Pure Storage FlashArray and Entrust KeyControl

Integration Guide

2025-02-10

Table of Contents

Chapter 1. Introduction

This document describes the integration of Pure Storage FlashArray with the Entrust KeyControl key management solution (KMS). Entrust KeyControl serves as a key manager for cloud keys and KMIP objects.

1.1. Product configurations

Entrust has successfully tested the integration of Entrust KeyControl with Pure Storage FlashArray in the following configurations:

System	Version
Pure Storage	FA-X10R2 v6.6.1
KeyControl	10.4.1

1.2. Requirements

Before starting the integration process, familiarize yourself with the Pure Storage FlashArray and Entrust KeyControl documentation:

- Pure Storage Documentation portal
- Entrust KeyControl online documentation

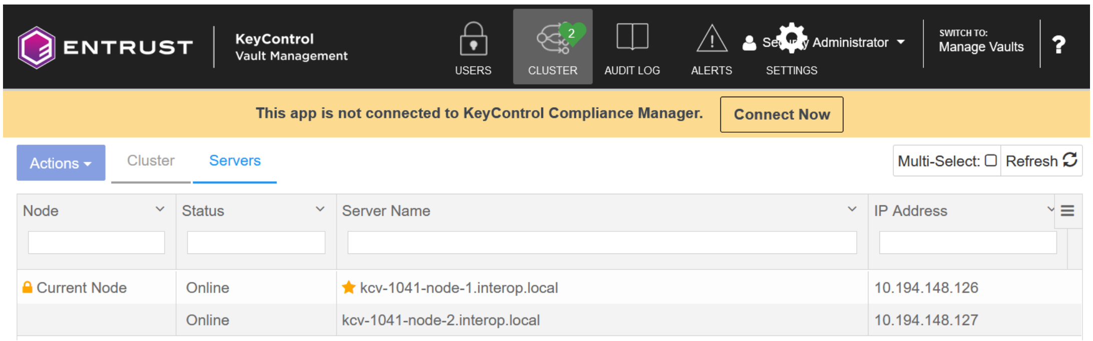
Chapter 2. Deploy KeyControl

2.1. Deploy a KeyControl cluster

For the purpose of this integration, a two-node cluster was deployed as follows:

1. Download the KeyControl software from Entrust TrustedCare. This software is available as an OVA or ISO image. This guide deploys an OVA installation.
2. Install the Entrust KeyControl software as described in KeyControl OVA Installation.
3. Configure the first Entrust KeyControl node as described in Configuring the First KeyControl Node (OVA Install).
4. Add a second Entrust KeyControl node to the 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. Sign in to the console to change the default NTP server if needed.

   This app is not connected to KeyControl Compliance Manager. Connect Now

Node	Status	Server Name	IP Address
Current Node	Online	★ kcv-1041-node-1.interop.local	10.194.148.126
	Online	kcv-1041-node-2.interop.local	10.194.148.127

5. Install the Entrust KeyControl license as described in Upgrading Your Trial License.

2.2. Additional Entrust KeyControl cluster configuration

After the KeyControl cluster is deployed, additional system configuration can be done as described in KeyControl System Configuration.

2.3. Configure authentication

This guide uses local account authentication.

For AD-managed Security groups, configure the LDAP/AD Authentication Server as described in Specifying an LDAP/AD Authentication Server.

2.4. Create DNS record for the Entrust KeyControl cluster

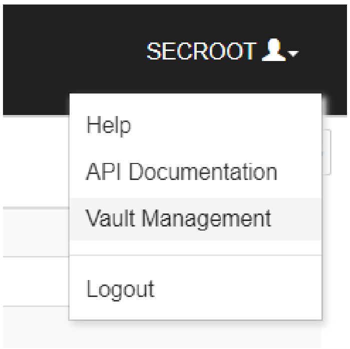
This guide uses the individual IP addresses of the Entrust KeyControl nodes.

To use hostnames, configure your DNS server giving each node in the KeyControl a unique name.

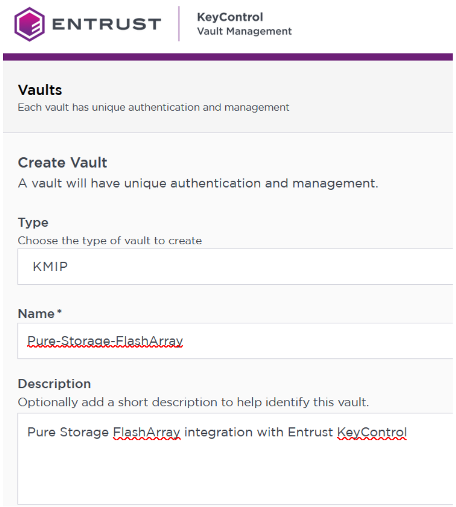
2.5. Create a KMIP vault in Entrust KeyControl

The Entrust KeyControl appliance supports different types of vaults. This section describes how to create a KMIP vault for this integration.

