Nutanix and Entrust KeyControl

Integration Guide

21 Oct 2022

Contents

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 v 5.5.1 Online Documentation Set, located in the Entrust Product Documentation.

For more information related to either product refer to Entrust KeyControl online customer portal and the Nutanix online services and portals.

1.2. Product configurations

The following versions have been tested for compatibility:

Product	Version
Nutanix AOS	v6.5.2 LTS
Entrust KeyControl	v5.5.1

2. Procedures

The following steps summarize the deployment of the KeyControl in cluster mode and the configuration of the data-at-rest encryption in Nutanix:

1. Deploy a KeyControl cluster
2. Select KeyControl as the KMIP Server and generate the certificate requests
3. Enable KMIP in the KeyControl cluster
4. Create a KMIP tenant
5. Create the KMIP client certificate bundles
6. Add KeyControl KMIP cluster to the Nutanix AHV cluster
7. Add KeyControl KMIP cluster certificates to the Nutanix AHV cluster
8. Enable encryption

2.1. Deploy a KeyControl cluster

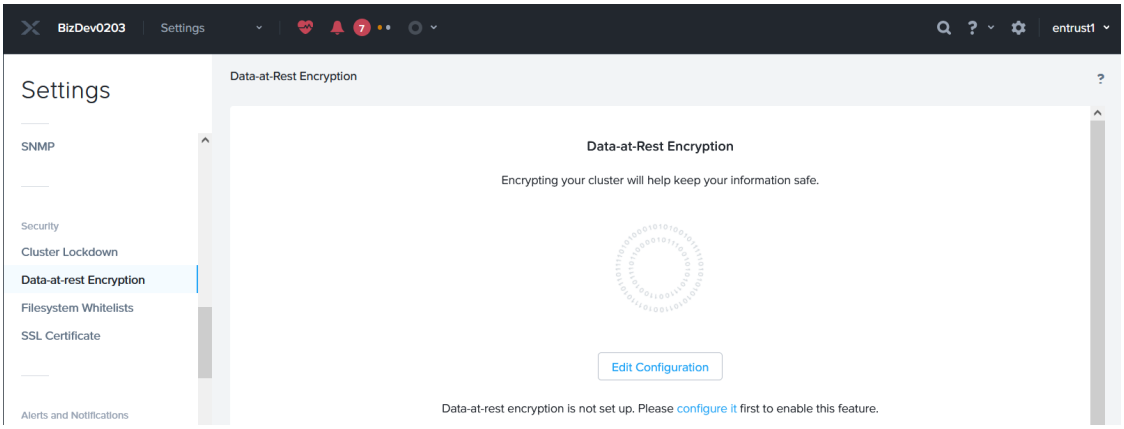
A two-node cluster was deployed for this integration. Refer to the following link for KeyControl installation instructions.

An OVA template was used to deploy the KeyControl node VM. The OVA template is available at Hytrust Software Downloads.

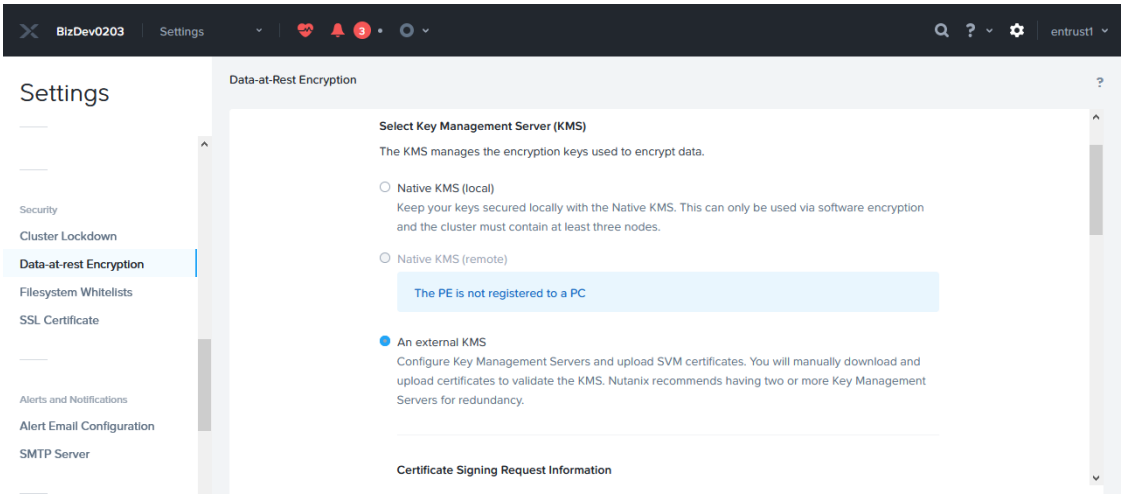
2.2. Select KeyControl as the KMIP Server and generate the certificate requests

