



Hitachi VSP G & E Series

KeyControl® Integration Guide

20 Oct 2022

Contents

| | |
|--|----|
| 1. Introduction | 3 |
| 1.1. Product configurations | 3 |
| 1.2. Requirements | 3 |
| 2. Procedures | 4 |
| 2.1. Deploy a KeyControl cluster | 4 |
| 2.2. Specify an LDAP/AD authentication server | 4 |
| 2.3. Enable KMIP | 6 |
| 2.4. Create tenant | 7 |
| 2.5. Add x509v3 extensions to the OpenSSL configuration file | 8 |
| 2.6. Create CSR | 8 |
| 2.7. Create tenant client certificate bundle | 9 |
| 2.8. Convert tenant client certificate to PKCS #12 format | 11 |
| 2.9. Import tenant client certificate into the VSP | 13 |
| 2.10. Configuration to support the Hitachi VSP | 13 |
| 2.11. Execute tests | 13 |
| 3. Integrating with an HSM | 14 |

1. Introduction

This document describes the integration of the Hitachi Virtual Storage Platform (referred to as VSP in this guide) with the Entrust KeyControl 5.5.1 (formerly HyTrust KeyControl) key management solution. Entrust KeyControl (referred to as KeyControl in this guide) serves as a key manager for storage encryption by using the open standard Key Management Interoperability Protocol (KMIP).

1.1. Product configurations

Entrust has successfully tested the integration of KeyControl with VSP in the following configurations:

| System | Version |
|--------------------|---------|
| Entrust KeyControl | 5.5.1 |

1.2. Requirements

Before starting the integration process, familiarize yourself with:

- The documentation and set-up process for the Hitachi VSP G & E Series family of products in the [Hitachi Vantara online documentation](#).
- The documentation and set-up process for Entrust KeyControl, see [Entrust KeyControl Product Documentation](#).
- Also see [Entrust DataControl and KeyControl v5.5.1 Online Documentation Set](#).

2. Procedures

Follow these steps to install and configure KeyControl with VSP.

- [Deploy a KeyControl cluster](#)
- [Specify an LDAP/AD authentication server](#)
- [Enable KMIP](#)
- [Create tenant](#)
- [Create tenant client certificate bundle](#)
- [Add x509v3 extensions to the OpenSSL configuration file](#)
- [Create CSR](#)
- [Create tenant client certificate bundle](#)
- [Convert tenant client certificate to PKCS #12 format](#)
- [Import tenant client certificate into the VSP](#)
- [Configuration to support the Hitachi VSP](#)
- [Execute tests](#)

2.1. Deploy a KeyControl cluster

This deployment consists of two nodes.

1. Download the KeyControl software from <https://my.hytrust.com/s/software-downloads>. This software is available both as an OVA or ISO image. The OVA installation method in VMware is used in this guide for simplicity.
2. Install KeyControl as described in [KeyControl OVA Installation](#).
3. Configure the first KeyControl node as described in [Configuring the First KeyControl Node \(OVA Install\)](#).
4. Add second KeyControl node to cluster as described in [Adding a New KeyControl Node to an Existing Cluster \(OVA Install\)](#).



Both nodes need access to an NTP server, otherwise the above operation will fail. Log in the console to change the default NTP server if required.

5. Install the keyControl license as described in [Managing the KeyControl License](#).

2.2. Specify an LDAP/AD authentication server

1. Log into the KeyControl webGUI using an account with Security Admin privileges.

2. Select **Settings** in the top menu bar.
3. Select **Authentication** in the **General Settings** pane.
4. Select **LDAP** in the **Type** drop-down box.
5. Enter your account info on the **Domain** tab and then select **Apply**.

General Settings ×

KeyControl Account Admin Key Parts Audit Log **Authentication** Mail Server Session Timeout SSL Configuration

Type:
LDAP

Domain Domain Controllers

Domain Name: ⓘ interop.com

Service Account Name: ⓘ keycontrol

Service Account Password: ⓘ ⓘ

UID Attribute: ⓘ 123

Apply

6. Select **Add Domain Controller** in the **Domain Controllers** tab.
7. Select **LDAP** in the **Server URL** drop-down box.
8. Enter a **Server URL**, **User Search Context**, and **Group Search Context**. Then select **Save and Close**.