1. Sign in to the Entrust KeyControl Vault Server web GUI using the **secroot** credentials.
2. From the user’s dropdown menu, select **Vault Management**.



3. In the Vault Management interface, select the **Create Vault** icon.
4. In the **Create Vault** page **Type** pull-down menu, select **KMIP**, then enter your information.



Vaults

Each vault has unique authentication and management

Create Vault

A vault will have unique authentication and management.

Type

Choose the type of vault to create

KMIP

Name *

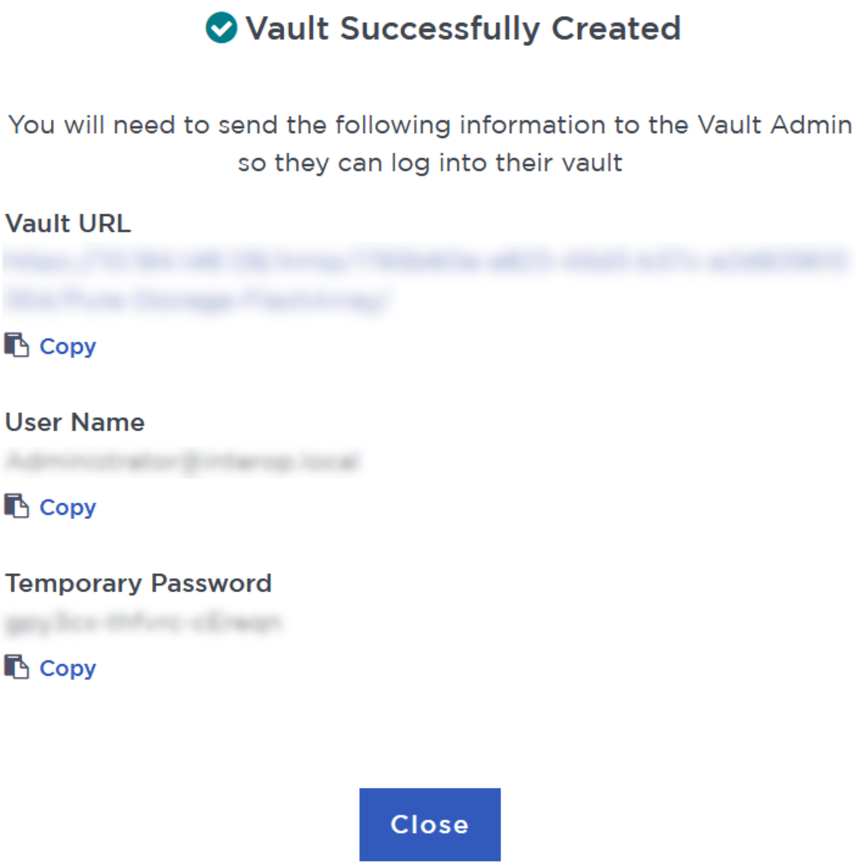
Pure-Storage-FlashArray

Description

Optionally add a short description to help identify this vault.

Pure Storage FlashArray integration with Entrust KeyControl

5. Select **Create Vault**, then select **Close**. A window with the newly created vault information appears. In addition, an email with the same vault information is sent to the security administrator.



Vault Successfully Created

You will need to send the following information to the Vault Admin so they can log into their vault

Vault URL

[redacted]

