



ENTRUST

Bring Your Own Key for Microsoft Azure Key Vault and Entrust KeyControl

Integration Guide

2024-04-24

Member of
Microsoft Intelligent
Security Association



Table of Contents

1. Introduction	1
1.1. Documents to read first	1
1.2. Product configurations	1
1.3. Features tested	1
1.4. Requirements	2
2. Install and configure Entrust KeyControl	3
2.1. Deploy an Entrust KeyControl cluster	3
2.2. Create an Entrust KeyControl Management Vault	3
3. Configure Microsoft Azure	5
3.1. Create an app registration in Azure	5
3.2. Add the app to the subscription Reader Role list	7
3.3. Create an Azure key vault	9
3.4. Add the app registration to the key vault access policies	12
4. Configure Entrust KeyControl as Microsoft Azure CSP	15
4.1. Create an Azure client secret	15
4.2. Create an Entrust KeyControl CSP account for Azure	16
5. Test integration	18
5.1. Create a key set in Entrust KeyControl	18
5.2. Create a cloud key in Entrust KeyControl	20
5.3. Create a cloud key in Azure key vault	23
5.4. Rotate a cloud key in Entrust KeyControl	25
5.5. Remove a cloud key in Entrust KeyControl	26
5.6. Upload a removed cloud key to Azure in Entrust KeyControl	27
5.7. Delete a cloud key in Entrust KeyControl	28
5.8. Cancel a cloud key deletion in Entrust KeyControl	29
6. Additional resources and related products	31
6.1. nShield Connect	31
6.2. nShield as a Service	31
6.3. KeyControl BYOK	31
6.4. Entrust digital security solutions	31
6.5. nShield product documentation	31

Chapter 1. Introduction

This document describes the integration of Microsoft Azure Key Vault Bring Your Own Key (referred to as Azure BYOK in this guide) with the Entrust KeyControl Key Management Solution (KMS).

1.1. Documents to read first

This guide describes how to configure the Entrust KeyControl server as a KMS in Azure BYOK.



Entrust KeyControl v10.2 supports BYOK as an add-on. You can request a free trial of Entrust KeyControl BYOK here: <https://go.entrust.com/keycontrol-byok-30-day-free-trial>.

To install and configure the Entrust KeyControl server see [KeyControl Installation and Upgrade Guide](#).

Also refer to the documentation and set-up process for Microsoft Azure BYOK in the [Microsoft Azure Key Vault online documentation](#).

1.2. Product configurations

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

System	Version
Entrust KeyControl	10.2

1.3. Features tested

Entrust has successfully tested the following features:

- Create cloud key
- Rotate cloud key
- Remove cloud key
- Upload removed cloud key
- Delete cloud key

- Cancel cloud key deletion

1.4. Requirements

Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

Chapter 2. Install and configure Entrust KeyControl

- [Deploy an Entrust KeyControl cluster](#)
- [Create an Entrust KeyControl Management Vault](#)

2.1. Deploy an Entrust KeyControl cluster

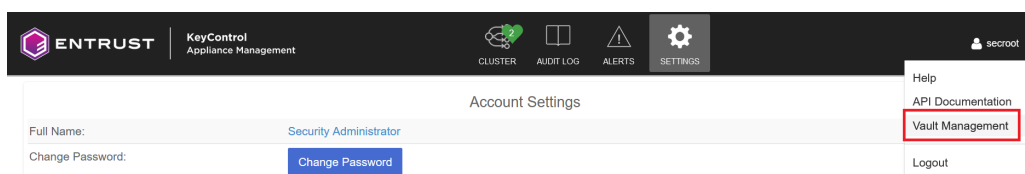
For this integration, Entrust KeyControl was deployed as a two-node cluster on premises. The installation software was downloaded in the form of an OVA file, deployed in VMware ESXi.

Follow the installation and set-up instructions in [KeyControl Installation and Upgrade Guide](#). If using an HSM, the integration guide with the Entrust nShield HSM is available at <https://www.entrust.com/documentation>. Search for the key phrase **KeyControl nShield HSM**.

2.2. Create an Entrust KeyControl Management Vault

To create an Entrust KeyControl Management Vault:

1. Sign in to the Entrust KeyControl Vault Server Appliance Manager.
2. In the home page, select the user's drop-down menu and select **Vault Management**.



3. Select **Create Vault**.

The **Create Vault** dialog appears.

4. In the **Type** drop-down box, select **Cloud Key Management**. Enter the required information.
5. Select **Create Vault**.

For example:

Type
Choose the type of vault to create
Cloud Key Management

Name*
Azure-BYOK-KeyControl

Description
Azure BYOK KeyControl CSP account.
Max. 300 characters

Administration
Invite an individual to have complete access and control over this vault. They will be responsible for inviting additional members.

Admin Name*
Administrator

Admin Email*
[redacted].com

Create Vault Cancel

- 6. You will receive an email with a URL and login credentials to the Entrust KeyControl vault. Bookmark the URL and save the credentials.

For example:



Administrator, you have been invited to become an administrator of the Cloud Key Management vault, Azure-BYOK-KeyControl.

To sign in, use the following:

URL: [https://\[redacted\].com/Azure-BYOK-KeyControl/](https://[redacted].com/Azure-BYOK-KeyControl/)

User Name: [redacted].com

Password: rfhzev-mc3Oly-[redacted]

- 7. Sign in to the above URL. Change the one-time password when prompted.

Chapter 3. Configure Microsoft Azure

- [Create an app registration in Azure](#)
- [Add the app to the subscription Reader Role list](#)
- [Create an Azure key vault](#)
- [Add the app registration to the key vault access policies](#)

3.1. Create an app registration in Azure

The app registration provides trust between your app and Azure.

1. Open a browser and sign in to the Azure portal <https://portal.azure.com/#home>.
2. Navigate to **Home > Azure Active Directory > App registrations**.
3. Select **New registration**.

The **Register an application** dialog.

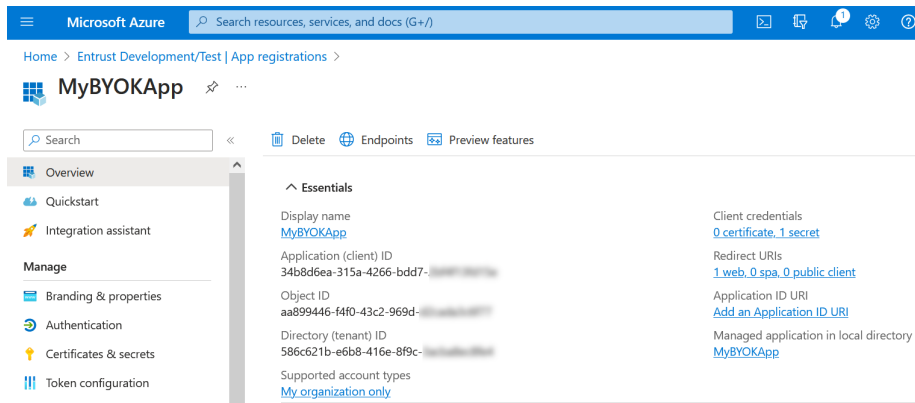
4. Enter the **Name**, a user-facing or friendly name. Select the applicable **Supported account types** and enter a **Redirect URI**.