The user and group search context can be found by running the following command lines on a terminal in the required domain:

```
dsquery user -name <known username> dsquery group -name <known group name>
```

For example:

```
C:\Windows\system32>dsquery user -name "Hitachi VSP"
"CN=Hitachi VSP,CN=Users,DC=interop,DC=com"
```

Edit Domain Controller interop.com ✕

Server URL: ⓘ
 LDAP://

STARTTLS: ⓘ

CA Certificate: ⓘ

Certificate needs to be in base64 encoded pem format. Required if STARTTLS or LDAPS is selected.

[Hide Advanced settings](#)

User Search Context (Base DN): ⓘ

Group Search Context (Base DN): ⓘ

Timeout: ⓘ

Minimum value of 1 second, max 15.

Notice the added domain controller.

General Settings ✕

[KeyControl Account](#)
[Admin Key Parts](#)
[Audit Log](#)
[Authentication](#)
[Mail Server](#)
[Session Timeout](#)
[SSL Configuration](#)

Type:

Domain [Domain Controllers](#)

ⓘ Important: The order in which the entries appear determines the order of precedence if there is a connection timeout. +

| <input type="checkbox"/> | Server URL | User Base DN | Group Base DN | Timeout |
|--------------------------|--------------------|-------------------|-------------------|---|
| <input type="checkbox"/> | ldap://interop.com | DC=interop,DC=com | DC=interop,DC=com | 5 seconds <input type="button" value="up"/> <input type="button" value="down"/> |

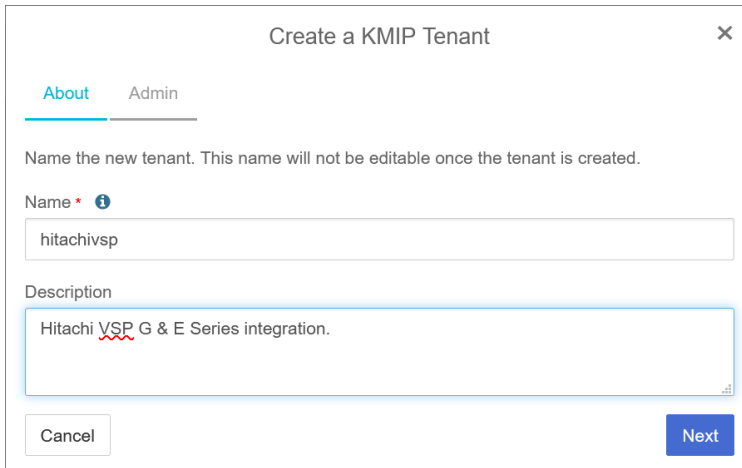
See the following link for additional information [Specifying an LDAP/AD Authentication Server](#).

2.3. Enable KMIP

1. Select **KMIP** in the menu bar in the KeyControl webGUI.
2. Select the **Settings** tab.
3. For **State**, select **Enable**. Then select **Apply**.
4. In the **Overwrite all existing KMIP Server settings?** dialog, select **Proceed**.

2.4. Create tenant

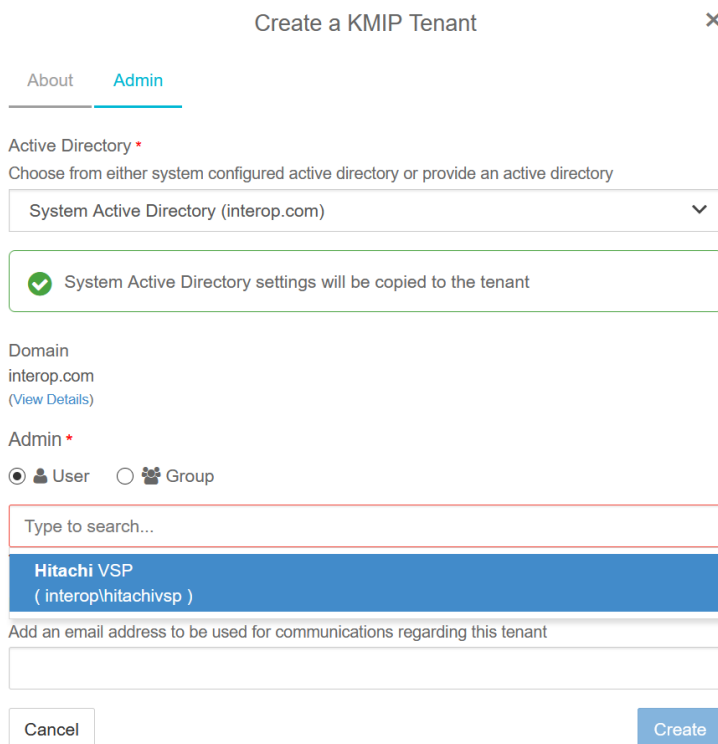
1. Select **KMIP** in the menu bar in the KeyControl webGUI.
2. Select the **Tenants** tab.
3. Select **Actions > Create a KMIP Tenant**.
4. Enter the name and description. Then select **Next**.