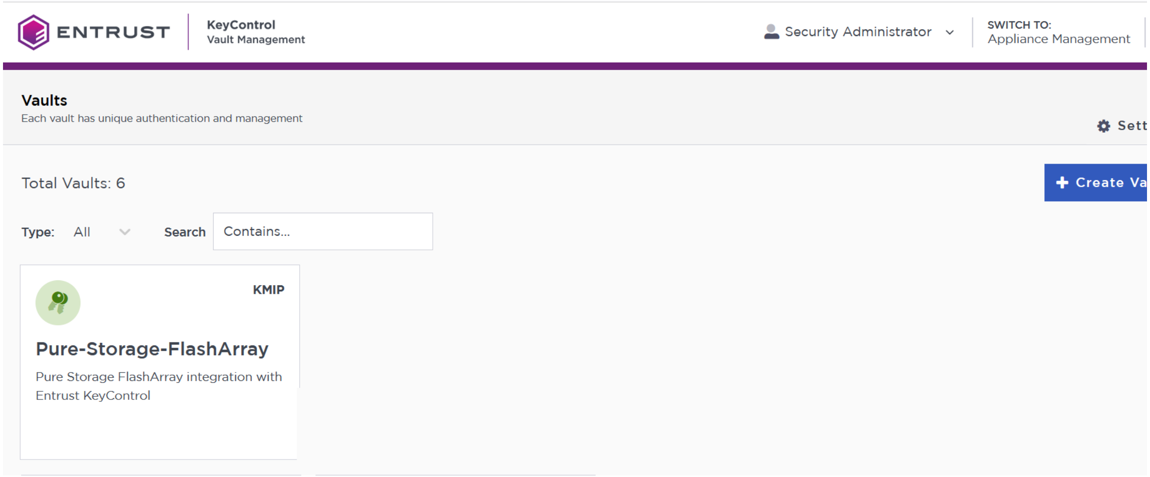
User Name

[redacted]

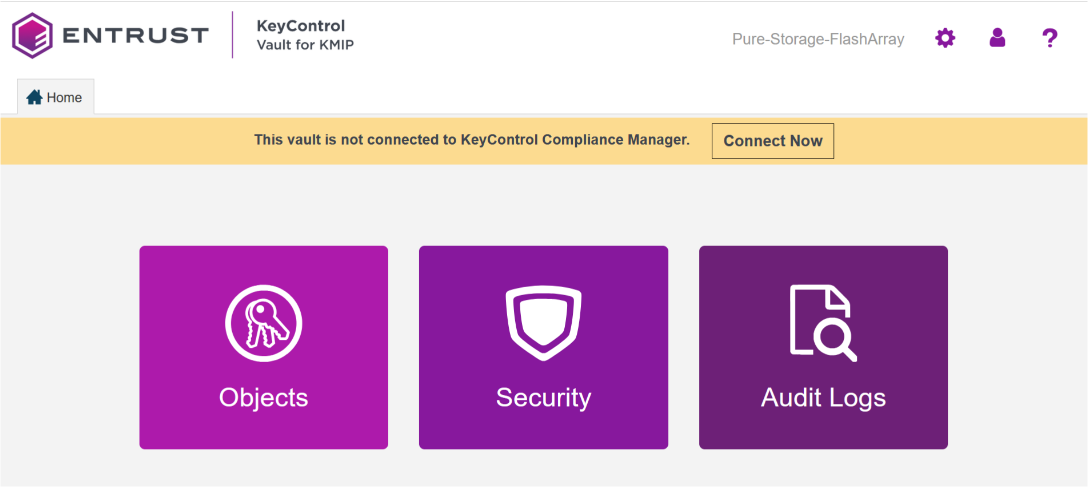
Temporary Password

[redacted]

6. Bookmark the **Vault URL** listed above.
7. The new vault is added to the **Vault Management** dashboard.



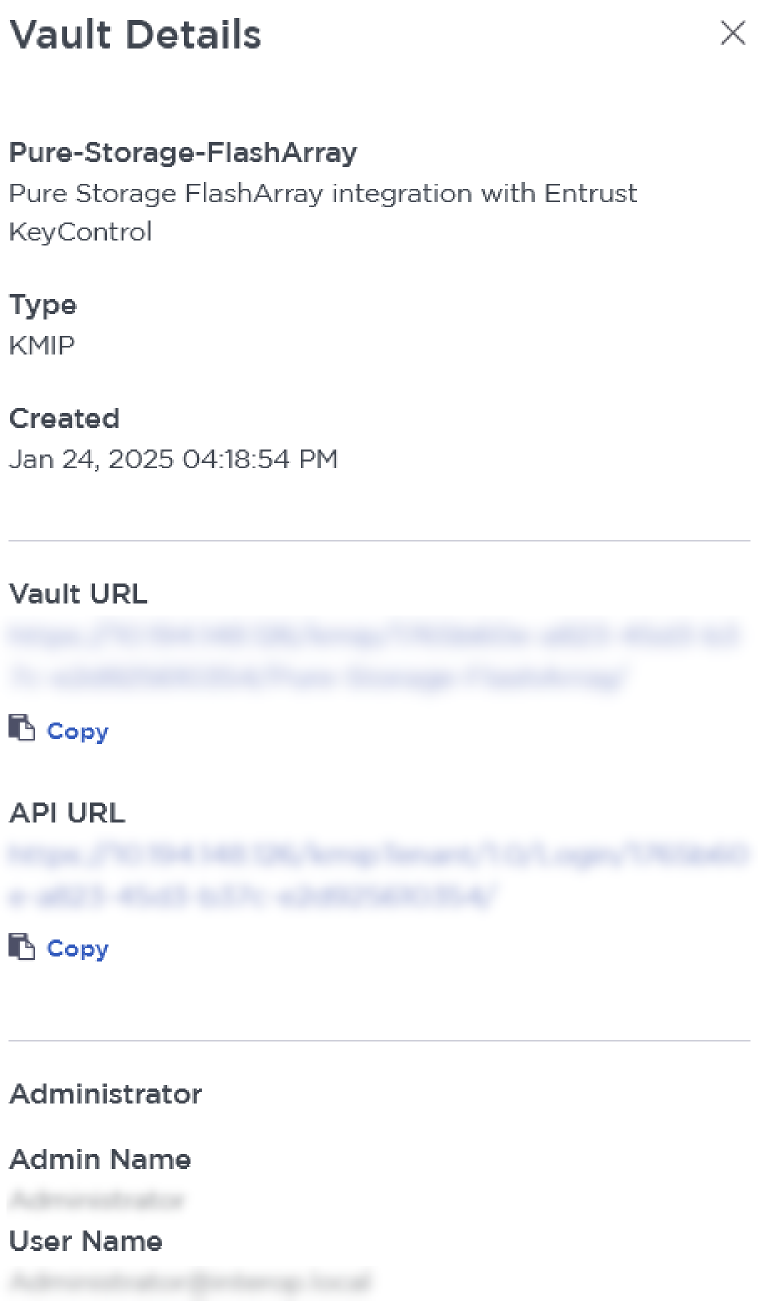
8. Sign in to the **Vault URL** with the temporary password. Change the temporary password when prompted. Sign in again to verify. Notice the vault name in the top right corner.



