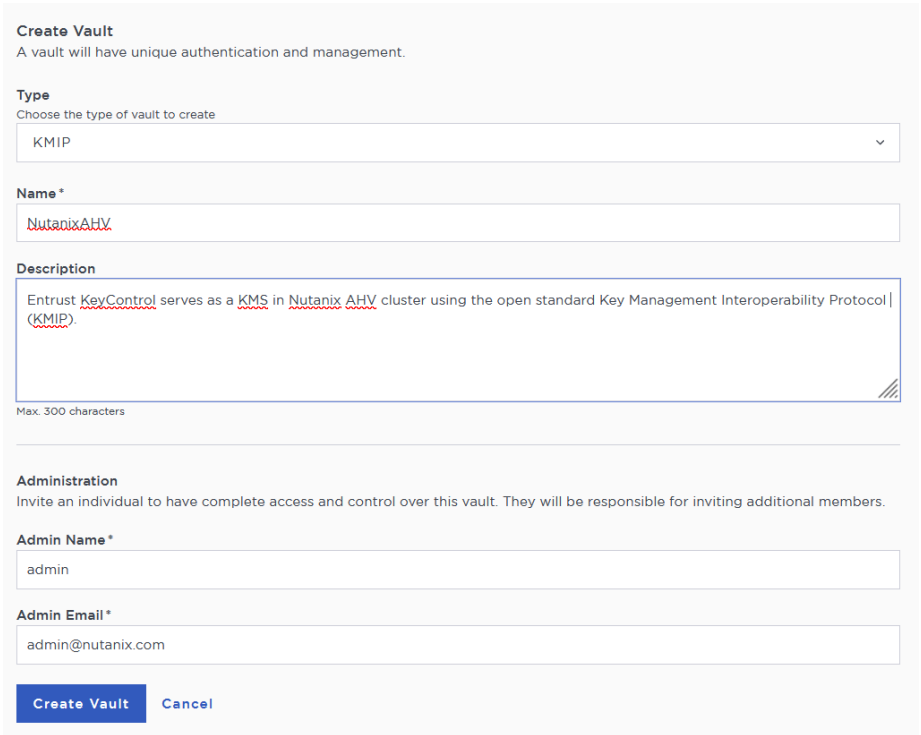
1. Sign in to the Entrust KeyControl Appliance Manager.
2. In the **Appliance Management** home page select **Vault Management**.



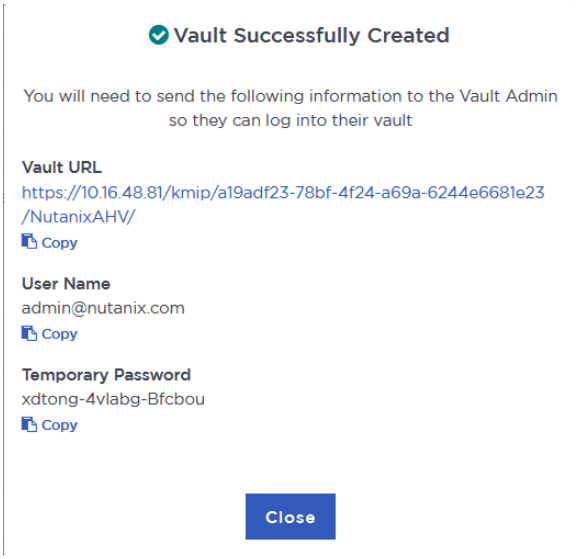
3. In the **Vault Management** home page, select **Create Vault**. The **Create Vault** dialog appears.