The screenshot shows a dialog box titled "Create a KMIP Tenant" with a close button (X) in the top right corner. Below the title bar are two tabs: "About" (selected) and "Admin". The main content area contains the following elements:

- A text instruction: "Name the new tenant. This name will not be editable once the tenant is created."
- A "Name" field with a red asterisk and an information icon. The text "hitachivsp" is entered.
- A "Description" field with the text "Hitachi VSP G & E Series integration." The word "VSP" is underlined in red.
- At the bottom, there are two buttons: "Cancel" on the left and "Next" on the right.

5. On the **Admin** tab, select the Active Directory.
6. Enter the required user in the search box.
7. Enter email address and select **Create**.



The screenshot shows the same dialog box, but with the "Admin" tab selected. The content is as follows:

- Two tabs: "About" and "Admin" (selected).
- A section titled "Active Directory" with a red asterisk. Below it is the instruction: "Choose from either system configured active directory or provide an active directory".
- A dropdown menu showing "System Active Directory (interop.com)".
- A green-bordered box with a checkmark icon and the text: "System Active Directory settings will be copied to the tenant".
- A "Domain" section with the text "interop.com" and a link "(View Details)".
- An "Admin" section with a red asterisk. It has two radio buttons: "User" (selected) and "Group".
- A search box with the placeholder text "Type to search...". Below it, a blue dropdown menu is open, showing "Hitachi VSP (interop/hitachivsp)".
- An instruction: "Add an email address to be used for communications regarding this tenant" above an empty text input field.
- At the bottom, there are two buttons: "Cancel" on the left and "Create" on the right.

See the following link for additional information [Creating a KMIP Tenant](#).

2.5. Add x509v3 extensions to the OpenSSL configuration file

The VSP requires the x509v3 extensions in the client certificate. KeyControl will generate the client certificate based on the client certificate request (CSR). As a result the CSR must contain the x509v3 extensions.

OpenSSL was used in this integration to generate the CSR. The following steps configure OpenSSL to generate a CSR with the x509v3 extensions.

1. Display the version of OpenSSL:

```
# /usr/local/bin/openssl version
OpenSSL 3.0.3 3 May 2022 (Library: OpenSSL 3.0.3 3 May 2022)
```

2. Edit `/usr/local/ssl/openssl.cnf`.
3. Add the following lines to the **[req]** section:
 - `req_extensions = v3_req`
 - `x509_extensions = usr_cert`
4. Un-comment the following lines in the **[usr_cert]** section:
 - `keyUsage = nonRepudiation, digitalSignature, keyEncipherment`
 - `extendedKeyUsage = critical,timeStamping`
5. Add the following line to the **[v3_req]** section:
 - `keyUsage = nonRepudiation, digitalSignature, keyEncipherment`
 - `extendedKeyUsage = serverAuth, clientAuth, codeSigning, emailProtection`

2.6. Create CSR

1. Create a key:

```
# /usr/local/bin/openssl genrsa -out svp.key 2048
```

2. Create a CSR from the key above:

```
# /usr/local/bin/openssl req -new -config /usr/local/ssl/openssl.cnf -key svp.key -out svp.csr
```