For more information, see Creating a Vault.

2.6. View the KMIP vault details

Back in the **Vault Management** dashboard, hover over the vault and select **View Details**.



Vault Details

Pure-Storage-FlashArray
Pure Storage FlashArray integration with Entrust KeyControl

Type
KMIP

Created
Jan 24, 2025 04:18:54 PM

Vault URL
[redacted]

API URL
[redacted]

Administrator

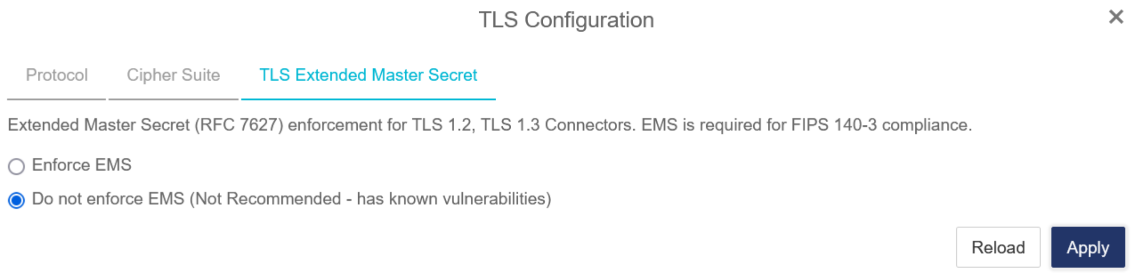
Admin Name
[redacted]

User Name
[redacted]

Chapter 3. Integrate Pure Storage FlashArray and KeyControl

3.1. Configure TLS EMS in KeyControl

1. Sign in to the KeyControl Vault Server web GUI using the **secroot** credentials.
2. The screen should default to **Appliance Management**. Otherwise, in the top-right corner select **Appliance Management**.
3. In the toolbar, select **Settings**.
4. Scroll down and select **TLS Configuration**.
5. In the **TLS Configuration** window, select the **TLS Extended Master Secret** tab.
6. Select the **Do not enforce EMS** radio button, Then select **Apply**.



Extended Master Secret (RFC 7627) enforcement for TLS 1.2, TLS 1.3 Connectors. EMS is required for FIPS 140-3 compliance.