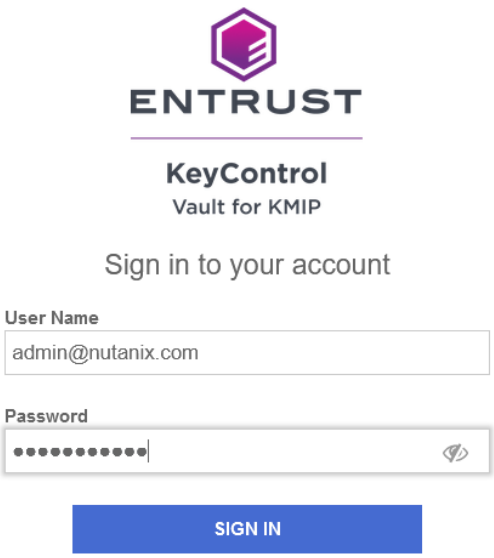
4. In the **Type** drop-down box, select **KMIP**. Enter the required information. Then select **Create Vault**. For example:



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

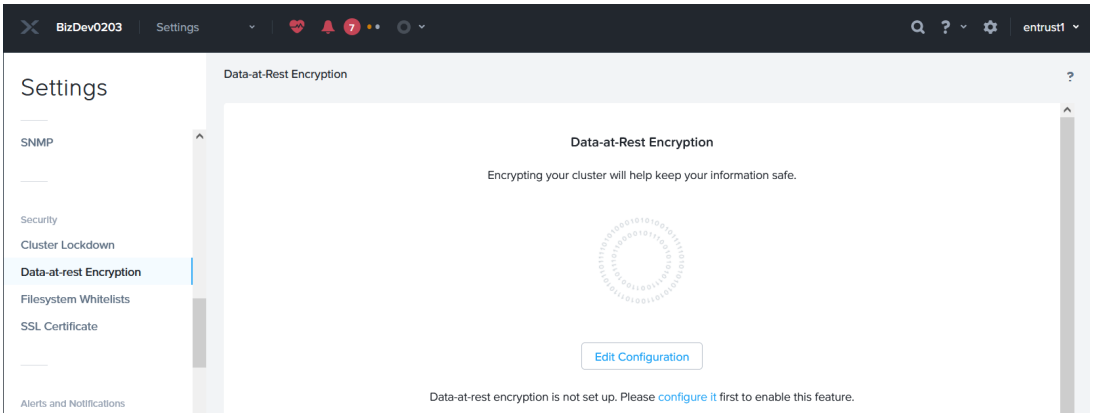
These instructions are performed on a different AHV cluster, not on the one that was used in Install and configure Entrust KeyControl. We want to encrypt this AHV cluster.

The steps to use Entrust KeyControl in cluster mode and data-at-rest encryption in Nutanix:

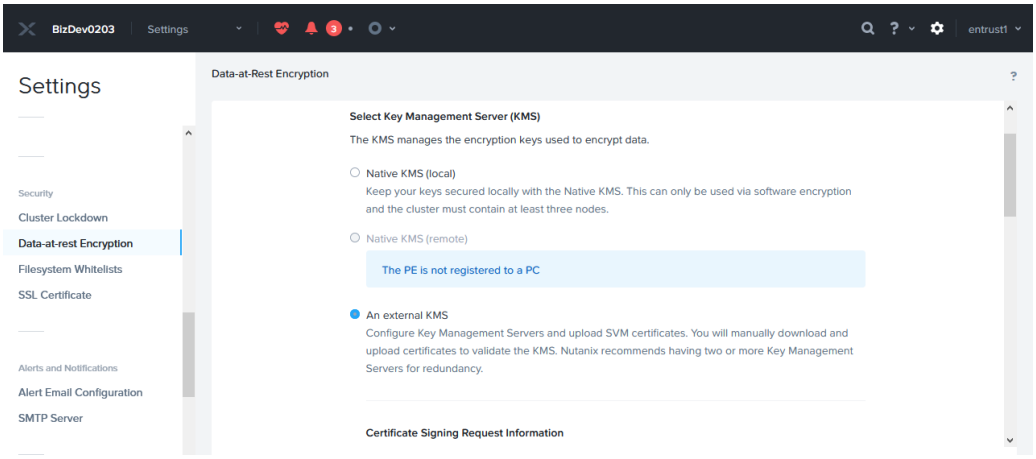
1. Select KeyControl as the KMIP Server and generate the certificate requests
2. Create the KMIP client certificate bundles
3. Add the Entrust KeyControl KMIP cluster to the Nutanix AHV cluster
4. Add the Entrust KeyControl KMIP cluster certificates to the Nutanix AHV cluster
5. Enable encryption