3. Notice the CSR contains the x509v3 extensions:

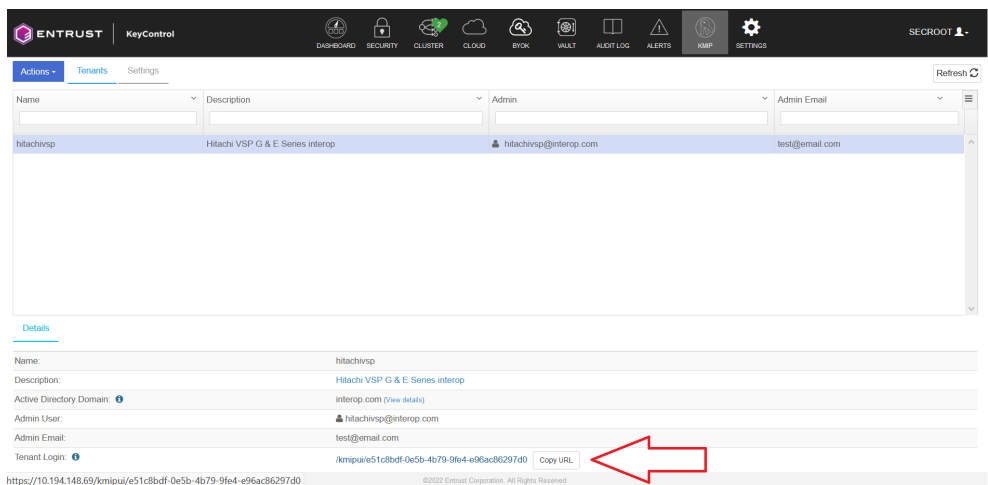

```

# openssl req -text -noout -verify -in svp.csr
verify OK
Certificate Request:
  Data:
    Version: 1 (0x0)
    ...
    Requested Extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Key Usage:
        Digital Signature, Non Repudiation, Key Encipherment
      X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication, Code Signing, E-mail Protection
    ...

```

2.7. Create tenant client certificate bundle

1. Select **KMIP** in the menu bar in the KeyControl webGUI.
2. Select the **Tenants** tab.
3. Highlight the required tenant.
4. Select the link on **Tenant Login**. A new tab in the browser opens.



5. Log in with the tenant credentials.



KeyControl

KMIP Sign In

User Name

hitachivsp@interop.com

Password

●●●●●●●●

SIGN IN

6. Select **Security** > **Client Securities**.
7. Select the **+** icon on right top corner to create new client certificate.
8. Specify the options and then select **Create**.

Create Client Certificate ✕

Certificate Name *

hitachivsp

Certificate Expiration *

May 19, 2023

Certificate Signing Request (CSR)

svp.csr **Browse**

Encrypt Certificate Bundle

Certificate Password *

●●●●●●

Confirm Password *

●●●●●●

[Cancel](#) **Create**

9. Select the certificate bundle you created and select **Download**.

Certificate Details



Name **hitachivsp**
Expiration **May 19, 2023, 1:14:46 PM**
Expires In (Days) **365**
Certificate Generated From External CSR **✔ Yes**

Download

Close

See the following link for additional information [KMIP Tenant Client Certificates](#).

2.8. Convert tenant client certificate to PKCS #12 format

1. Extract the **hitachivsp.pem** file from the tenant client certificate bundle zip file created in [Create tenant client certificate bundle](#). Save the **cacert.pem** file for use in [Import tenant client certificate into the VSP](#).

| Name | Size | Packed Size | Modified | Attributes | Encrypted | CRC | Method | Host OS | Version | Volume I... |
|----------------|-------|-------------|------------------|------------|-----------|----------|---------|---------|---------|-------------|
| cacert.pem | 4 710 | 2 491 | 2022-05-19 17:14 | 0rw----- | - | D246423D | Deflate | Unix | 20 | 0 |
| hitachivsp.pem | 4 903 | 2 722 | 2022-05-19 17:14 | 0rw----- | - | E95AD1FE | Deflate | Unix | 20 | 0 |

2. Convert to PKCS #12 format using OpenSSL:

```
# /usr/local/bin/openssl pkcs12 -export -out hitachivsp.p12 -in hitachivsp.pem -inkey svp.key -passin pass:hitachi -passout pass:hitachi
```

