Nutanix Prism Central and Entrust KeyControl

with nShield® HSM Integration Guide
Contents

1. Introduction .................................................. 4
   1.1. Product configurations .................................. 4
   1.2. Supported nShield hardware and software versions ............... 4
   1.3. Requirements ..................................................... 4
2. Procedures ..................................................... 6
   2.1. Deploy a KeyControl node .................................. 6
   2.2. Select the KeyControl node as Key Management Server and generate the certificate requests .................. 7
   2.3. Create the KMIP client certificate bundles ...................... 9
   2.4. Add KeyControl as a certificate authority for Nutanix Prism Central ................. 12
   2.5. Add a second KeyControl node to the cluster .................. 15
   2.6. Create the KMIP Client Certificate Bundles in the second KeyControl node ............ 15
   2.7. Select the second KeyControl node as a second Key Management Server .......... 16
   2.8. Configure access to the nShield HSM ........................ 17
   2.9. Configure the KeyControl nodes as clients of the HSM ............ 17
   2.10. Enable KMIP service and KMIP key wrapping ................. 21

Contact Us .................................................................. 23
1. Introduction

This document describes the configuration of Nutanix Prism Central for integration with the Entrust KeyControl (formerly HyTrust KeyControl) key management solution with an Entrust nShield® hardware security module (HSM) root of trust. Nutanix solutions are compatible with the HyTrust Entrust KeyControl solution. Entrust KeyControl can serve as a key manager for storage encryption by using the open standard called the Key Management Interoperability Protocol (KMIP).

1.1. Product configurations

We have successfully tested the integration with the following versions:

<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>

1.2. Supported nShield hardware and software versions

We have successfully tested the integration with the following nShield HSM hardware and software versions:

<table>
<thead>
<tr>
<th>Product</th>
<th>Firmware</th>
<th>Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect XC</td>
<td>FIPS 12.50.11</td>
<td>12.60.10</td>
</tr>
</tbody>
</table>

1.3. Requirements

Familiarize yourself with:

- The Nutanix Prism Center features and documentation.
- The Entrust KeyControl features and documentation.
- The Entrust nShield HSM documentation.

A remote nShield HSM was used in the test environment. It was configured by the HSM administrator at Entrust.

Installation and configuration instructions for the HSM located on-site, remotely, or remotely via the serial console are available in the following nShield Support articles, and the Installation Guide for the HSM:
• https://nshieldsupport.entrust.com/hc/en-us/articles/360021378272-How-To-Locally-Set-up-a-new-or-replacement-nShield-Connect
• https://nshieldsupport.entrust.com/hc/en-us/articles/360014011798-How-To-Remotely-Setup-a-new-or-replacement-nShield-Connect
2. Procedures

This interop testing was performed in the Nutanix lab. All access to the lab was via a Microsoft Windows virtual desktop infrastructure (VDI). From this VDI we accessed a VMware ESXi vSphere server through its web UI. This ESXi server was made available for us to deploy the KeyControl nodes as virtual machines (VM). A Nutanix Prism Central cluster comprised of three nodes was also available to us via its web UI from the VDI. This Nutanix Prism Central cluster was deployed in a different hardware than the ESXi server.

The nShield HSM was located at Entrust. The Nutanix lab provided a public IP for each of the two KeyControl nodes we created. The Entrust IT department made the necessary configuration to allow enrollment of the KeyControl nodes located in the Nutanix lab as client of the HSM located at Entrust.

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.
8. Configure access to the nShield HSM.
9. Configure the KeyControl Nodes as clients of the HSM.

To pass functional compatibility and obtain a Nutanix Ready badge, you can execute the test cases from the KMS Validation Test Kit from Nutanix. The tests include retrieving a private-public key pair (KEK) under various fail-over scenarios and validating with re-keys. This guide does not describe the test cases or their execution.

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.
3. Select **Data-at-rest Encryption** under **Security** on the **Settings** left pane.
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.
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**.

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. We used 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.
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 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.

### 2.8. Configure access to the nShield HSM

This integration was performed in the Nutanix lab. The HSM was remote to the KeyControl nodes, behind the Entrust corporate firewall. It was not on the same network as the KeyControl nodes, neither was it an nShield as a Service (nSaaS) configuration. The Entrust firewall was configured to allow access from the public IP addresses of the KeyControl nodes in the Nutanix lab. The HSM was configured to accept the public IP addresses of the KeyControl nodes in the Nutanix lab as clients.

1. Obtain the public IP of the KeyControl nodes. Each KeyControl node was given a unique public IP in the Nutanix lab.

2. Have the nShield HSM firewall admin, in this case the Entrust IT department, allow connection from the IPs above.

3. Have the nShield HSM admin, in this case Entrust, allow enrollment from the IPs above.

4. Request the world and module files of the HSM. It is provided as a *.zip* file.

5. Copy the *.zip* file to the Nutanix lab access Win10-PartnerVDI computer.

### 2.9. Configure the KeyControl nodes as clients of the HSM

1. Log in to the web UI of either of the KeyControl nodes using an account with Security Admin privileges.

2. Select **Settings > HSM Server Settings**. Select **nCipher nShield Connect HSM**

3. Select **Initialize** and then **OK**.
4. Select **Complete Setup** and then **Continue**.

---

**nCipher Clients**

There were 2 nCipher clients initialized.