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

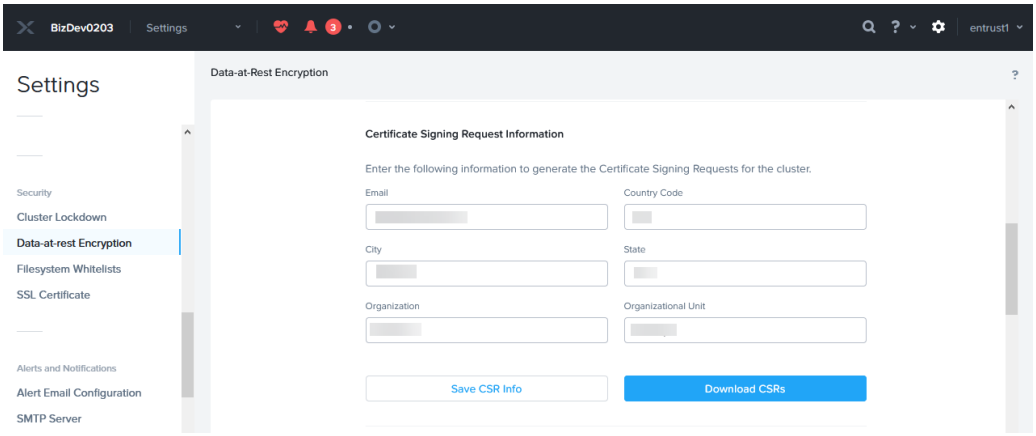
1. Log into the Nutanix Prism Element web UI.
2. Select the **Settings** pull-down menu in the toolbar, scroll down, and select **Settings** again. The **Gear** icon in the top right of the toolbar does the same operation.
3. Select **Data-at-rest Encryption** under **Security** on the **Settings** left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



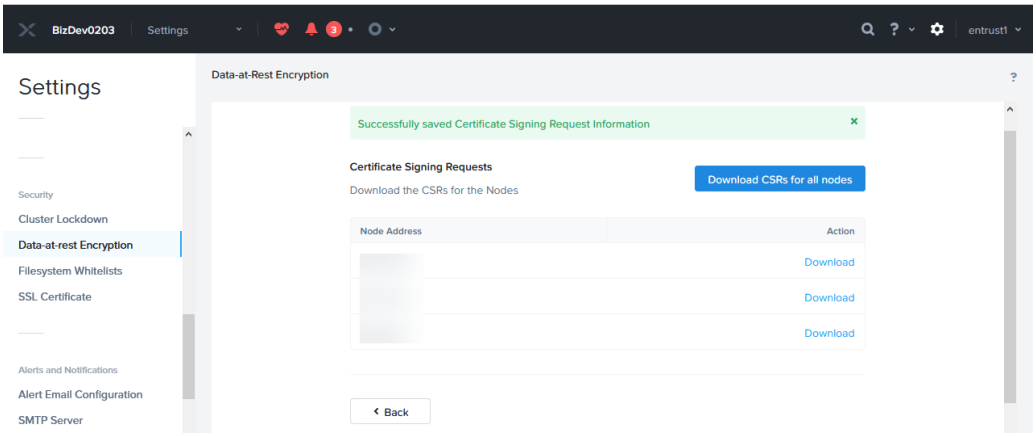
4. Select **An external KMS**.