To select KeyControl as the KMIP Server and generate the certificate requests:

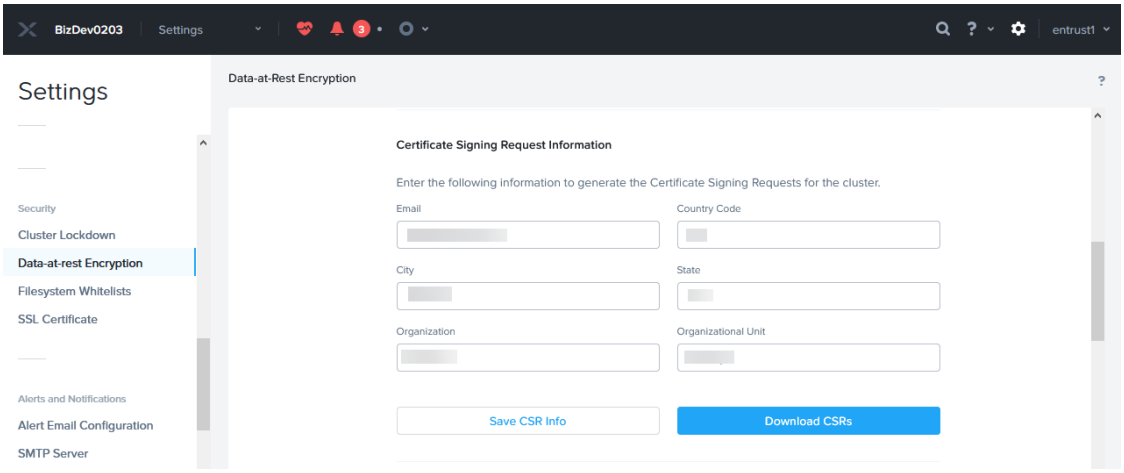
1. Log into the Nutanix Prism Element web UI.
2. Select the **Settings** pull-down menu in the toolbar, scroll down, and select **Settings** again. The **Gear** icon in the top right of the toolbar does the same operation.
3. Select **Data-at-rest Encryption** under **Security** on the **Settings** left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



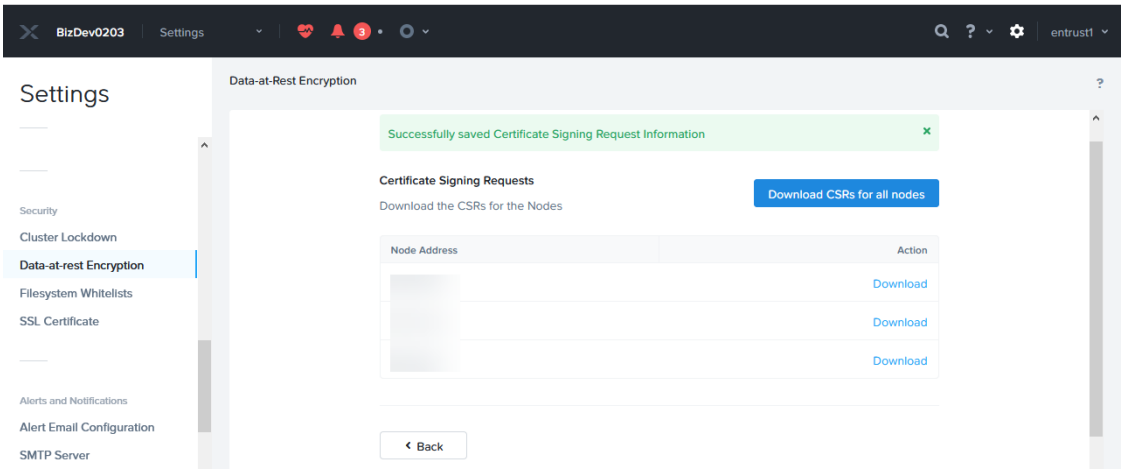
4. Select **An external KMS**.