3. View the content of PKCS #12 formatted tenant client certificate bundle:

```

## /usr/local/bin/openssl pkcs12 -in hitachivsp.p12 -info -nodes
Enter Import Password:
MAC: sha256, Iteration 2048
MAC length: 32, salt length: 8
PKCS7 Encrypted data: PBES2, PBKDF2, AES-256-CBC, Iteration 2048, PRF hmacWithSHA256
Certificate bag
Bag Attributes
    localKeyID: 39 7C CD 50 10 5A D1 08 F4 1D 36 5D EC 2C 9F D4 03 DF 09 7F
subject=C = US, ST = Florida, L = Sunrise, O = Entrust, OU = Testing, CN = Interop, emailAddress = test@entrust.com
issuer=C = US, O = HyTrust Inc., CN = HyTrust KeyControl Certificate Authority
-----BEGIN CERTIFICATE-----
MIIEGzCCAwOgAwIBAgIERWmATANBgkqhkiG9w0BAQsFADBXMQswCQYDVQGEwJV
UzEVMBMGAlUEChMMSH1UcnVzdCBJbmMuMTEwLWYDVQDEYhIeVRYdXN0IEtleUNv
bnRyb2wgQ2VydG6lmaWNhdGUgQXV0aG9yaXR5MjB4XDIyMDUxOTE3MTQ0N1oXDTIz
MDUxOTE3MTQ0N1owYgxCzAJBgNVBAYTAlVTMRAdDgYDVQIDAdG6G9yaWRhMRAw
DgYDVQIDAdTdw5aXNlMRAdDgYDVQIDAdFbnRydXN0MRAdDgYDVQIDAdUZXR0
aW5nMRAdDgYDVQIDAdJbnRlcm9wMR8wHQYJKoZIhvcNAQkBFhB0ZXN0QG9udHJ1
c3QuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA4lspigtffsEm
AQTYNlXeIvo8rG9AOPampKNJ6vZyZUmMjXlthh1LZC4YL0png2KPCRRMgzhlavP
Xd71ygtSF+Y2nK0y3zTfxVn/60XpsfiPqIKrvBfkLoBOJ1RBP5X0b7DTHqTafZ4E
9I+FLPLXfqi/UGyaNUOgrfVehszZbnT07N3W8Ib1KszSdCma8Z7B05xeHQqG9E+9
qembYLHmhMYj8Ce+d5Jy+N5FKGwnyNH12Az+WALcLTPpnEE5LSPk4DHGrj2jBow
KUdohIRKTYN50S7nq66YztSkdsrLZ04IYrmv+5ajkveqbCU5Ryv0tLSVpzOnkLm+
8TrxBueGpQIDQABo4G8MI65MAKGA1UdEwQCAAAwLAYJYIZIAyb4QgENBB8WHU9w
ZW5TU0wgR2VuZCJhdGVkIENlcnRpZmZlYXR1bG0GA1UdDgQWBERTUd8eezyJhW6A
d0t8tJxR+JfITjAfBgNVHSMGDAWgBTZyL94G7MoJrAs23seS670EqowTALBgND
HQ8EBAMCBAwMQYDVR0LBComKAYIKwYBBQUHAWGECsGAQUFBwMCGgrBgEFBQcD
AwYIKwYBBQUHAWQwDQYJKoZIhvcNAQELBQADggEBAM1gRZK6jWTQARyEoqDyhPkW
6evJzmIpwZohSeN+iDHGp8yU8SwM5YaFyihKTCePIy5xNtz1R30701S1hdqVX0FqQ
ioSOKuS75mvIS/cQ90wFST0ge3qnC7kEqj8XtXrNTJM7FoOWGFkKk/8IBtNbKnNL
wr6KJr0TmFoYUf2OUYC3RByvdzJ3xs2VMVITuXgviUw1ZVV/OJpNL1Tdmxh9Ii2h
qhIQujcu3MQ/teaWn+K4FDMqL5xVFCsYAF0fy62Z8M9jFsKfNjTHQ99uqYNTxGp
bruaJADx74yNn3F10pjFjJmP869gtfN3tBp1evYCBQTOQMObE13dUn2FU990DQY=
-----END CERTIFICATE-----
PKCS7 Data
Shrouded Keybag: PBES2, PBKDF2, AES-256-CBC, Iteration 2048, PRF hmacWithSHA256
Bag Attributes
    localKeyID: 39 7C CD 50 10 5A D1 08 F4 1D 36 5D EC 2C 9F D4 03 DF 09 7F
Key Attributes: <No Attributes>
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDiWymKC19+wSYB