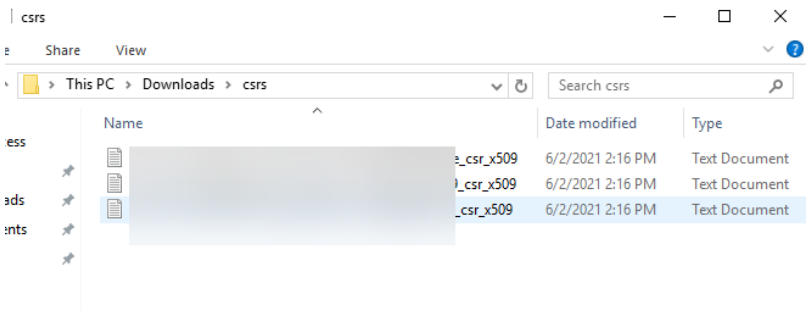
5. Scroll down to **Certificate Signing Request Information**. Fill the request form, then select **Save CSR Info**.



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

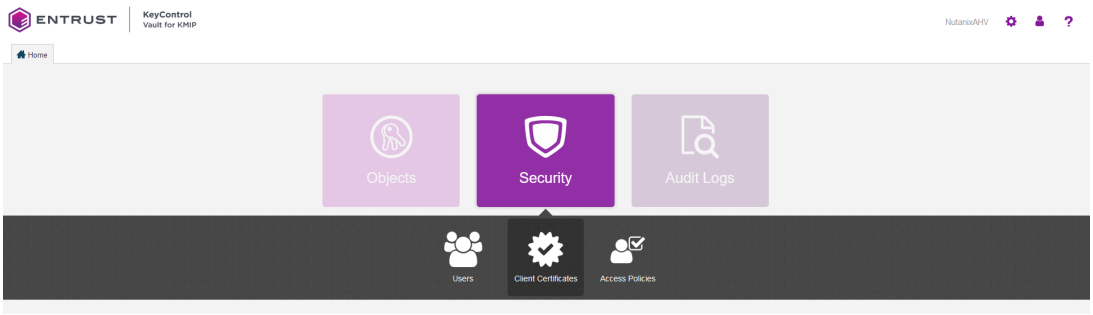


7. The compressed `csrs.zip` file is created. Save the file locally. Extract the files. Notice that a certificate request was created for each node in the Nutanix AHV cluster.

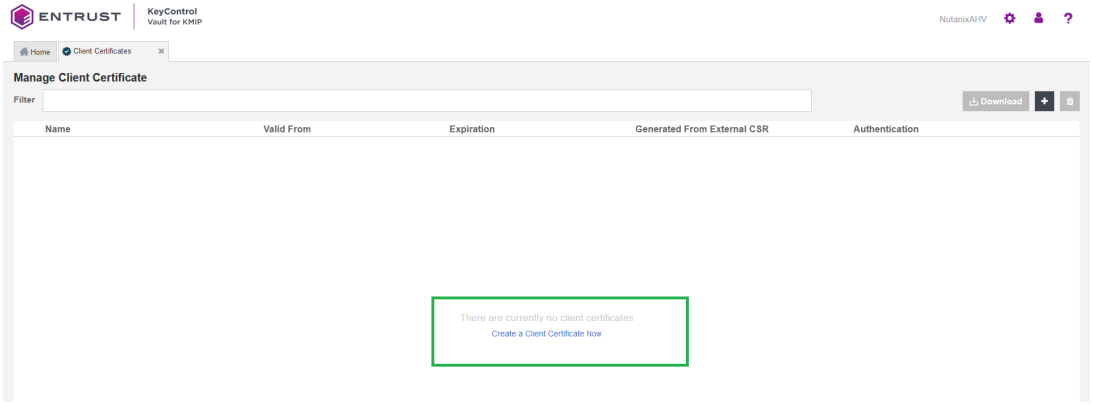


3.2. Create the KMIP client certificate bundles

1. Log into the Entrust KeyControl vault created in section [test:::create-keycontrol-vault].
2. Select the **Security** incon, and then the **Client Certificates** icon.