For example:

The screenshot shows the 'Register an application' dialog in the Azure portal. The dialog is titled 'Register an application' and has a search bar at the top. Below the search bar, there is a breadcrumb trail: 'Home > Entrust Development/Test | App registrations >'. The main heading is 'Register an application'. There are three sections: 1. 'Name': A text input field with the value 'MyBYOKApp' and a checkmark icon on the right. Below the field is the text: '* Name' and 'The user-facing display name for this application (this can be changed later)'. 2. 'Supported account types': A section titled 'Supported account types' with the subtext 'Who can use this application or access this API?'. It contains four radio button options: 'Accounts in this organizational directory only (Entrust Development/Test only - Single tenant)' (selected), 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)', 'Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)', and 'Personal Microsoft accounts only'. Below the options is a link 'Help me choose...'. 3. 'Redirect URI (optional)': A section titled 'Redirect URI (optional)' with the subtext 'We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.'. It contains a dropdown menu set to 'Web' and a text input field with the value 'https://localhost' and a checkmark icon on the right. Below the input fields is a link 'Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications...'. At the bottom of the dialog is a blue button labeled 'Register' and a link 'By proceeding, you agree to the Microsoft Platform Policies'.

5. Select **Register**.

The newly created registration appears.



6. Select **API permissions**. Alternatively, select **Home > Azure Active Directory > App Registrations > <Display name> > API permissions**.

7. Select **Add a permission** and add the following permissions:

Microsoft API	Permission	Type
Microsoft Graph	Application.ReadWrite.All	Application
Microsoft Graph	User.Read (granted by default)	Delegated
Azure Key Vault	user_impersonation	Delegated
Azure Service Management	user_impersonation	Delegated

For example:

Microsoft Azure | Search resources, services, and docs (G+)

Home > Entrust Development/Test | App registrations > MyBYOKAppRegistration

MyBYOKAppRegistration | API permissions

Search | Refresh | Got feedback?

Overview
Quickstart
Integration assistant

Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Entrust Development/Test

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Azure Key Vault (1)				
user_impersonation	Delegated	Have full access to the Azure Key Vault service	No	...
▼ Azure Service Management (1)				
user_impersonation	Delegated	Access Azure Service Management as organization users	No	...
▼ Microsoft Graph (2)				
Application.ReadWrite.All	Application	Read and write all applications	Yes	⚠ Not granted for Entrust... ...
User.Read	Delegated	Sign in and read user profile	No	...

For additional information, see [Creating a Service Principal](#).

3.2. Add the app to the subscription Reader Role list



The **Owner** permission of the subscription is required to perform this operation.

1. Navigate to **Home > Subscriptions**.
2. Select your subscription.
3. Select **Access control (IAM)**.
4. Select **Add** and then select **Add role assignment** from the pull-down menu.

Home > Subscriptions > Entrust Enterprise Dev/Test Subscription

Subscriptions | Entrust Development/Test

+ Add | Manage Policies

Search | Subscriptions == global filter
My role == all
Status == all
Add filter

Entrust Enterprise Dev/Test Subscription | Access control (IAM)

Subscription

Search | + Add | Download role assignments | Edit columns | Refresh

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Add role assignment
Add co-administrator
Add custom role

View my access

5. In the **Add role assignment** dialog, select the **Reader** role and then select the **Members** tab.

Home > Subscriptions > Entrust Enterprise Dev/Test Subscription | Access control (IAM) >

Add role assignment ...

Role **Members** Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Assignment type

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Search by role name, description, or ID Type: All Category: All

Name ↑	Description ↑↓
Reader	View all resources, but does not allow you to make any changes.

6. Select **Select members**, search for the app **Display name**, and select it.

7. Select **Save**.

Add role assignment ...

Role **Members** Review + assign

Selected role Reader

Assign access to User, group, or service principal Managed identity

Members **+ Select members**

Name	Object ID	Type
No members selected		

Description Optional

Select members

Select

MyBYOKApp

Selected members: MyBYOKAppRegistration Remove

Select Close

Review + assign Previous Next

The new subscription **Reader** role is added.

Microsoft Azure Search resources, services, and docs (G+)

Home > Subscriptions > Entrust Enterprise Dev/Test Subscription

Entrust Enterprise Dev/Test Subscription | Access control (IAM)

Subscription

Search

+ Add Download role assignments Edit columns Refresh Remove Feedback

Name	Type	Role	Scope	Condition
> Contributor				
> Cost Management Reader				
> Management Group Reader				
> Monitoring Reader				
> Owner				
Reader				
MyBYOKApp	App	Reader	This resource	None

3.3. Create an Azure key vault

An existing Azure key vault with **Permission model** equals **Vault access policy** can be used for this integration. A new Azure key vault was created in this integration to show the entire process.

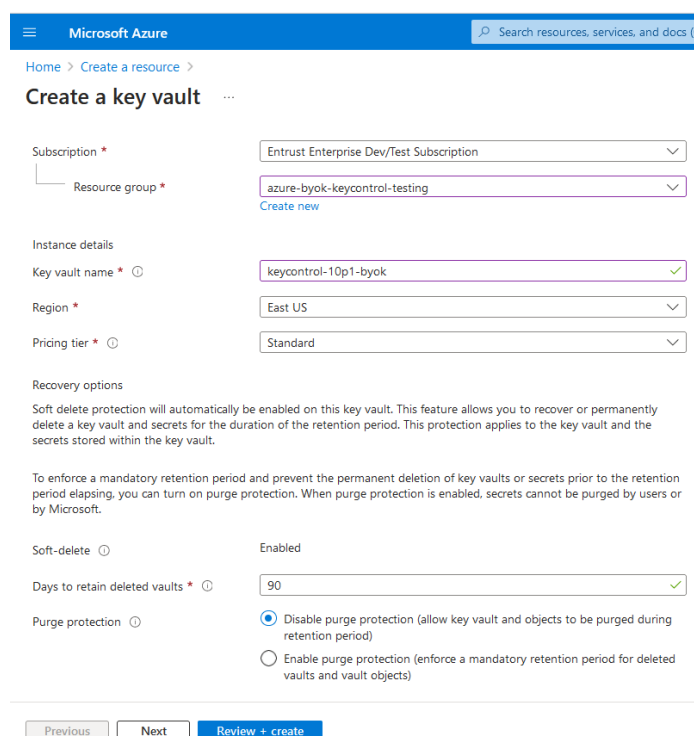
For an existing Azure key vault, proceed to section [Add the app registration to the key vault access policies](#) directly, skipping this section entirely.

1. Open a browser and sign in to the Azure portal <https://portal.azure.com/#home>.
2. In the home page, select the **Create a resource** icon.
3. Select **Key Vault**.

The **Create a key vault** dialog appears.

4. In the **Basics** tab select the **Subscription** and **Resource group** from the pull-down menu. Enter the instance details.
5. Select **Next**.