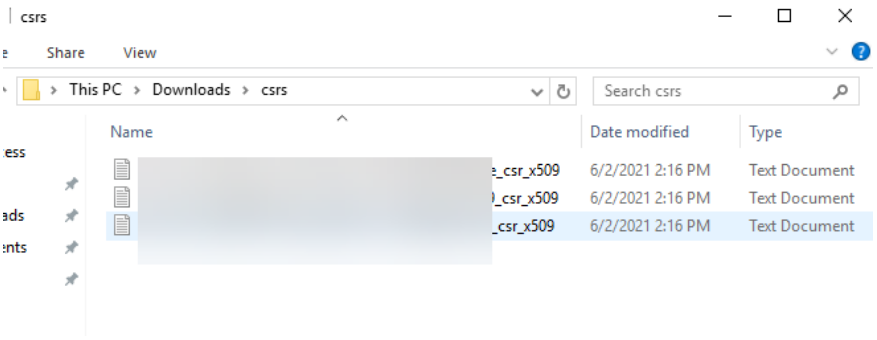
5. Scroll down to **Certificate Signing Request Information**. Fill the request form, then select **Save CSR Info**.



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.



2.3. Enable KMIP in the KeyControl cluster

To enable KMIP in the KeyControl cluster:

1. Log into the KeyControl server web UI using an account with Security Admin privileges.
2. Select **KMIP** in the toolbar menu. Then select the **Settings** tab.
3. Use the pull-down menu to change the **State** to **ENABLED**. Then select **Apply**.

2.4. Create a KMIP tenant

To create a KMIP tenant:

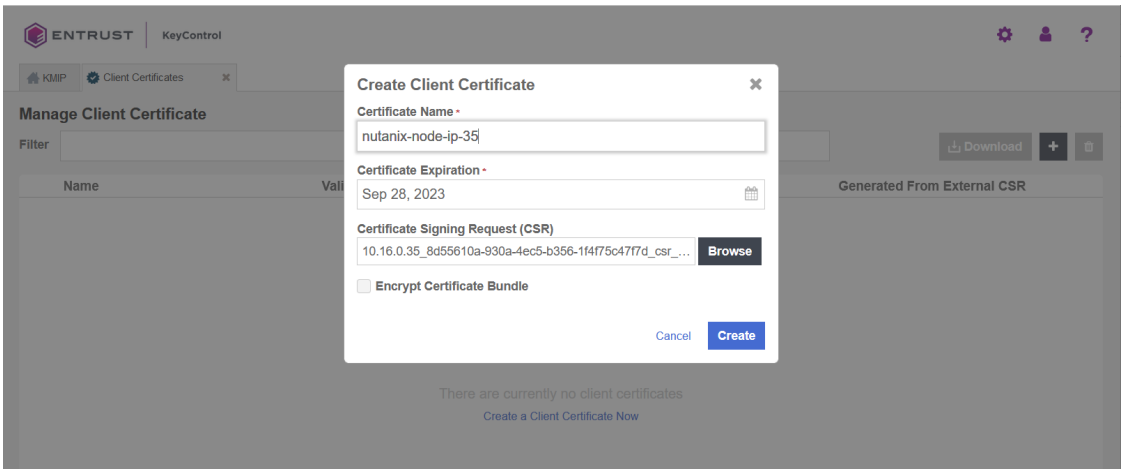
1. Log into the KeyControl server web UI using an account with Security Admin privileges.
2. Select **KMIP** in the toolbar menu. Then select the **Tenant** tab.
3. Select **Create a KMIP Tenant** in the **Actions** pull-down menu.
4. Enter the **Name** and **Description** and select **Next**.

5. Select the **Authentication Type**. Then select **Next**. This integration was performed using **Local User Authentication**.
6. Enter the **Administrator** credentials and select **Create**.