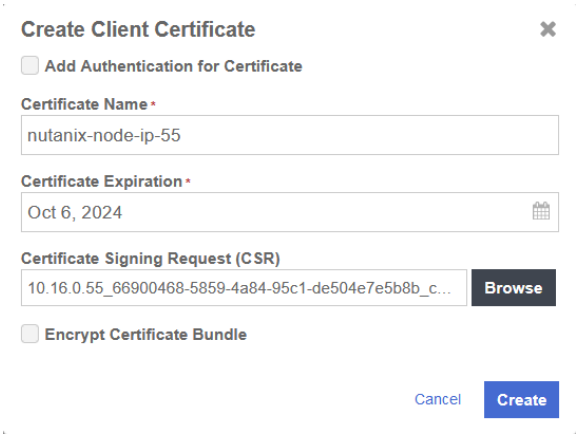


3. Select **Create a Client Certificate Now**.

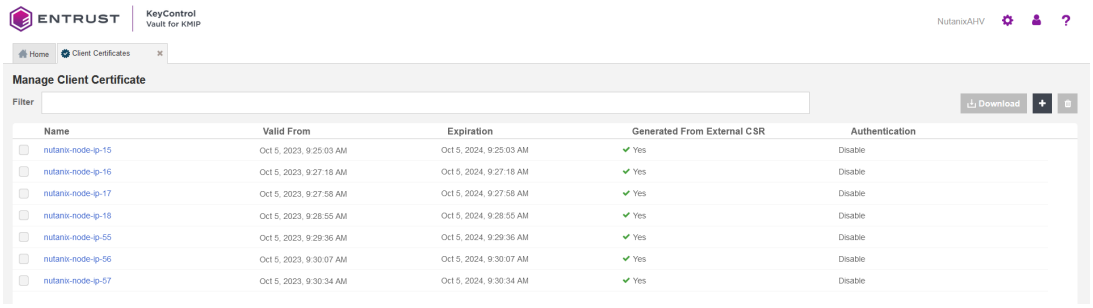


4. Enter the **Certificate Name** in the text box. Choose a name unique per a given node in the Nutanix cluster, for example the last octet of the node's IP address as part of the name.
5. Select **Load File** and choose the certificate request from section Select KeyControl as the KMIP Server and generate 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.

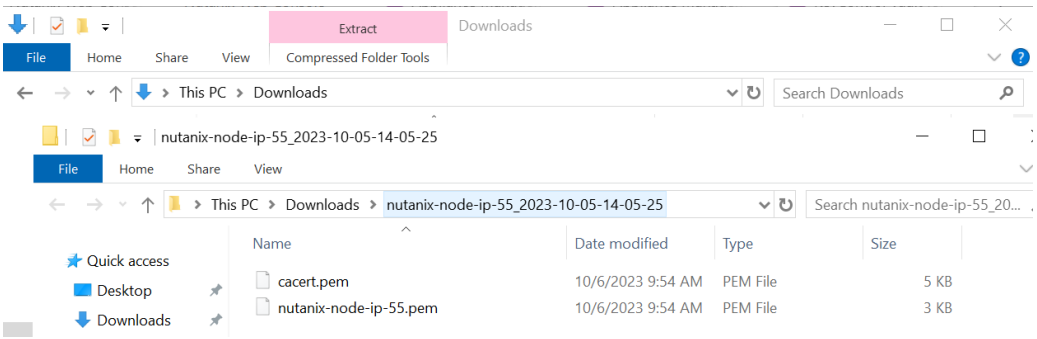
Then select **Create**.



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`.