For example:

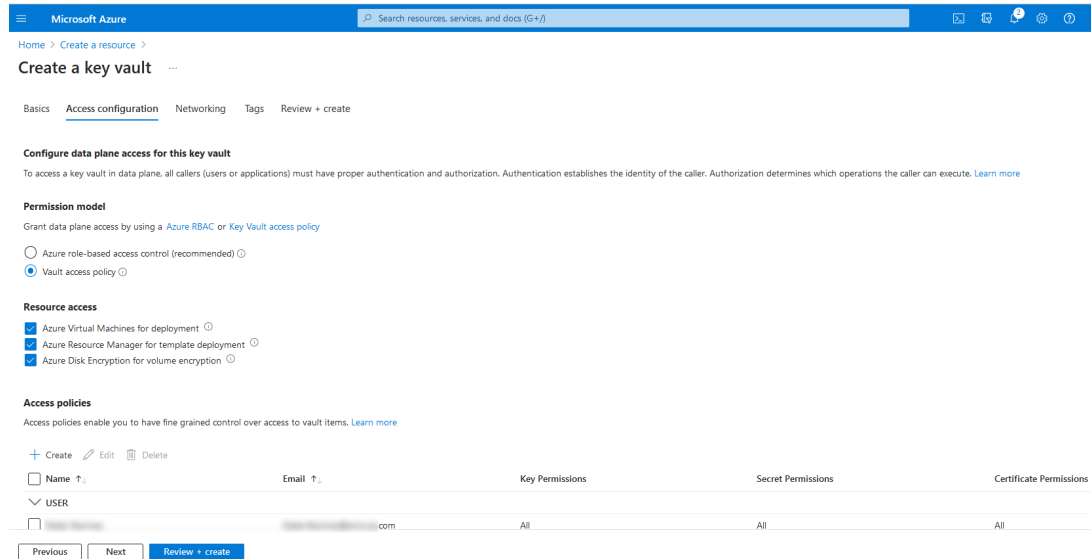


The screenshot shows the 'Create a key vault' dialog in the Azure portal. The 'Basics' tab is selected. The 'Subscription' dropdown is set to 'Entrust Enterprise Dev/Test Subscription'. The 'Resource group' dropdown is set to 'azure-byok-keycontrol-testing', with a 'Create new' link below it. Under 'Instance details', the 'Key vault name' is 'keycontrol-10p1-byok', the 'Region' is 'East US', and the 'Pricing tier' is 'Standard'. Under 'Recovery options', 'Soft-delete' is 'Enabled'. 'Days to retain deleted vaults' is set to '90'. 'Purge protection' is set to 'Disable purge protection (allow key vault and objects to be purged during retention period)'. At the bottom, there are three buttons: 'Previous', 'Next', and 'Review + create'.

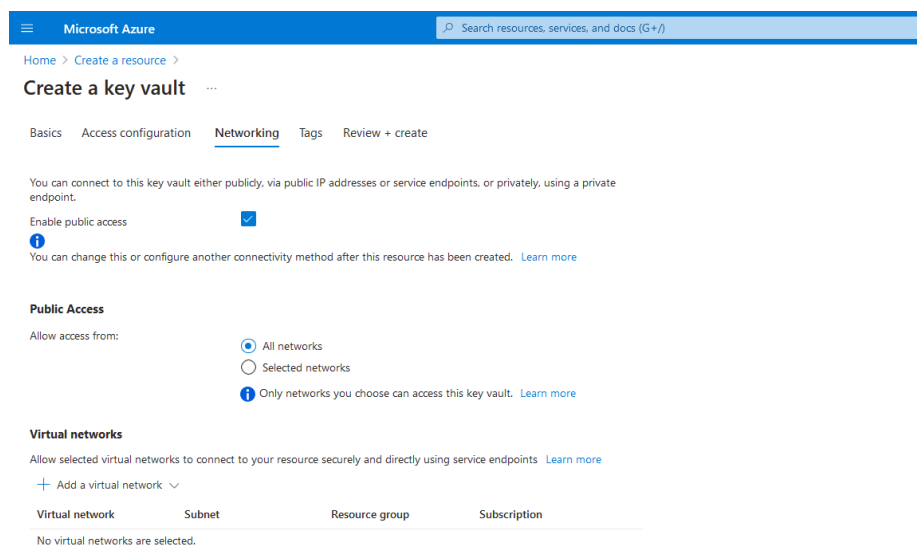
6. In the **Access configuration** tab, select the **Permission model**, **Resource access**, and **Access policies**.
7. If you are using **Vault access policy** for the **Permission model**:

- a. Select the user.
- b. Select **Edit** and select all permissions that apply.
- c. Select **Save** and **Next**.

All **Key Permissions**, **Secrets Permissions**, and **Certificate Permissions** were selected for the purpose of this integration.



- 8. In the **Networking** tab, select **Enable public access**.
- 9. Under **Public access**, select **All networks**.
- 10. Select **Next**.



Exception
Enabling access to resources requires you allow trusted Microsoft services to bypass firewall.

Allow trusted Microsoft services to bypass this firewall

This setting is related to firewall only. In order to access this key vault, the trusted service must also be given explicit permissions the Access Policies section. [Learn more](#)

Private endpoint
Create a private endpoint to allow a private connection to this resource. Additional private endpoint connections can be created within the key vault or private link center. [Learn more](#)

+ Create a private endpoint

Name	Subscription	Resource group	Region	Subnet	Private DNS Zone
Click on add button to add private endpoint					

- In the **Tags** tab enter the required **Name** and **Value**. These were left blank for the purpose of this integration.
- Select **Next**.
- Review the information and select **Create**.

Microsoft Azure

Home > Create a resource >

Create a key vault

Basics

Subscription	[REDACTED]
Resource group	azure-byok-keycontrol-testing
Key vault name	keycontrol-10p1-byok
Region	East US
Pricing tier	Standard
Soft-delete	Enabled
Purge protection during retention period	Disabled
Days to retain deleted vaults	90 days

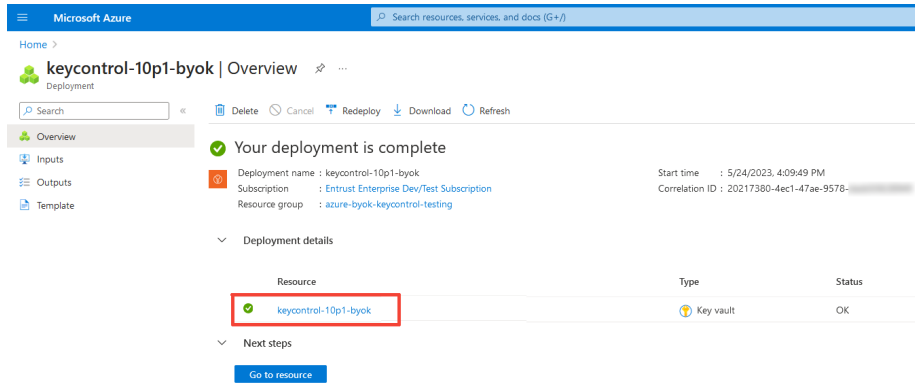
Access configuration

Azure Virtual Machines for deployment	Enabled
Azure Resource Manager for template deployment	Enabled
Azure Disk Encryption for volume encryption	Enabled
Permission model	Vault access policy
Access policies	2

Networking

Connectivity method	Public endpoint (all networks)
Selected networks	0
Allow trusted Microsoft services to bypass this firewall	Yes

- A deployment page appears. The newly created Azure vault is included.



3.4. Add the app registration to the key vault access policies

These steps configure the key vault policies to allow access by the app.

1. Navigate to **Home > Key vault > <Key_vault_name> > Access policies.**
2. Select **Create.**

The **Create and access policy** dialog appears.