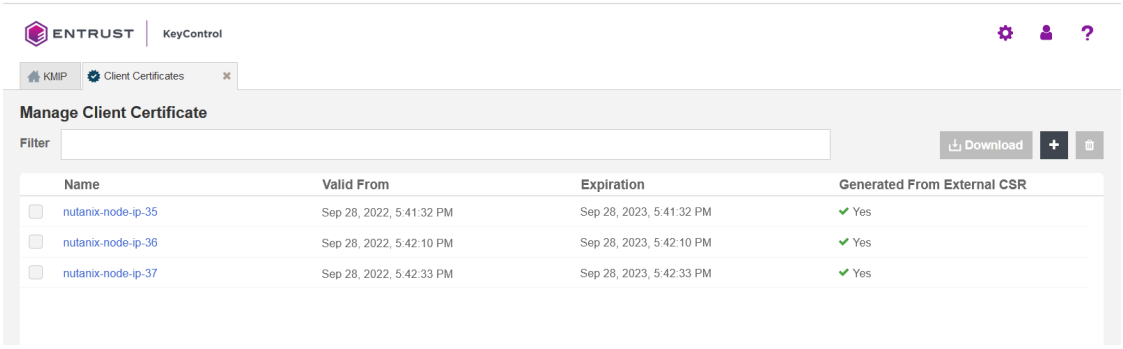
2.5. Create the KMIP client certificate bundles

To create the KMIP client certificate bundles:

1. Log into the KeyControl server web UI using an account with Security Admin privileges.
2. Select **KMIP** in the toolbar menu. Then select the **Tenant** tab.
3. Select the tenant and scroll down to **Tenant Login**. Click on the link. A new tab opens.
4. Login with the tenant credentials.
5. Select the **Security** icon. Then select the **Client Certificates**. The **Client Certificates** tab appears.
6. Select **Create**, the plus sign to the right.
7. 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.
8. Select **Load File** and choose the certificate request from the section above 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**.

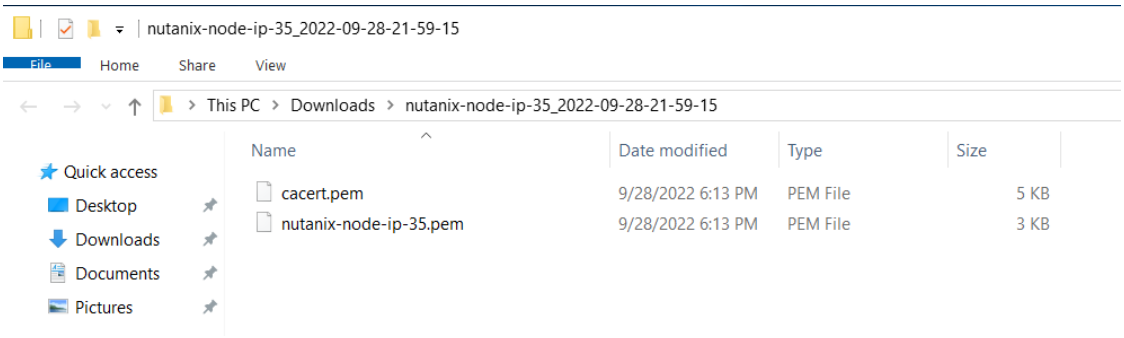


9. Create certificates for the other nodes.



10. Select one of the certificates created above. Then select **Download**.

11. 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`.



