# Contents

1. Introduction ............................................................... 3  
   1.1. Product configurations ........................................... 3  

2. Procedures ............................................................... 4  
   2.1. Deploy a KeyControl node ....................................... 4  
   2.2. Select the KeyControl node as Key Management Server and generate the certificate requests ........................................... 4  
   2.3. Create the KMIP client certificate bundles ....................... 7  
   2.4. Add KeyControl as a certificate authority for Nutanix Prism Central ......................... 9  
   2.5. Add a second KeyControl node to the cluster .................. 12  
   2.6. Create the KMIP Client Certificate Bundles in the second KeyControl node .................. 12  
   2.7. Select the second KeyControl node as a second Key Management Server .................. 13  

3. Integrating with an HSM ................................................. 15
1. Introduction

This document describes the configuration of Nutanix Prism Central for integration with the Entrust KeyControl key management solution. Entrust KeyControl can serve as a key manager for storage encryption by using the open standard called the Key Management Interoperability Protocol (KMIP).

Before configuring this integration, familiarize yourself with the features and documentation for Nutanix Prism Central and Entrust KeyControl.

1.1. Product configurations

The following versions have been tested for compatibility:

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nutanix Prism Central</td>
<td>5.20 LTS</td>
</tr>
<tr>
<td>Entrust KeyControl</td>
<td>5.4</td>
</tr>
</tbody>
</table>
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 node.
2. Select the KeyControl node as the Key Management server and generate the certificate requests.
3. Create the KMIP client certificate bundle.
4. Add KeyControl as a Certificate Authority (CA) for Nutanix Prism Central.
5. Add a second KeyControl node to cluster.
6. Create the KMIP Client Certificate Bundles in the second KeyControl node.
7. Select the second KeyControl node as a second Key Management Server.

2.1. Deploy a KeyControl node

Refer to the KeyControl node installation instructions. An OVA template was used to deploy the KeyControl node VM. The OVA template is available at https://my.hytrust.com/s/software-downloads.

2.2. Select the KeyControl node as Key Management Server and generate the certificate requests

1. Log into the Nutanix Prism Central 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.
4. Select **Edit Configuration** or **Continue Configuration**.

5. Select **An external KMS**.

6. Scroll down to **Certificate Signing Request Information**.

   Fill the request form, then select **Save CSR Info**.
7. Select **Download CSRs**.

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

8. The compress **csrs.zip** file is created. Save it locally. Extract the files. Notice that a certificate request was created for each node in the Nutanix Prism Central cluster.
2.3. 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.
3. Select the **Basic** tab. Specify the options that you want to use. Ensure the state is set to **Enabled**.

![KeyControl server UI](image)

4. Select **Apply**. At the prompt, select **Proceed** to confirm the configuration. If this server was already enabled, KeyControl restarts and refreshes its object list.
5. Select the **Client Certificates** tab. Then select **Actions > Create Certificate**.

![Client Certificates options](image)

6. Enter name in the **Create a New Client Certificate** dialog box. This operation will be
repeated for each node in the Nutanix cluster. Choose a name unique per node in the cluster, for example the last octet of the node’s IP address as part of the name.

7. Select **Load File** and select the certificate request from the section above corresponding the particular node. Do not specify a password. Leave it blank.

8. Create certificates for the other nodes.

9. Select a certificate created above. Then select **Actions > Download Certificate**. The KeyControl web UI downloads `<username_datetimestamp>.zip`. Unzip it. It contains a user certification/key file called `username.pem` and a server certification file called `cacert.pem`. 
10. Repeat the step above for the other Nutanix nodes.

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

2.4. Add KeyControl as a certificate authority for Nutanix Prism Central

1. Log into the Nutanix Prism Central web UI.
2. Select the Settings pull-down menu in the toolbar, scroll down and select Settings again.
4. Select Continue Configuration. Scroll down and select Add Key Management Server.
5. Enter the IP address of KeyControl and port. The default port is 5696. Select Save.

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

7. Scroll up to the **Key Management Server** section and select **Manage Certificates**. This is not a button, but plain text in blue font.

8. Select **Upload Files**, select a `username.pem` created above, then select **Submit**.

9. Notice the status for the node corresponding to the selected certificate displaying **Uploaded**. Select **Test CS** and the status should change to **Verified**.
10. Repeat the above for the other nodes. Then select Back.

11. Scroll down in the same pane and select Enable Encryption. Enter the word ENCRYPT to confirm encryption. Then select Encrypt.

12. The following display confirms that the cluster is now encrypted.
2.5. Add a second KeyControl node to the cluster

Deploy a second KeyControl node using the OVA template and instructions described above. Then add the newly created KeyControl Node to the existing cluster.

2.6. Create the KMIP Client Certificate Bundles in the second KeyControl node

Nutanix treats each node in the KeyControl cluster as an independent KMIP server. Therefore, you must create a KMIP client certificate bundle at each KeyControl node. You can use the certificate signing request created in the Nutanix cluster above to create the bundles at each KeyControl node.

Follow the steps in Create the KMIP client certificate bundles to create the second KeyControl node. Notice the resulting bundles in the KeyControl cluster.
2.7. Select the second KeyControl node as a second Key Management Server

1. Log into the Nutanix Prism Central web UI.
2. Select the **Settings** pull-down menu in the toolbar, scroll down and select **Settings** again.
3. Select **Data-at-rest Encryption** under **Security** on the **Settings** left pane.
4. Select **Continue Configuration**. Scroll down and select **Add Key Management Server**.
5. Enter the IP address of the second KeyControl node and port. The default port is 5696. Select **Save**.

6. Notice both KeyControl nodes listed as Key Management Servers.

7. Select **Manage Certificates** above for the second KeyControl node.
8. Select **Upload Files**, select a `username.pem` created above for the second KeyControl node, then select **Submit**.
The system does not complain if the selected certificate is that of the first KeyControl node. However, the high availability (HA) functionality might not work in some scenarios.

9. Notice the status for the node corresponding to the selected certificate displaying **Uploaded**. Select **Test CS** and the status should change to **Verified**.

10. Repeat the above for the other Nutanix nodes.
3. Integrating with an HSM

You can use a hardware security module (HSM) to establish a root of trust for your encryption keys. For guidance on integrating Entrust KeyControl with an HSM, consult with your HSM vendor. If you are using an nShield HSM, refer to the *Entrust KeyControl nShield HSM Integration Guide* available in the Entrust documentation library.