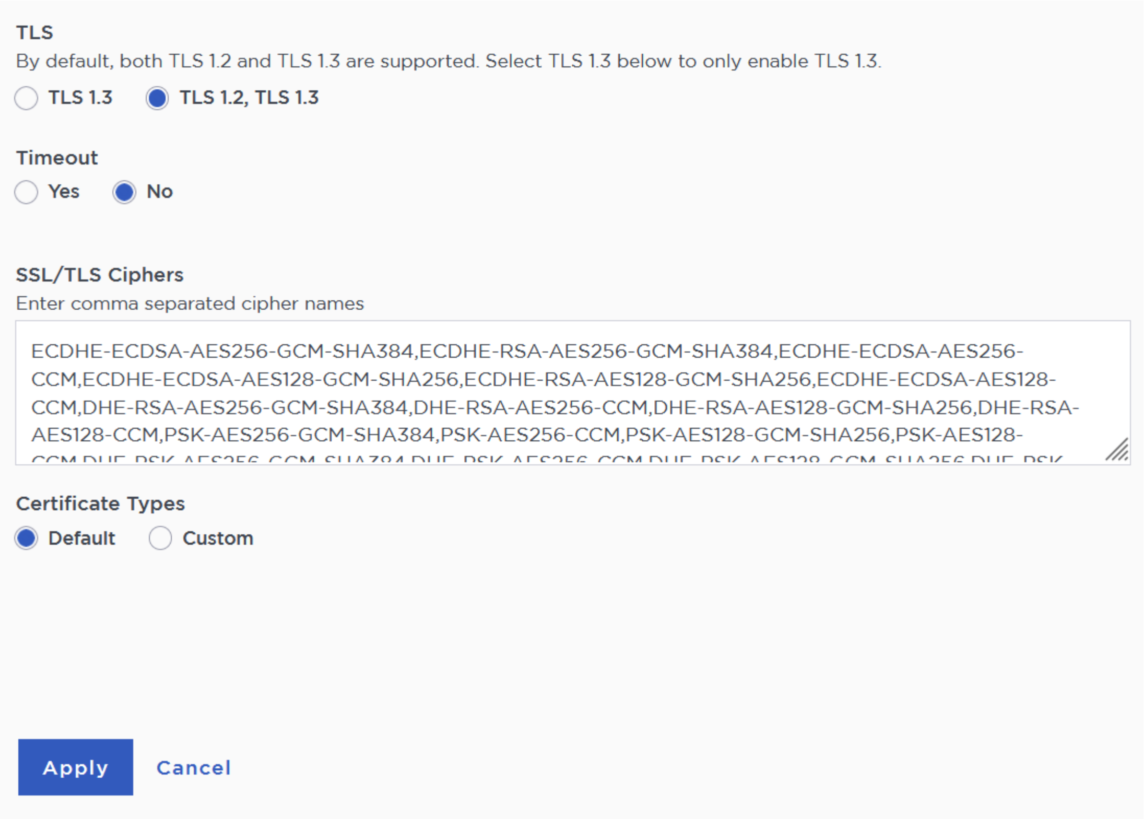
○ Enforce EMS

● Do not enforce EMS (Not Recommended - has known vulnerabilities)

3.2. Configure the TLS version in KeyControl

The tested version of Pure Storage FlashArray supports TLS v1.2. Configure KeyControl accordingly.

1. Sign in to the KeyControl Vault Server web GUI using the **secroot** credentials.
2. In the top-right corner select **Manage Vaults**.
3. In the top-right corner, select **Settings**.
4. Under **TLS**, select the **TLS 1.2, TLS 1.3** radio button.
5. Under **Certificate Types**, select according to your deployment, then select **Apply**.



TLS

By default, both TLS 1.2 and TLS 1.3 are supported. Select TLS 1.3 below to only enable TLS 1.3.

○ TLS 1.3 ● TLS 1.2, TLS 1.3

Timeout

○ Yes ● No

SSL/TLS Ciphers

Enter comma separated cipher names

ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-AES256-GCM-SHA384,ECDHE-ECDSA-AES256-CCM,ECDHE-ECDSA-AES128-GCM-SHA256,ECDHE-RSA-AES128-GCM-SHA256,ECDHE-ECDSA-AES128-CCM,DHE-RSA-AES256-GCM-SHA384,DHE-RSA-AES256-CCM,DHE-RSA-AES128-GCM-SHA256,DHE-RSA-AES128-CCM,PSK-AES256-GCM-SHA384,PSK-AES256-CCM,PSK-AES128-GCM-SHA256,PSK-AES128-CCM,DHE-PSK-AES256-GCM-SHA384,DHE-PSK-AES256-CCM,DHE-PSK-AES128-GCM-SHA256,DHE-PSK-

Certificate Types

● Default ○ Custom

3.3. Create a certificate signing request in Pure Storage FlashArray

1. Sign in to the Pure Storage FlashArray CLI with administrator privileges.
2. Create a self-signed certificate.

```
interop@denqamgmtscl03> purecert create entrust-kmip-cert --self-signed \
--common-name entrust-keycontrol

Name               Status       Key Algorithm  Key Size  Issued To           Issued By
entrust-kmip-cert  self-signed  rsa            2048      entrust-keycontrol  entrust-keycontrol

Valid From               Valid To                 Country  State/Province  Locality
2025-01-27 11:52:28 MST  2035-01-25 11:52:28 MST  -        -               -

Organization        Organizational Unit  Email  Common Name
Pure Storage, Inc.  Pure Storage, Inc.   -      entrust-keycontrol
```