12. Repeat the step above for the other certificates.

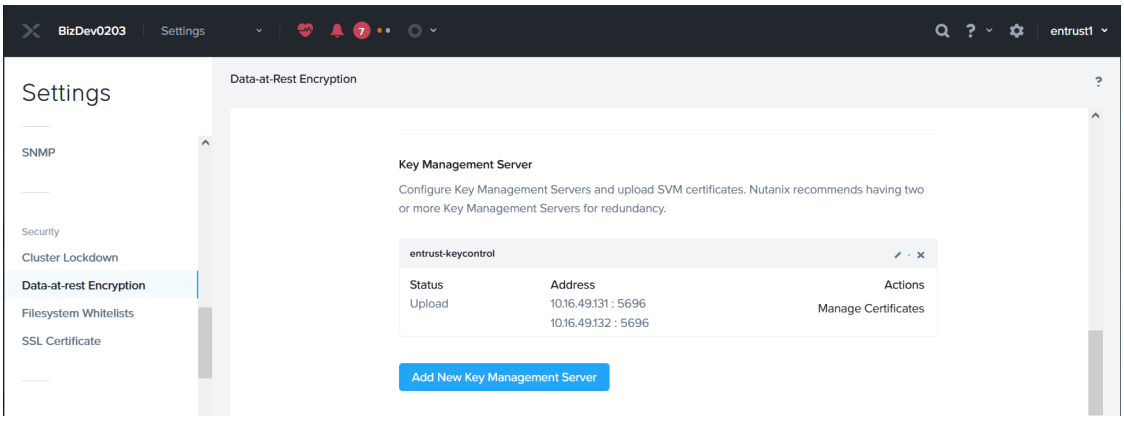
The `cacert.pem` file for each node above are identical. The `username.pem` files are unique for each node.

2.6. Add KeyControl KMIP cluster to the Nutanix AHV cluster

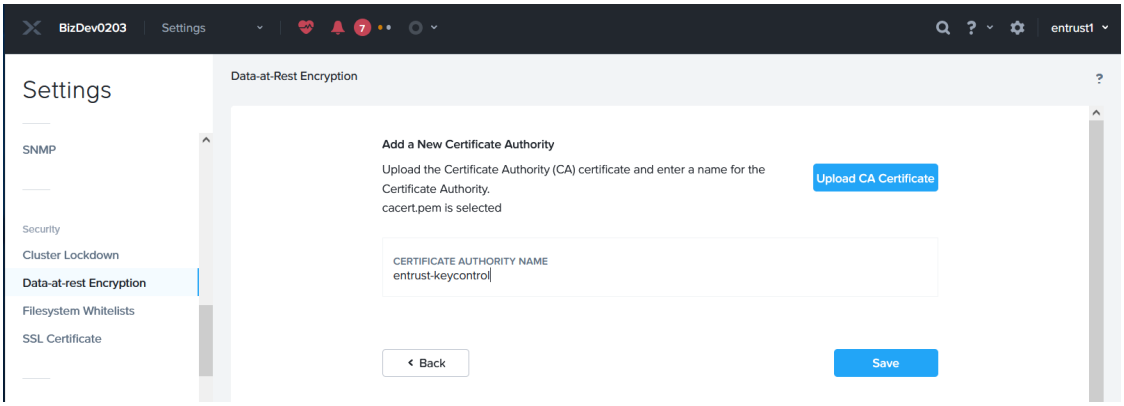
To add KeyControl KMIP cluster to the Nutanix AHV cluster:

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**.