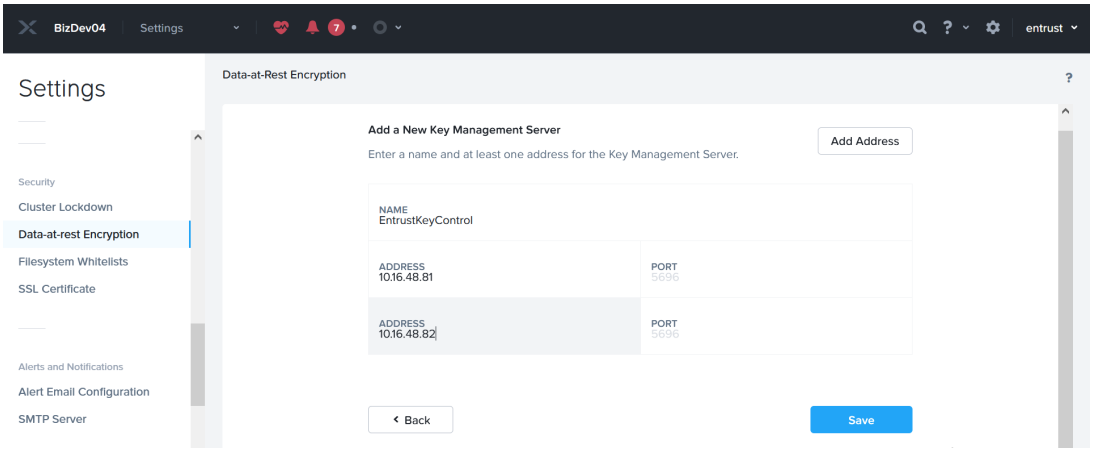


9. Repeat the step above for the other certificates.

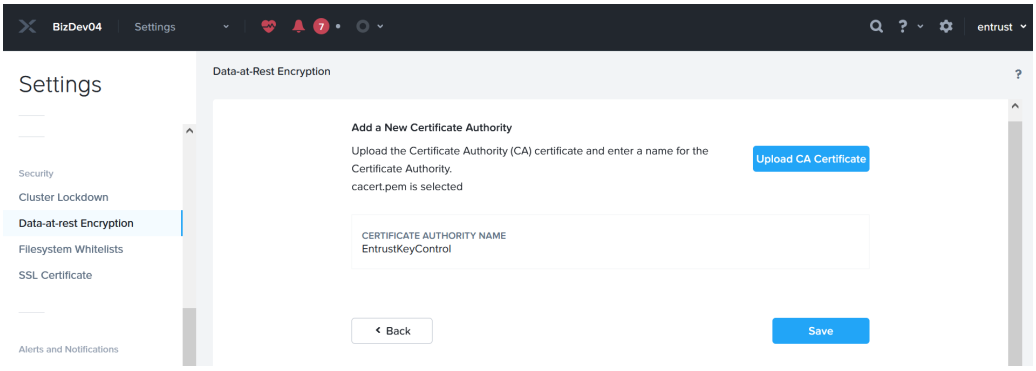
The `cacert.pem` file for each node above are identical. The `username.pem` files are unique for each node.

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 KeyContol cluster, and the IP address of all the nodes in the cluster. The default port is 5696. Then select **Save**.