3. In the **Permissions** tab select the following **Key permissions.**

Key permissions	Selection
Key Management Operations	All
Privileged Key Operations	All
Rotation Policy Operations	All

4. Select **Next.**
5. In the **Principal** tab, enter the **Display name** of the app. After the app is found, select the app.
6. Select **Next.**

For example:

Microsoft Azure Search resources, services, and docs (G+)

Home > keycontrol-10p1-byok | Access policies >

Create an access policy ...

keycontrol-10p1-byok

Permissions Principal Application (optional) Review + create

Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

MyBYOKApp

MyBYOKApp
34b8d6ea-315a-4266-bdd7-...

Selected item

MyBYOKApp
34b8d6ea-315a-4266-bdd7-...

Previous Next

7. Select **Next** in the **Application (optional)** tab.

8. Review the information and select **Create**.

For example:

Microsoft Azure Search resources, services, and docs (G+)

Home > keycontrol-10p1-byok | Access policies >

Create an access policy ...

keycontrol-10p1-byok

Permissions Principal Application (optional) Review + create

Key Permissions

Key Management Operations	All selected
Cryptographic Operations	None selected
Privileged Key Operations	All selected
Rotation Policy Operations	All selected

Secret Permissions

Secret Management Operations	None selected
Privileged Secret Operations	None selected

Certificate Permissions

Certificate Management Operations	None selected
Privileged Certificate Operations	None selected

Principal

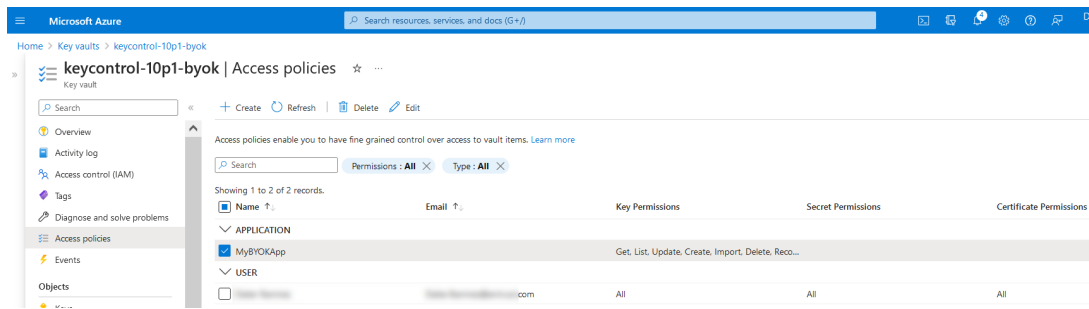
Principal name	MyBYOKApp
Object ID	51af2410-5204-4c87-a4e8-...

Application

Authorized application	None selected
Object ID	None selected

Previous Create

9. The **Access policies** page appears. The new vault access policy is included.



For additional information, see [Set Permissions for the BYOK Service by Configuring Each Azure Key Vault](#).

Chapter 4. Configure Entrust KeyControl as Microsoft Azure CSP

- [Create an Azure client secret](#)
- [Create an Entrust KeyControl CSP account for Azure](#)

4.1. Create an Azure client secret

This secret is required to create the Entrust CSP account for Azure. It expires after a set period. You must create the Entrust KeyControl CSP account for Azure before the secret expiration date.

1. Navigate to **Home > Azure Active Directory > App registrations > <App-registration-name> > Certificates & secrets.**
2. Select **New client secret.**

The **Add a client secret** dialog appears.

3. Enter the **Description** and select the expiration date.
4. Select **Add.**

The **Certificates & secrets** page appears. For example:

The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar and navigation links. The main content area is titled 'MyBYOKAppRegistration | Certificates & secrets'. On the left, there's a sidebar with navigation options like 'Overview', 'Quickstart', 'Integration assistant', and 'Manage'. The 'Manage' section is expanded to show 'Certificates & secrets'. The main content area shows a table of client secrets. The table has columns for 'Description', 'Expires', 'Value', and 'Secret ID'. There is one entry in the table: 'Entrust CSP account for Azure secret' with an expiration date of '11/27/2023' and a value 'Del8Q-paxLnVUOw3bkd...'. The Secret ID is 'd6b32caa-7981-4dd8-b759-...'. There are also some informational messages and a '+ New client secret' button.

5. Copy and save the **Value** of the new client secret.



This value appears in Azure Portal only temporarily. When the portal hides the client secret, it cannot be retrieved and a new secret must be created.

For additional information, see [Creating a client secret in Azure Active Directory](#).

4.2. Create an Entrust KeyControl CSP account for Azure

The following steps establish the connection between Entrust KeyControl and Azure, making Entrust KeyControl the CSP of the Azure application.

1. Sign in to the Entrust KeyControl Vault URL bookmark from [Create an Entrust KeyControl Management Vault](#).
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CSP Accounts** tab.
4. In the **Action** icon, select **Add CSP Account** in the drop-down menu.

The **Add CSP Account** dialog appears.

5. In the **Details** tab enter the **Name** and **Description**.
6. In the **Admin Group** drop-down menu box select **Cloud Admin Group**.
7. In the **Type** drop-down menu box select **Azure**.
8. Enter the following from the Azure account:

Item	Value
Azure AD Tenant ID	Home > Azure Active Directory > App registrations > <Display name> > Directory (tenant) ID
Subscription ID	Home > Subscription > Subscription ID
Client ID	Home > Azure Active Directory > App registrations > <Display name> > Application (client) ID
Client Secret	Value of the secret created in Create an Azure client secret .

For example:

Add CSP Account ✕

Details
Schedule

Name *

Description

Admin Group *

Type *

Azure AD Tenant ID *

Subscription ID *

Client ID *

Client Secret *

Cancel
Continue

9. Select **Continue**.
10. In the **Schedule** tab, define the rotation schedule.
11. Select **Apply**.

For example:

Add CSP Account ✕

Details
Schedule

Define a schedule for which client secrets are rotated.

Rotation Schedule *

Never Define Schedule

Cancel
Apply

The new CSP account is created.

CSP Account Name	Description	Admin Group	Key Set	Type
MyBYOKAppRegistration	Entrust KeyControl CSP account for Azure BYOK	Cloud Admin Group		AZURE

Chapter 5. Test integration

- Create a key set in Entrust KeyControl
- Create a cloud key in Entrust KeyControl
- Create a cloud key in Azure key vault
- Rotate a cloud key in Entrust KeyControl
- Remove a cloud key in Entrust KeyControl
- Upload a removed cloud key to Azure in Entrust KeyControl
- Delete a cloud key in Entrust KeyControl
- Cancel a cloud key deletion in Entrust KeyControl

5.1. Create a key set in Entrust KeyControl

This key set will be used to create a cloud key in Entrust KeyControl.

1. Sign in to the Entrust KeyControl Vault URL bookmark from [[test-integration:::create-keycontrol-vault](#)].
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **Key Sets** tab.
4. Select **Actions > Create Key Set**.

The **Choose the type of keys...** dialog appears.

5. Choose **Azure Key**.

The **Create Key Set** dialog appears.

6. In the **Details** tab enter a **Name** and **Description**.
7. In the **Admin Group** menu select **Cloud Admin Group**.