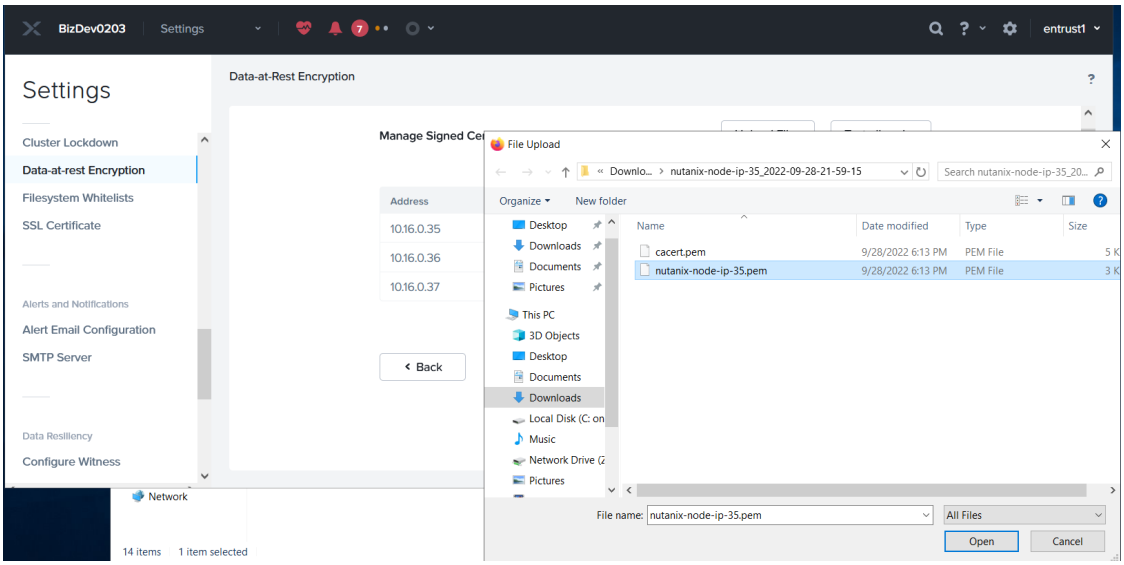


2.7. Add KeyControl KMIP cluster certificates to the Nutanix AHV cluster

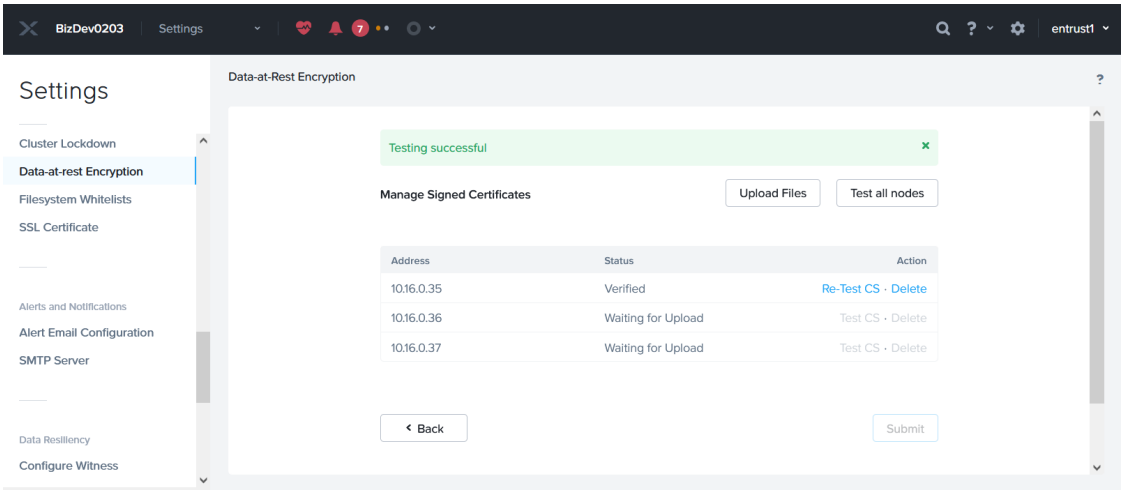
To add KeyControl KMIP cluster certificates to the Nutanix AHV cluster:

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.

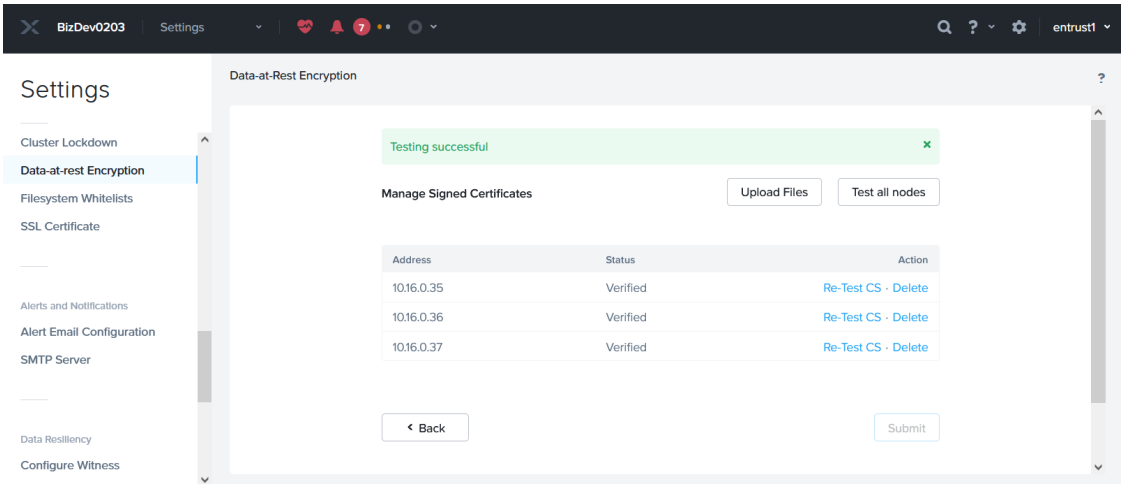
5. Select the **Manage Certificates** hyperlink of the **entrust-keycontrol** cluster. This hyperlink is below **Actions**.
6. Select **Upload Files**, and choose a `username.pem` created above, then select **Submit**.