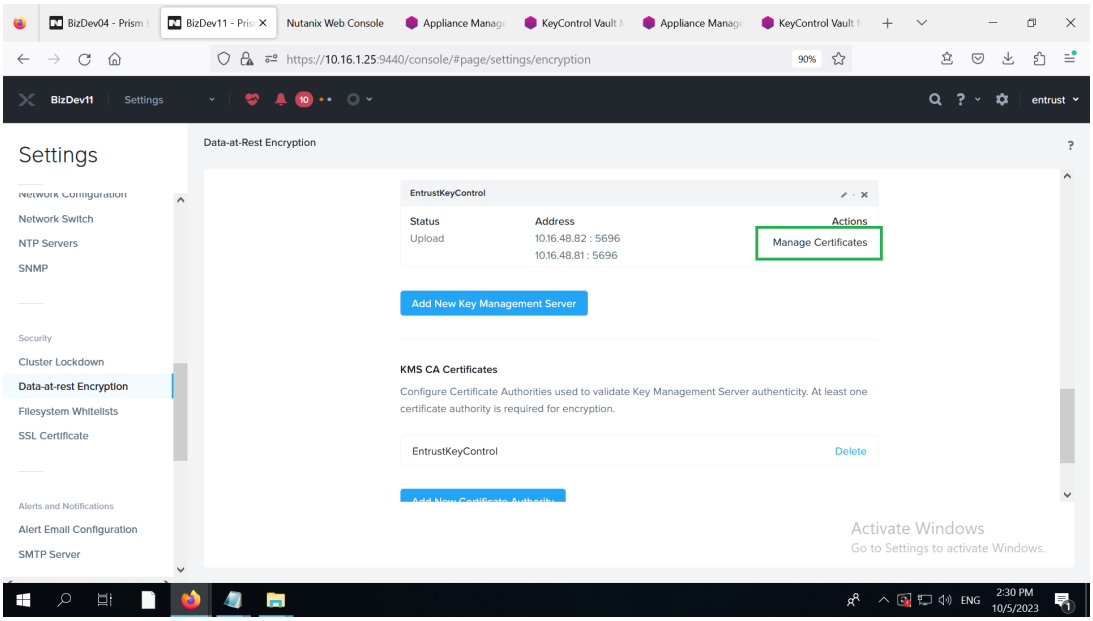
6. Select **Add New Certificate Authority** further down. Name the CA, then select **Upload CA Certificate**, and choose one of the `cacert.pem` files created above. All `cacert.pem` files are identical. Then select **Save**.



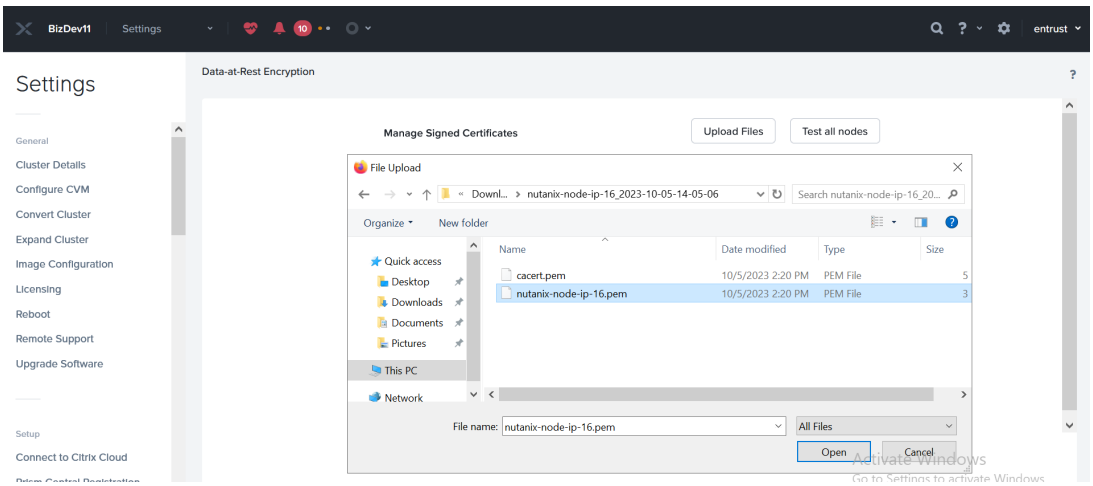
3.4. Add the Entrust KeyControl KMIP cluster certificates to the Nutanix AHV cluster