3. Display the self-signed certificate created above.

```
interop@denqamgmtscl03> purecert list entrust-kmip-cert --certificate
-----BEGIN CERTIFICATE-----
MIurioqwerCgAwIBAgIEfhphKTANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJV
.
.
.

I10E4uaYtxxxKYUv
```

```
-----END CERTIFICATE-----
```

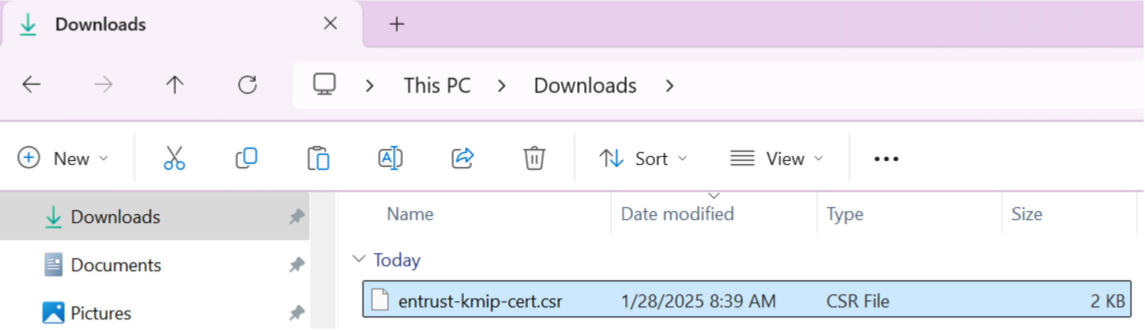
4. Construct a certificate signing request (CSR).

```
interop@denqamgmtscl03> purecert construct entrust-kmip-cert --certificate-signing-request

-----BEGIN CERTIFICATE REQUEST-----
MIIC2jCCruiotwpueritoerkGA1UEAwwSZW50cnVzdC1rZXljb250cm9sMRswGQYD
.
.
.

3i62111tOn1hZNU4ekw=
-----END CERTIFICATE REQUEST-----
```

5. Copy the above certificate into a text editor and create a `csr` file.

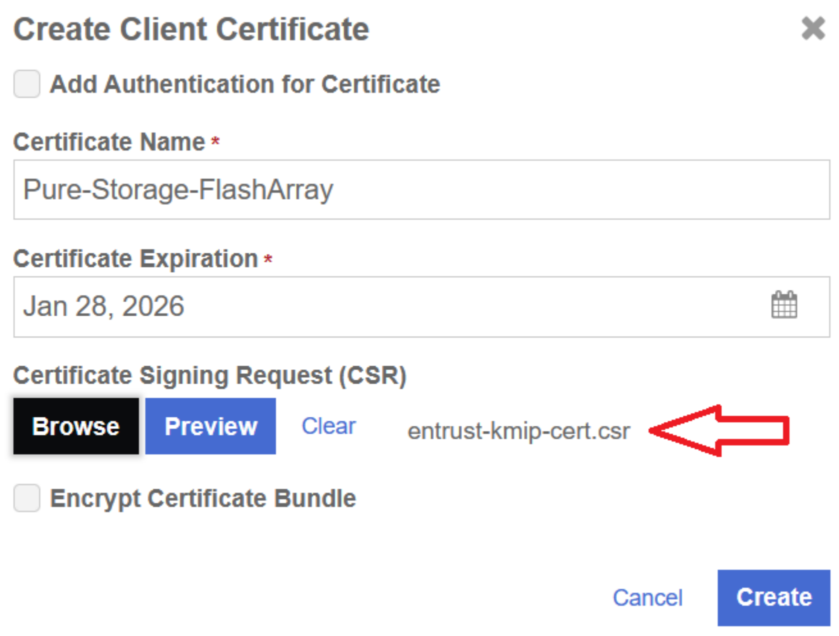


Name	Date modified	Type	Size
entrust-kmip-cert.csr	1/28/2025 8:39 AM	CSR File	2 KB

3.4. Create the client certificate bundle in KeyControl

The following steps describe how to import into KeyControl the csr created in Create a certificate signing request in Pure Storage FlashArray and create the client certificate bundle.

1. Sign in to the KMIP vault URL created in Create a KMIP Vault in the KeyControl.
2. Select the **Security** icon. Then select the **Client Certificates** icon.
3. Select the **+** icon to create a client certificate. Enter the certificate name and expiration date, and upload the csr created in section Create a certificate signing request in Pure Storage FlashArray. Then select **Create**.