For example:

Create Key Set ✕

[Details](#) | [CSP Account](#) | [HSM](#) | [Schedule](#)

Name *

AzureBYOK

Description

Azure BYOK integration testing with Entrust KeyControl

Admin Group *

Cloud Admin Group

Cancel Continue

8. Select **Continue**.

9. In the **CSP Account** tab, select the CSP account created in [\[test-integration:::create-keycontrol-csp-account\]](#).

For example:

Create Key Set ✕

[Details](#) | [CSP Account](#) | [HSM](#) | [Schedule](#)

CSP Account *

Choose an existing CSP Account or add a new one to use with this Key Set.

MyBYOKAppRegistration

+ Add CSP Account

Cancel Continue

10. Select **Continue**.

11. In the **HSM** tab, select **Enable HSM** if using one. In that case ensure the HSM is configured prior to this step.

For example:

Create Key Set ✕

[Details](#) | [CSP Account](#) | [HSM](#) | [Schedule](#)

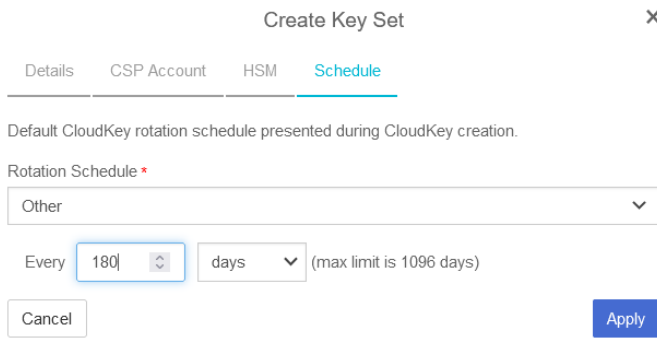
Enable HSM

If checked, the HSM linked to KeyControl will be used for generating cryptographic material for Cloudkeys in this Key Set.

Cancel Verify HSM connection Continue

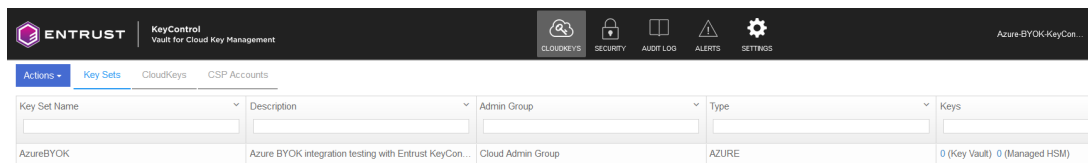
12. Select **Continue**.

13. In the **Schedule** tab, select a **Rotation Schedule** matching the selection made during [\[test-integration:::create-azure-client-secret\]](#). For example:



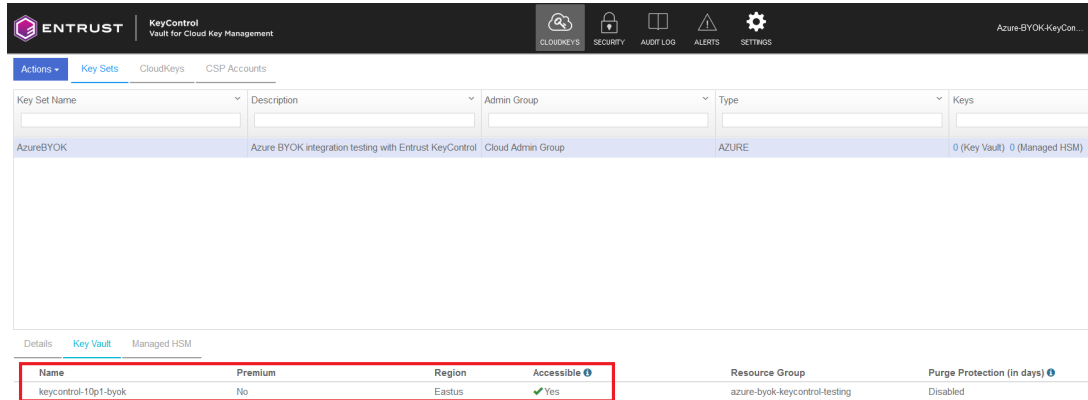
14. Select **Apply**.

The key set is added. For example:



15. Verify the Azure key vault created in [\[test-integration:::create-azure-keyvault\]](#) is listed in the **Key Vault** tab with setting **Accessible** set to **Yes**.

For example:



For additional information, see [Creating a Key Set](#).

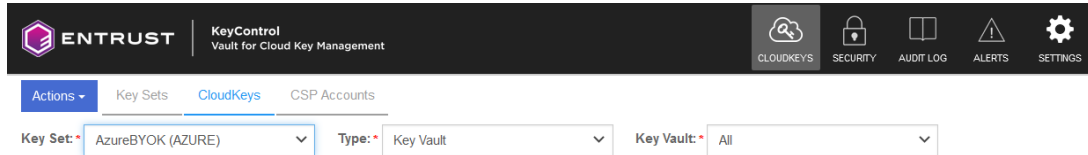
5.2. Create a cloud key in Entrust KeyControl

The following steps create a cloud key in Entrust KeyControl and verify it is available in Azure key vault.

1. Sign in to the Entrust KeyControl Vault URL bookmark from [\[test-integration:::create-keycontrol-vault\]](#).
2. Select the **CLOUDKEYS** icon on the toolbar.

3. Select the **CloudKeys** tab.
4. In the **Key Set** menu, select the **Key Set** created in [Create a key set in Entrust KeyControl](#).
5. In the **Type** menu, select **Key Vault**.

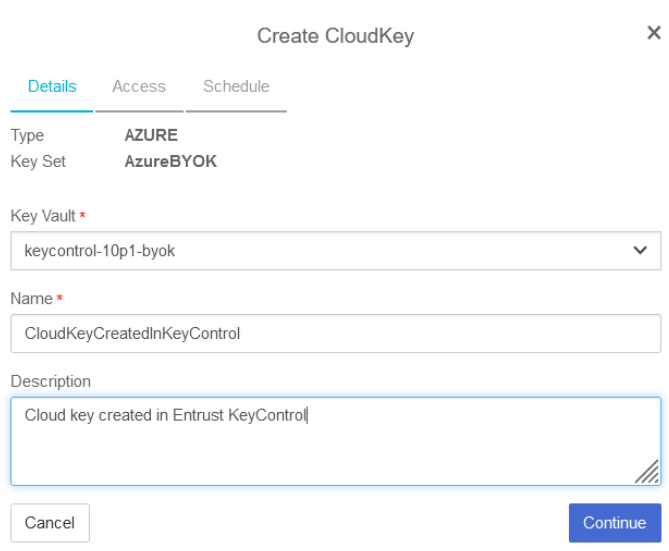
For example:



6. Select **Actions > Create CloudKey**.

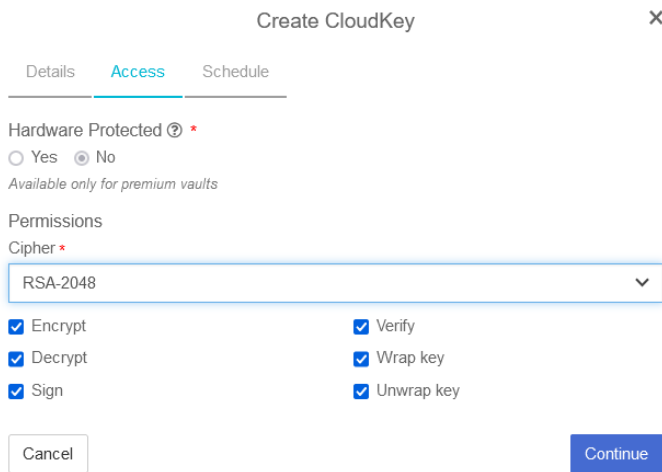
The **Create CloudKey** dialog appears.