1. Log into the Nutanix Prism Element web UI.

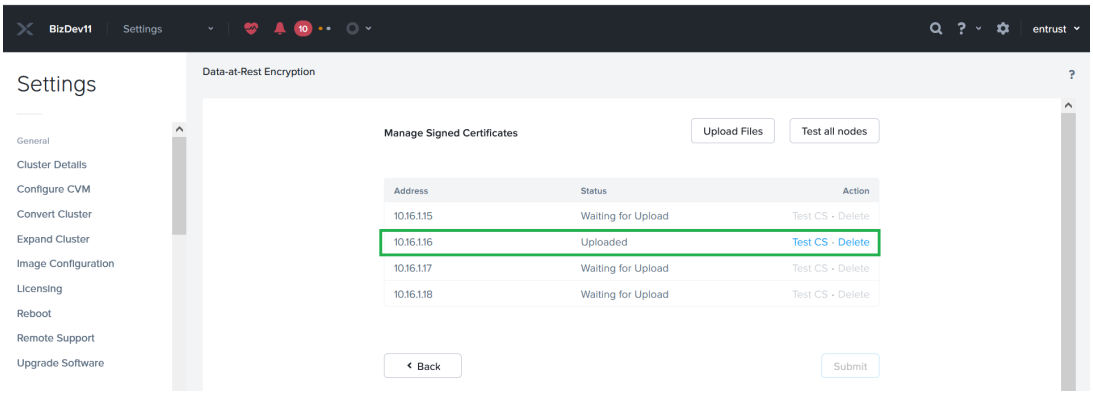
2. Select the **Settings** icon to the right of the toolbar to bring up the **Settings** menu.
3. Select **Data-at-rest Encryption** under **Security** on the **Settings** left pane.
4. Select **Continue Configuration**. Then scroll down to the **Key Management Server** section.
5. Select the **Manage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



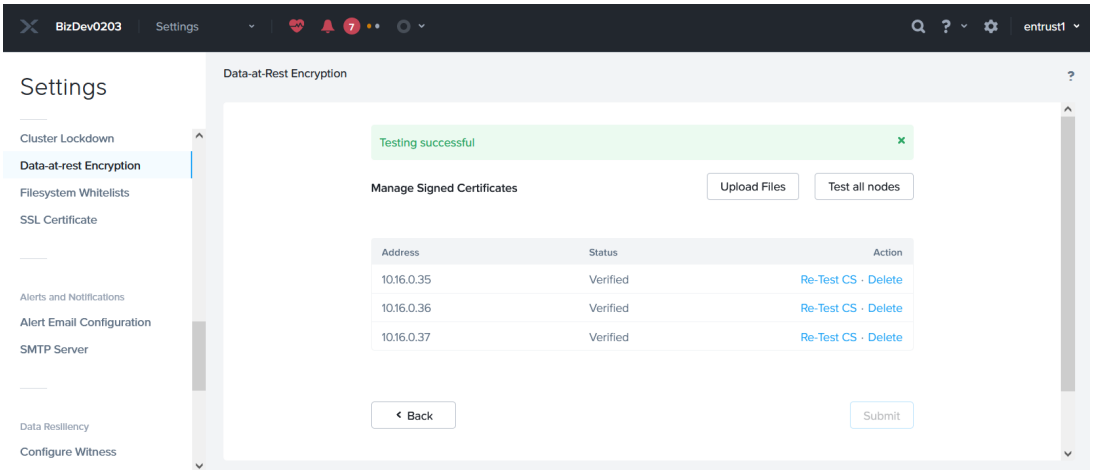
6. Select **Upload Files**, and choose a `username.pem` created above, then select **Submit**.



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



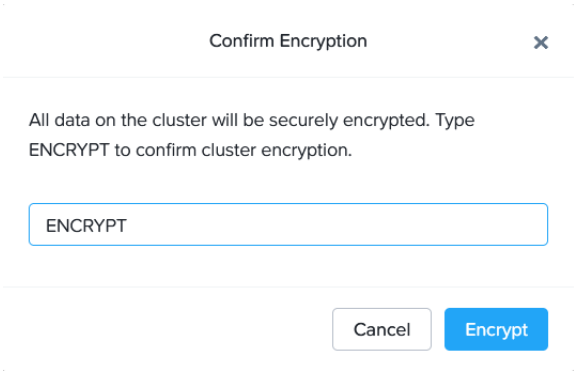
8. Repeat the above for the other nodes.



3.5. Enable encryption

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**.



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