BNg2Vd6W+Jysb0A48Cako0nq9nJrNSYwLcu2GHUtkLhgvSmeDY08JEwyDOGvpu9d
3vXKC2wX5jaco7LfNN/Fwf8bRemx+I+ogqu8F+QugE4nVEE+xc5vsNmepNp9ngT0
j4Us+Vd+qL9QbJo1Q6Ct9VygZNLudPTs3dbwhUqzNJ0IxrXnsE7nF4c6ob0T72p
6ZtgseaExgmLwJ753knL43kUoZafI0eXYDP5YCVxMs+mcQTktI+TgMcauPaMgJAp
R2geJEphM3nRlueobpj01KR2ystnTghua/7Lq0S96psJTLHK860tJWnM6eQub7x
0vEG54a1AgMBAECggEAaGLG6jA6fsr2CrXANXa0KxQfjQPVGyzstTo0aW3zwcSh
jJpYEobe6v91d+9kVOYrnKakmORF1+wfwMvsj5uK4s6g2sXHRJYup+Vj9yDbr95P
6ccxCZH/Ac7bu9LoKVmxZOKnydb+h7Wq1VmmceIfDmMLryIWT3/7hp3DaMrpbr0U
+t0bN0DNSiU0+0hWXff63muW5WebEtrEAmrROgd+5TLhustVujiggKTeB8WGOSLz
kaLzPVjkfIOU6RDTzJexSK+It7uciaAPbvCwtoCcaGqKw+qw899tZnw1S1x46mxB
FBUqiUPjLXDctfPftsUU4zyZMd6/L/nke1NuroqIQKBgQDyHTEEQ8wNFMBIBJW
+sIiBHEbJNZ81WOW50+A5DR/9LRKBKsQ5G53gP6cK9zfyOMCZctZtIxwHipMhP8
YOAH+X8pPLAFJF6ic4B+A9DxbFCZLP3/Tr8Gv3Mh5TmtoJXk1IYfBDSAr5HQf5
pdC9VI8zccq9HLfWq9b0IixnFPQKBgQDvVpQ79JWGxjmrq5ZNYIe5mf9U4koFugw6
UwvhCGKx0TSo1haWLVSG1pONVU21Di8te9uI08rLwsBgId097xya6SWE7ekX6fC
Arj+AQEsCay6TdSfILDDeoM0YkSYnLokaoJ/9kzz4PIHT1N4uSe01Di0KkrEVxyOt
pRHY18ptiQKBgBY+Uv4F5zRRiLUSpDyzevRvDgkLYD3FXXVf2fn6D+MLM2b+XIDR
EGFYIVt4N6mJph+BRKZwLPrb+pzfFySdeKlR6YYej9usPcRgViS9qwOTJPB9rrQ
3AtvW2PgDPEJUX5EPaWcOfTi/tSGM0ZfUocibqmwXr4WN6SmQC47twAogBALB
0sGpWsa1/wV6KXRnqm3sDI9J19JVpV6n6Us1Nv8yumYty+Nyy7eGg/cKMr3AMLP
aWxKpPEATHz4HFGcxNK90RJthG6xQDdRpsWM0noPU+pfLDhgozk5pdaxnJ1lb2y
Z1iepjC8yzm/1AQuipmhoH0RVE1X2Y0Pp1fnWDhZAoGABV/Ne1oaXJT2gEgAXCm
QLco/VfKaFFyIv/pViEPcW3W4p05+AaVmSff8gid4VJ6YNIH2cbszaMwUnRKnzHy
89uLN01aVMEbjN0GJkqZUb18YaOyI8pg1wzDrVhpoV9CNWQPq/J9WytVyYfmfLLr
e2DXuNht5BmG7ouca7XEnU0=
-----END PRIVATE KEY-----

```

2.9. Import tenant client certificate into the VSP

1. Import the `hitachivsp.p12` and `cacert.pem` certificates into the VSP as required.
2. You can now use standard API calls to interact with KeyControl.

2.10. Configuration to support the Hitachi VSP

A change to KeyControl configuration file is required to support the Hitachi VSP. Contact Entrust customer support so they can perform this change remotely.

Once the KeyControl server instance is configured for the Hitachi VSP, it may not work with other KMIP client integrations. A separate KeyControl instance may be required to support other clients.

2.11. Execute tests

Execute the test as described in Hitachi's internal documentation.

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](#).