7. In the **Key Vault** menu, select the Azure key vault created in [\[test-integration:::create-azure-keyvault\]](#).
8. In the **Details** tab, enter the **Name** and **Description**. For example:

The screenshot shows the 'Create CloudKey' dialog box. It has three tabs: 'Details', 'Access', and 'Schedule'. The 'Details' tab is active. Below the tabs, there are several fields: 'Type' is 'AZURE', 'Key Set' is 'AzureBYOK', 'Key Vault' is a dropdown menu with 'keycontrol-10p1-byok' selected, 'Name' is a text input field with 'CloudKeyCreatedInKeyControl', and 'Description' is a text input field with 'Cloud key created in Entrust KeyControl'. At the bottom, there are 'Cancel' and 'Continue' buttons.

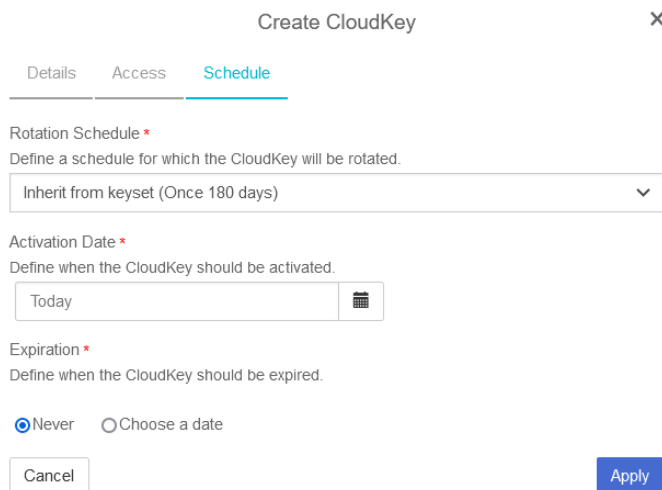
9. Select **Continue**.
10. In the **Access** tab, select the required **Cipher**.

For example:



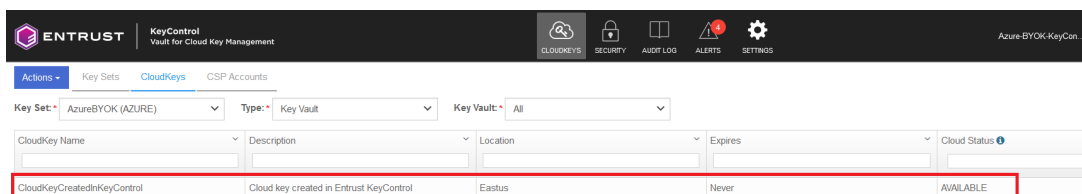
- 11. Select **Continue**.
- 12. In the **Schedule** tab, select the **Rotation Schedule**, **Activation Date**, and **Expiration**.

For example:

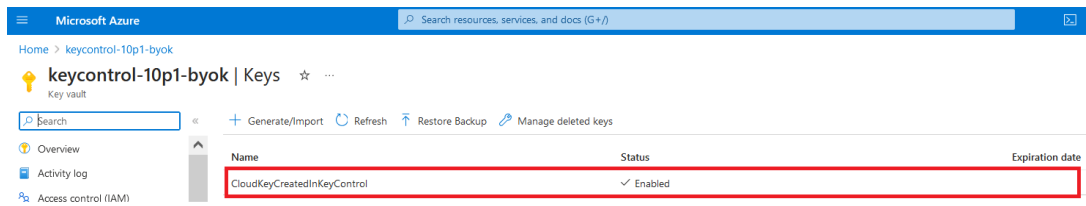


- 13. Select **Apply**.

The cloud key is created.



- 14. Verify the cloud key created in Entrust KeyControl is available in Azure key vault.



For additional information, see [Creating a CloudKey](#).

5.3. Create a cloud key in Azure key vault

The following steps create a cloud key in Azure key vault and import it into Entrust KeyControl.

To create a cloud key in Azure Key Vault:

1. Navigate to **Home > Key vaults > <Key_vault_name> > Keys > Generate/Import**.

The **Create a key** dialog appears.

2. Enter the **Name** and the required key properties.

For example:

Create a key ...

Options:

Name *

Key type RSA EC

RSA key size 2048 3072 4096

Set activation date

Set expiration date

Enabled Yes No

Tags

Set key rotation policy

Confidential Key Options

Exportable

Immutable

Confidential operation policy

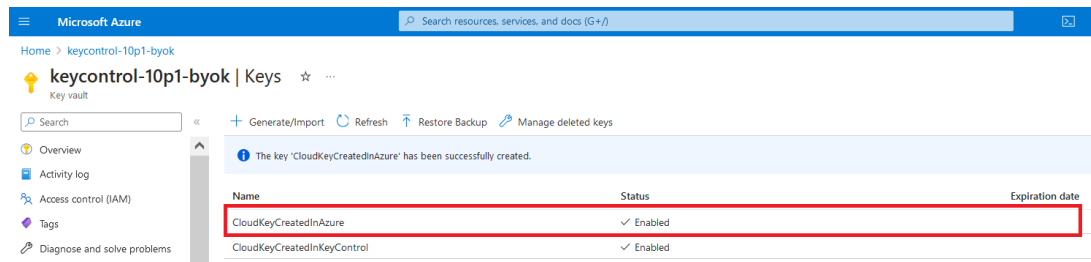
Create

3. Select **Create**.

The cloud key is created.

4. Verify the newly created key.

For example:



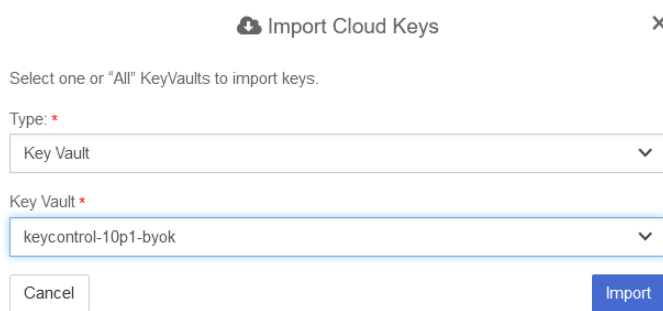
To import the cloud key created in Azure into Entrust KeyControl:

1. Sign in to the Entrust KeyControl Vault URL bookmark from [\[test-integration:::create-keycontrol-vault\]](#).
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **Key Sets** tab.
4. Select the key set created in [Create a key set in Entrust KeyControl](#).
5. Select **Actions > Import CloudKey**.