Create Client Certificate

□ Add Authentication for Certificate

Certificate Name *

Pure-Storage-FlashArray

Certificate Expiration *

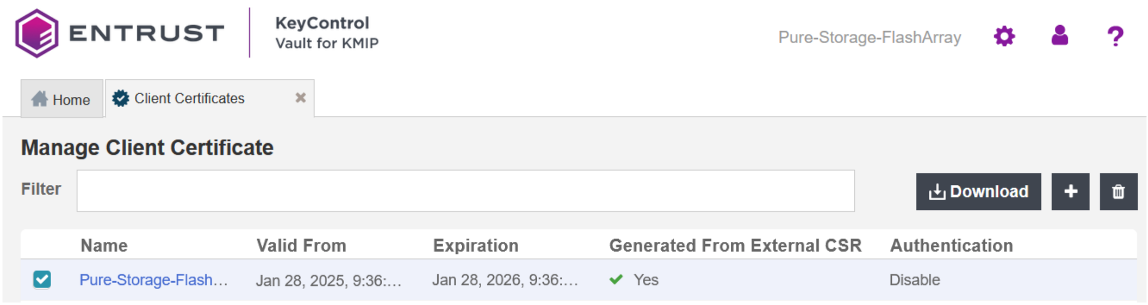
Jan 28, 2026

Certificate Signing Request (CSR)

entrust-kmip-cert.csr

□ Encrypt Certificate Bundle

4. Notice the new client certificate.

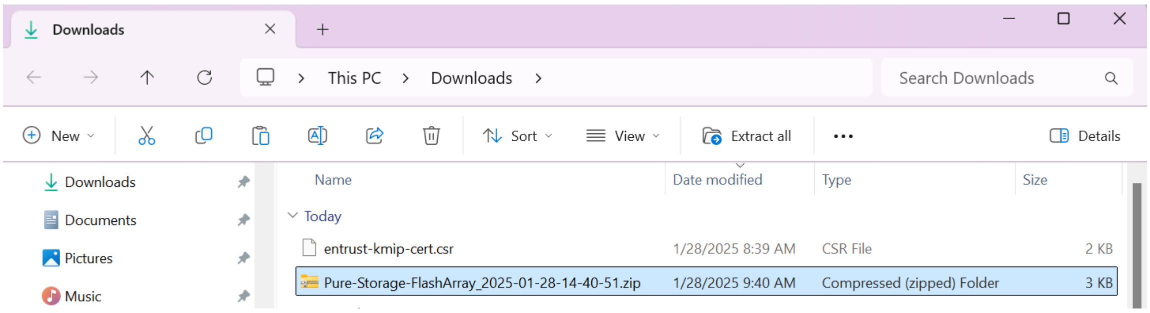


Manage Client Certificate

Filter

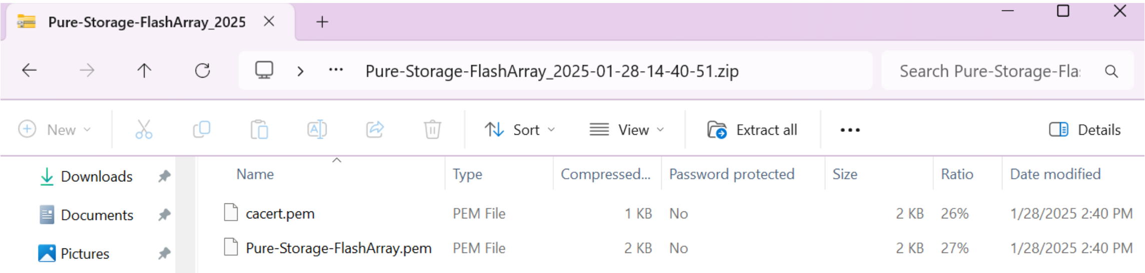
	Name	Valid From	Expiration	Generated From External CSR	Authentication
☑	Pure-Storage-Flash…	Jan 28, 2025, 9:36:…	Jan 28, 2026, 9:36:…	✓ Yes	Disable

5. Select the certificate. Then select **Download** and save it for later use.



Name	Date modified	Type	Size
Today			
entrust-kmip-cert.csr	1/28/2025 8:39 AM	CSR File	2 KB
Pure-Storage-FlashArray_2025-01-28-14-40-51.zip	1/28/2025 9:40 AM	Compressed (zipped) Folder	3 KB

6. The client certificate bundle `.zip` file includes the signed client certificate and CA certificate on `.pem` format.



Name	Type	Compressed...	Password protected	Size	Ratio	Date modified
cacert.pem	PEM File	1 KB	No	2 KB	26%	1/28/2025 2:40 PM
Pure-Storage-FlashArray.pem	PEM File	2 KB	No	2 KB	27%	1/28/2025 2:40 PM

For more information, see Managing KMIP Client Certificates.

3.5. Input the client bundle into Pure Storage FlashArray

1. Sign in to the Pure Storage FlashArray CLI with administrator privileges.
2. Update the Pure Storage FlashArray certificate with the signed key details. When prompted, paste the client certificate contained within the `Pure-Storage-FlashArray.pem` file from section Create the client certificate bundle in KeyControl.