---

**Next Step**

In the Client List, the IP addresses and key hashes of all the clients are listed. These need to be sent to the HSM Administrator.

Note: You may skip this step if you are using nShield as a Service where the details are NOT needed to be sent to the HSM Administrator.

- Copy IP addresses and key hashes to clipboard

---

**What's next?**

After giving the IP addresses and key hashes to the HSM Administrator (not needed for nShield as a Service), you will receive a Security World Bundle. At this point, the remaining setup workflow can be started.

The following information will be needed to complete the setup:

- The following server details: Server Name/FQDN, Server IP, ESN, Port and Key Hash.
- The Security World Bundle file that is provided by the HSM Administrator.
- Create softcard information consisting of Label and Password.

---

Ok
Before continuing with the setup, the IP Addresses and Key Hashes should have been given to the HSM Administrator (not needed for nShield as a Service) and in return, the HSM Administrator should have provided a Security World Bundle. With this bundle, you should have what you need to finish setting up the HSM server.

The following is needed to complete the setup:

- The following server details: Server Name/FQDN, Server IP, ESN, Port and Key Hash.
- The Security World Bundle file that is provided by the HSM Administrator.
- Create softcard information consisting of Label and Password.

5. Enter the HSM info. Then select **Enroll and Continue**.
6. Select Load File. Then select the .zip file from above containing the world and module files for the HSM. Then select Upload and Continue.

```markdown
nShield HSM Server Setup

Get Started  Enrollment  Security World  Softcard

Upload Security World Bundle

A security world bundle file needs to be provided from the HSM Administrator. Upload this file in order to enroll the KeyControl nodes.

SecurityWorldFiles.zip

Cancel  Upload and Continue
```

7. Enter the Softcard details, then select Complete Setup.

```markdown
nShield HSM Server Setup

Get Started  Enrollment  Security World  Softcard

Create Softcard

Create a label and passphrase to link to the HSM Server.

⚠️ Keep a record of the softcard label and password. These will both be needed during a Master Key Recovery (MKR).

Softcard Label *

hmssoftcard

Softcard Password *

******

Cancel  Complete Setup
```

8. Notice the nCipher State is ENABLED.

Select Test.
9. The following confirms the KeyControl node is now ready to use the HSM.

Both KeyControl nodes in the cluster are now clients of the HSM. You do not need to repeat the configuration steps for the other KeyControl node.

2.10. Enable KMIP service and KMIP key wrapping

Configure KMIP to use the HSM by enabling the HSM in the KMIP settings.

1. In the top menu bar, select **KMIP > Basic**.

2. In the **KMIP Key Wrapping** field, select **System HSM (nShield Connect HSM: xxx.xxx.xxx.xxx)**.

3. In the **HSM Root Key Label** field, enter a unique name for the HSM Root Key.
4. In the **KEK Cache Timeout** field, enter how long you want KeyControl to cache the HSM-derived Key Encryption Keys (KEKs).

   The maximum length is 24 hours. If you set the parameter to 0, no cache is used and KeyControl has to use the HSM every time. If you want to use caching, select a value according to your organization’s security policies.

5. Select **Apply**.

To confirm that KeyControl uses the HSM, check for the following messages in the KeyControl Audit Logs:

- **System, Successfully generated Key Encryption Key on HSM**
- **Successfully enabled encryption of KMIP objects**
## Contact Us

<table>
<thead>
<tr>
<th><strong>Web site</strong></th>
<th><a href="https://www.entrust.com">https://www.entrust.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Support</strong></td>
<td><a href="https://nshieldsupport.entrust.com">https://nshieldsupport.entrust.com</a></td>
</tr>
<tr>
<td><strong>Email Support</strong></td>
<td><a href="mailto:nShield.support@entrust.com">nShield.support@entrust.com</a></td>
</tr>
<tr>
<td><strong>Online documentation:</strong></td>
<td>Available from the Support site listed above.</td>
</tr>
</tbody>
</table>

You can also contact our Support teams by telephone, using the following numbers:

### Europe, Middle East, and Africa

- **United Kingdom:** +44 1223 622444  
  One Station Square  
  Cambridge, UK CB1 2GA

### Americas

- **Toll Free:** +1 833 425 1990
- **Fort Lauderdale:** +1 954 953 5229  
  Sawgrass Commerce Center – A Suite 130  
  13800 NW 14 Street  
  Sunrise, FL 33323 USA

### Asia Pacific

- **Australia:** +61 8 9126 9070  
  World Trade Centre Northbank Wharf Siddeley St  
  Melbourne VIC 3005 Australia
- **Japan:** +81 50 3196 4994
- **Hong Kong:** +852 3008 3188  
  31/F, Hysan Place,  
  500 Hennessy Road,  
  Causeway Bay
ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they’re crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it’s no wonder the world’s most entrusted organizations trust us.