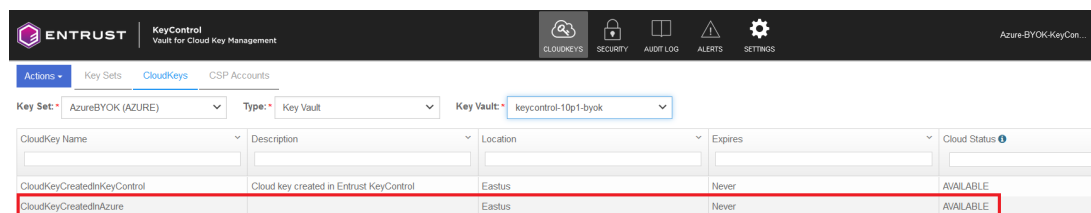
The **Import Cloud Keys** dialog appears.

6. In the **Type** menu, select **Key Vault**.
7. In the **Key Vault** menu, select the Azure key vault created in [\[test-integration:::create-azure-keyvault\]](#).

For example:



8. Select **Import**.
9. Verify the cloud key created in Azure key vault is available in Entrust KeyControl.



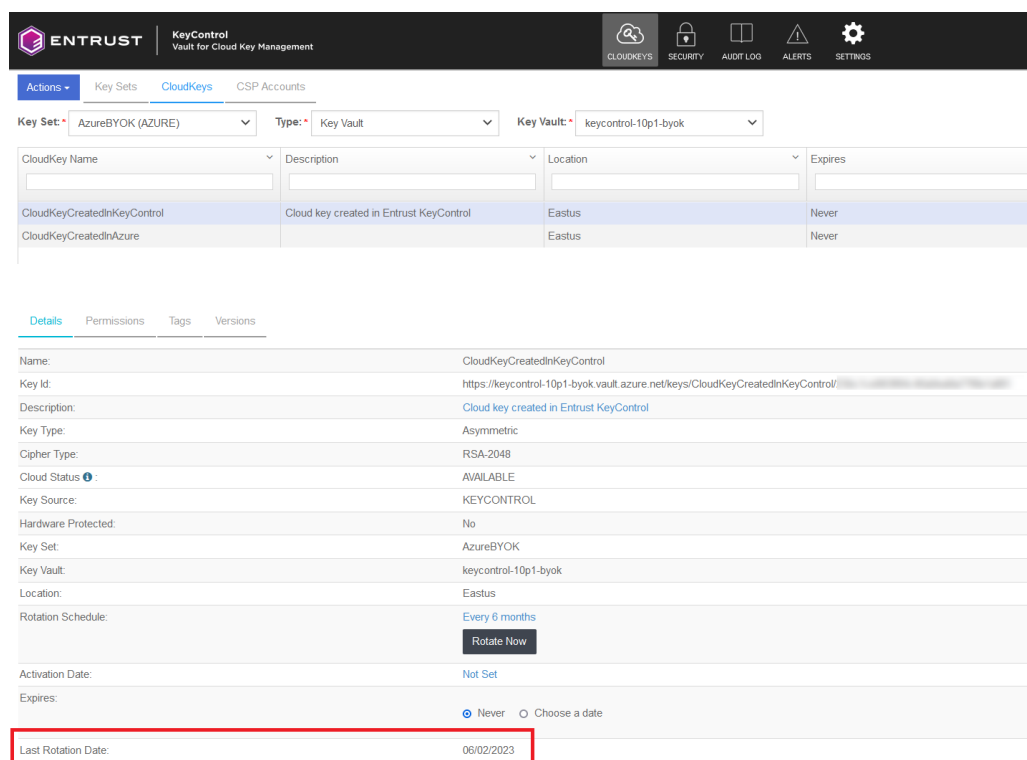
5.4. Rotate a cloud key in Entrust KeyControl

To rotate a cloud key in Entrust KeyControl:

1. Sign in to the Entrust KeyControl Vault URL bookmark from [[test-integration:::create-keycontrol-vault](#)].
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.
4. Select the key to rotate. Then, scroll down until you see the **Rotate Now** control.
5. Select **Rotate Now**.

The key has been rotated.

For example:



The screenshot shows the Entrust KeyControl interface. At the top, there's a navigation bar with the Entrust logo and 'KeyControl Vault for Cloud Key Management'. Below that, there are tabs for 'Actions', 'Key Sets', 'CloudKeys', and 'CSP Accounts'. The 'CloudKeys' tab is active. Below the tabs, there are filters for 'Key Set' (AzureBYOK (AZURE)), 'Type' (Key Vault), and 'Key Vault' (keycontrol-10p1-byok). A table lists cloud keys with columns for 'CloudKey Name', 'Description', 'Location', and 'Expires'. The 'CloudKeyCreatedInKeyControl' key is selected. Below the table, there are tabs for 'Details', 'Permissions', 'Tags', and 'Versions'. The 'Details' tab is active, showing key details such as Name, Key Id, Description, Key Type, Cipher Type, Cloud Status, Key Source, Hardware Protected, Key Set, Key Vault, Location, Rotation Schedule, Activation Date, Expires, and Last Rotation Date. The 'Last Rotation Date' is highlighted with a red box and shows '06/02/2023'. A 'Rotate Now' button is visible next to the 'Rotation Schedule' field.

6. In Azure, navigate to **Home > Key vaults > <Key_vault_name> > Keys**.
7. Select the key you want to rotate.
8. Verify that the key has been rotated.

For example:

Version	Status
CURRENT VERSION	
23bc1ce903f84c46a0ea9a	✓ Enabled
OLDER VERSIONS	
c890d1a12a984f36a66f05	✓ Enabled

5.5. Remove a cloud key in Entrust KeyControl

A removed cloud key in Entrust KeyControl will no longer be available for use in Azure. However, Entrust KeyControl will keep a copy of the removed cloud key, which could be reloaded to Azure for use.

1. Sign in to the Entrust KeyControl Vault URL bookmark from [\[test-integration:::create-keycontrol-vault\]](#).
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.
4. Select the key to be removed.
5. Select **Actions > Remove from Cloud**.

The **Remove from Cloud** dialog appears.

6. Type the name of the cloud key in **Type CloudKey Name**.

For example:

Remove from Cloud ×

⚠ Removing the key from the cloud will remove the key material from the KMS. An application will no longer be able to use this key from the cloud.

Appliance Management will keep a copy of the key. This copy can always be uploaded back to the cloud.

Are you sure you want to remove the following CloudKey from the cloud?

CloudKey **CloudKeyCreatedInKeyControl**

KeyId **https://keycontrol-10p1-byok.vault.azure.net/keys/CloudKeyCreatedInKeyControl/**

Type CloudKey Name *

7. Select **Remove**.
8. Verify the status change in Entrust KeyControl.

For example:

CloudKey Name	Description	Location	Expires	Cloud Status
CloudKeyCreatedInKeyControl	Cloud key created in Entrust KeyControl	Eastus	Never	NOT AVAILABLE
CloudKeyCreatedInAzure		Eastus	Never	AVAILABLE

9. Verify the key is gone from Azure.

For example:

Name	Status	Expiration date
CloudKeyCreatedInAzure	✓ Enabled	

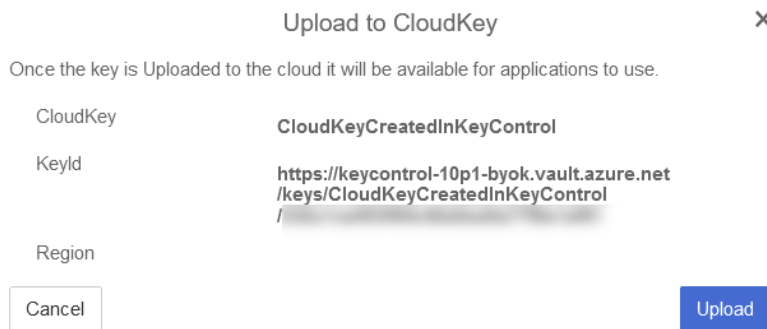
For additional information, see [Removing a CloudKey from the Cloud](#).