   The client certificate includes the lines “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----” and all text between them.

```
interop@denqamgmtscl03> purecert setattr entrust-kmip-cert --certificate
Please enter certificate followed by Enter and then Ctrl-D:

-----BEGIN CERTIFICATE-----
MIIDyDCCArCgRTIQOPTJKPRAwIBAgIEfhphKjANBgkqhkiG9w0BAQsFADBXMQswC
.
.
.
f+qTL000zjC9iSWa
-----END CERTIFICATE-----
Name               Status    Key Algorithm  Key Size  Issued To
entrust-kmip-cert  imported  rsa            2048      entrust-keycontrol

Issued By                           Valid From               Valid To
HyTrust KeyControl Certificate Authority  2025-01-29 11:52:20 MST  2026-01-28 11:52:20 MST

Country  State/Province  Locality  Organization        Organizational Unit  Email
-        -               -         Pure Storage, Inc.  Pure Storage, Inc.   -

Common Name
entrust-keycontrol
```

3. Create the KMIP server configuration. When prompted, paste the CA certificate contained within the `cacert.pem` file from section Create the client certificate bundle in KeyControl.

   For the URI, enter the name or IP of the first KeyControl node. The CA certificate includes the lines `-----BEGIN CERTIFICATE-----` and `-----END`

`CERTIFICATE-----` and all text between them.

```
interop@denqamgmtscl03> purekmip create Entrust-KeyControl-KMIP-Server \
--uri 10.194.148.126:5696 --certificate entrust-kmip-cert --ca-certificate
Please enter CA certificate followed by Enter and then Ctrl-D:

-----BEGIN CERTIFICATE-----
MIID9TC urtoiqpeurtioewCAt2gAwIBAgIEZxphGjANBgkqhkiG9w0BAQsFADBX
.
.
.
XURIE3S1a3f8u
-----END CERTIFICATE-----
Name                            URI                 Certificate        Ca Certificate Configured
Entrust-KeyControl-KMIP-Server  10.194.148.126:5696  entrust-kmip-cert  True
```

4. Update the KMIP server information by adding the second KeyControl node. Notice both KeyControl nodes, in a comma separated list.

```
interop@denqamgmtscl03> purekmip setattr Entrust-KeyControl-KMIP-Server \
--uri 10.194.148.126:5696,10.194.148.127:5696 --certificate entrust-kmip-cert
Name                            URI                 Certificate        Ca Certificate Configured
Entrust-KeyControl-KMIP-Server  10.194.148.126:5696  entrust-kmip-cert  True
Entrust-KeyControl-KMIP-Server  10.194.148.127:5696  entrust-kmip-cert  True
```

3.6. Test secure connection from Pure Storage FlashArray to KeyControl

1. Sign in to the Pure Storage FlashArray CLI with administrator privileges.
2. Test the connections to each KeyControl node.

```
interop@denqamgmtscl03> purekmip test Entrust-KeyControl-KMIP-Server
Name                            URI                 Status  Details
Entrust-KeyControl-KMIP-Server  10.194.148.126:5696  OK
Entrust-KeyControl-KMIP-Server  10.194.148.127:5696  OK
```

3.7. Enable enhanced data security in Pure Storage FlashArray

1. Enable enhanced data security using the KeyControl KMIP server.

```
interop@denqamgmtscl03> purearray enable security-token --kmip Entrust-KeyControl-KMIP-Server
Enabled  Type  Signature                                                          Server
True     KMIP  ded2ca2146869dbcddd6a26117f8f16e07f4a4889bbdcf162b2bcb5996492f90  Entrust-KeyControl-KMIP-
Server
```

2. List the security token.

```
interop@denqamgmtscl03> purearray list --security-token
Enabled  Status   Type  Signature                                                         Server
True     enabled  KMIP  ded2ca2146869dbcddd6a26117f8f16e07f4a4889bbdcf162b2bcb5996492f90  Entrust-
KeyControl-KMIP-Server
```

3. Wait up to 30 minutes before executing the next command.
4. Again, test the connections to each KeyControl node.

```
interop@denqamgmtscl03> purekmip test Entrust-KeyControl-KMIP-Server
Name                            URI                  Status  Details
Entrust-KeyControl-KMIP-Server  10.194.148.126:5696  OK
Entrust-KeyControl-KMIP-Server  10.194.148.127:5696  OK
```

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

5.1. nShield Connect

5.2. nShield as a Service

5.3. KeyControl

5.4. KeyControl BYOK

5.5. KeyControl as a Service

5.6. Entrust products

5.7. nShield product documentation