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



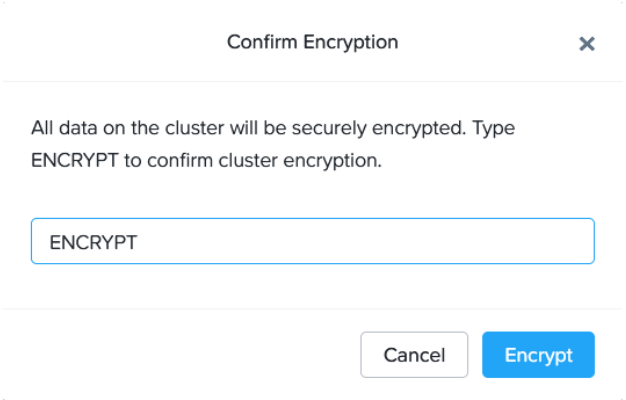
8. Repeat the above for the other nodes.



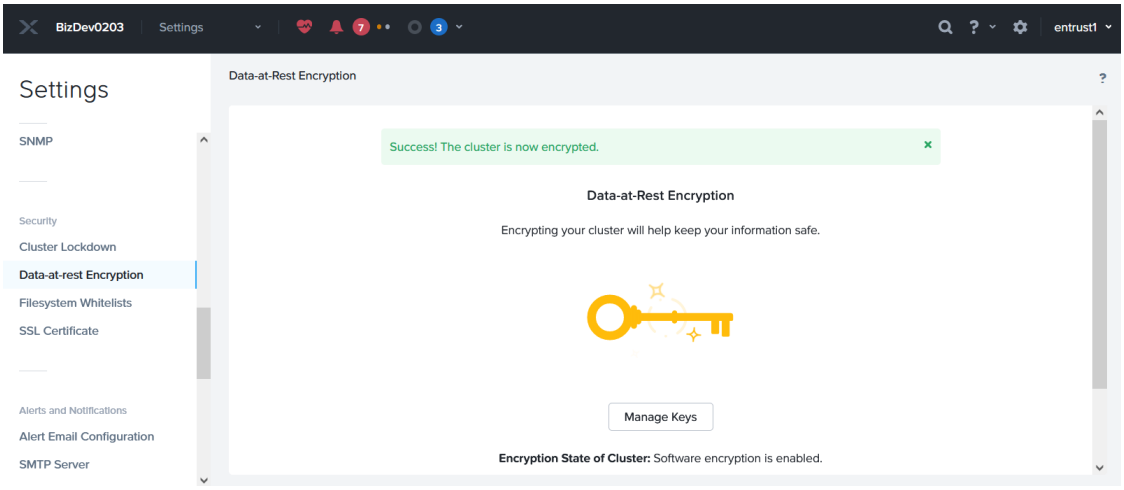
2.8. Enable encryption

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**.



6. The following display confirms that the cluster in now encrypted.


BizDev0203
Settings
entrust1
Settings
SNMP
Security
Cluster Lockdown
Data-at-rest Encryption
Filesystem Whitelists
SSL Certificate
Alerts and Notifications
Alert Email Configuration
SMTP Server
Data-at-Rest Encryption
Success! The cluster is now encrypted.
Data-at-Rest Encryption
Encrypting your cluster will help keep your information safe.
Manage Keys
Encryption State of Cluster: Software encryption is enabled.

3. 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.