5.6. Upload a removed cloud key to Azure in Entrust KeyControl

To upload a removed cloud key to Azure in Entrust KeyControl:

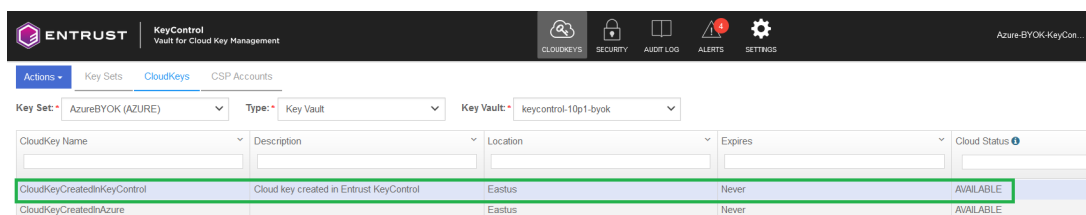
1. Sign in to the Entrust KeyControl Vault URL bookmark from [[test-integration:::create-keycontrol-vault](#)].
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.
4. Select the key to be uploaded.
5. Select **Actions > Upload to Cloud**.

The **Remove from Cloud** dialog appears. For example:

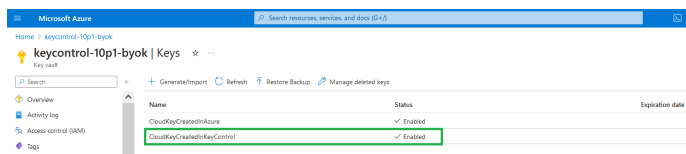


6. Select **Upload**.

7. Verify the status change in Entrust KeyControl. For example:



8. Verify the key is now available in Azure. For example:



5.7. Delete a cloud key in Entrust KeyControl

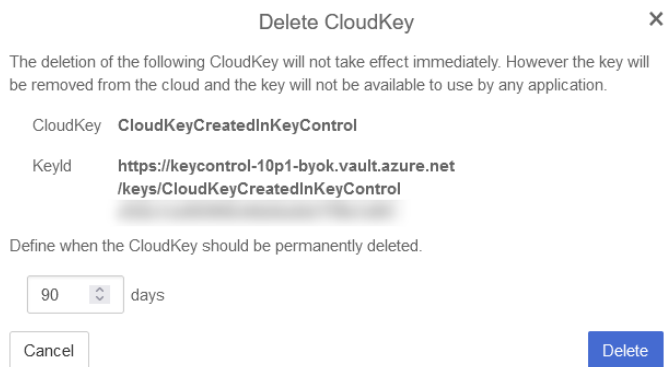
The deletion of a cloud key does not take effect immediately. However, after a user defined interval, the key will be permanently removed.

1. Sign in to the Entrust KeyControl Vault URL bookmark from [\[test-integration:::create-keycontrol-vault\]](#).
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.
4. Select the key to deleted.
5. Select **Actions > Delete CloudKey**.

The **Delete CloudKey** dialog appears.

6. Select a time in **Define when the CloudKey should be permanently deleted**.

For example:



7. Select **Delete**.

8. Verify the status change in Entrust KeyControl.

For example:

CloudKey Name	Description	Location	Expires	Cloud Status
CloudKeyCreatedInKeyControl	Cloud key created in Entrust KeyControl	Eastus	Never	PENDING DELETE
CloudKeyCreatedInAzure		Eastus	Never	AVAILABLE

9. Verify the key is gone from Azure. For example:

Name	Status	Expiration date
CloudKeyCreatedInAzure	✓ Enabled	

For additional information, see [Deleting a CloudKey](#).

5.8. Cancel a cloud key deletion in Entrust KeyControl

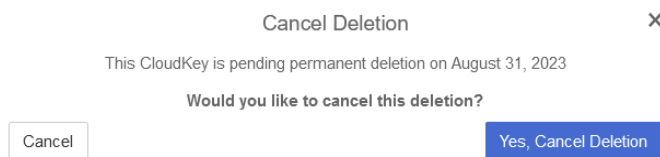
The deletion of a key can be canceled while the time in the **Define when the CloudKey should be permanently deleted** setting has not expired.

1. Sign in to the Entrust KeyControl Vault URL bookmark from [[test-integration:::create-keycontrol-vault](#)].
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.

4. Select the key deletion to be canceled.
5. Select **Actions > Cancel Deletion**.

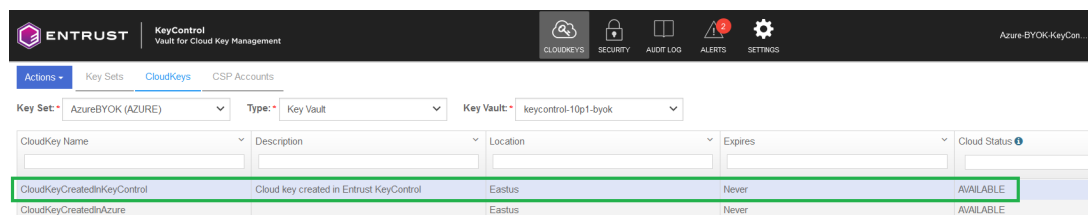
The **Cancel Deletion** dialog appears.

For example:



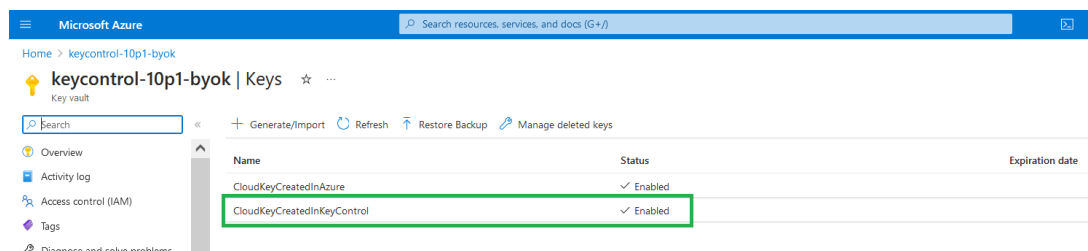
6. Select **Yes, Cancel Deletion**.
7. Verify the status change in Entrust KeyControl.

For example:



CloudKey Name	Description	Location	Expires	Cloud Status
CloudKeyCreatedInKeyControl	Cloud key created in Entrust KeyControl	Eastus	Never	AVAILABLE
CloudKeyCreatedInAzure		Eastus	Never	AVAILABLE

8. Verify the key is now available in Azure. For example:



Name	Status	Expiration date
CloudKeyCreatedInAzure	✓ Enabled	
CloudKeyCreatedInKeyControl	✓ Enabled	

For additional information, see [Canceling a CloudKey Deletion](#).

Chapter 6. Additional resources and related products

6.1. nShield Connect

6.2. nShield as a Service

6.3. KeyControl BYOK

6.4. Entrust digital security solutions

6.5. nShield product documentation