

Bring Your Own Key for AWS Key Management Service and Entrust KeyControl

Integration Guide

2024-11-21

© 2025 Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction
1.1. Product configurations
1.2. Requirements
2. Deploy and configure KeyControl
2.1. Deploy a KeyControl cluster
2.2. Additional KeyControl cluster configuration
2.3. Configure authentication
2.4. Create DNS record for the KeyControl cluster
2.5. Create a Cloud Keys Vault in the KeyControl
2.6. View the Cloud Keys Vault details
3. Create a AWS AIM user service account
3.1. Create a AWS BYOK service account policy
3.2. Create AWS AIM user service account
4. Integrate BYOK for AWS Key Management Service and Entrust KeyControl 15 $$
4.1. Create an AWS CSP account
4.2. Create a key set in KeyControl
5. Test the integration
5.1. Create a cloud key in KeyControl
5.2. Create a cloud key in AWS Key Management Service
5.3. Remove a cloud key in KeyControl
5.4. Delete a cloud key in KeyControl
5.5. Cancel a cloud key deletion in KeyControl
5.6. Rotate a cloud key in KeyControl
6. Integrating with an HSM
7. Additional resources and related products
7.1. nShield Connect
7.2. nShield as a Service
7.3. KeyControl
7.4. KeyControl BYOK
7.5. KeyControl as a Service
7.6. Entrust products
7.7. nShield product documentation

Chapter 1. Introduction

This document describes the integration of AWS Bring Your Own Key (referred to as AWS BYOK in this guide) with the Entrust KeyControl key management solution (KMS). KeyControl serves as a key manager for cloud keys and KMIP objects.

1.1. Product configurations

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

System	Version
Entrust KeyControl	10.3.1

1.2. Requirements

Before starting the integration process, familiarize yourself with:

- AWS Key Management Service
- Entrust KeyControl Online Documentation Set

Chapter 2. Deploy and configure 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 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. Sign in to the console to change the default NTP server if required.

ENTRUST	KeyControl Vault Management			DG ALERTS	SETTINGS	💄 Security Administrator	▼ SAATICH TO: Manage Vaults	?
Actions - Cluster	Servers						Multi-Select 🗆 Refre	esh 🕻
Node Y	Status ~	Server Name				Y IP Address	~	=
Current Node	Online	🖈 Ale TONIC - E CALL F HAR						^
	Online	Automptic Distance over						
								~
Name:		🛨 ka tilgalis i tana turnat						
Status:		Online						
Authenticated:		Yes						
Domain:		Appliance Management Ar	dmin Group					
IP Address:								
Certificate:		Internal Web server: Defa External Web server: Defa	ult ault					

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

2.2. Additional 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 KeyControl cluster

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

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

2.5. Create a Cloud Keys Vault in the KeyControl

The KeyControl Vault appliance supports different type of vaults. For example: cloud key management, KMIP, PASM, database, and others. This section describes how to create a Cloud Keys vault for this integration.

Refer to the Creating a Vault section of the admin guide for more details.

- 1. Sign in to the KeyControl Vault Server web user interface:
 - a. Use your browser to access the IP address of the server.
 - b. Sign in using the **secroot** credentials.
- 2. From the user's dropdown menu, select **Vault Management**.



- 3. In the KeyControl Vault Management interface, select the **Create Vault** icon.
- 4. In the **Create Vault** page, select **Cloud Keys**. Then enter your information.

Create Vault A vault will have unique authentication and management.	
Туре	
Choose the type of vault to create	
Cloud Keys	~
Name*	
AWS-BYOK-KC	
Description	
AWS BYOK integration with Entrust KeyControl	
	//.
Max. 300 characters	
Email Notifications	OFF
Les Mill needs to be configured to turn on email notifications Use email to communicate with Vault Adminsitrators, including their temporary passwords. Turning off email notifications means you will see and need to give temporary passwords to Vault Admins.	
Administrator 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*	
Create Vault Cancel	

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 **secroot**.

Example vault information window:

Vault Successfully Created
You will need to send the following information to the Vault Admin so they can log into their vault
Vault URL
🚯 Сору
User Name
🔁 Сору
Temporary Password
🔁 Сору
Close
Example email:
ENTRUST KeyControl
Administrator, you have been invited to become an administrator of the KMIP vault, CommVault.
To sign in, use the following:
URL:
User Name:
Password:
If you have any issues, <u>contact support</u> .
©2023 Entrust Corporation. All Rights Reserved

6. Bookmark the **Vault URL** listed above.

The newly created Vault is added to the **Vault Management** dashboard.

For example:

ENTRUST KeyControl Vault Management	SWITCH TO: Appliance Management
Vaults Each vault has unique authentication and management	ې Se
Total Vaulte: 2	+ Create V
Cloud Keys	
AWS-BYOK-KC	
AWS BYOK integration with Entrust Key Control	

7. Sign in to the **Vault URL** with the temporary password. Change the initial password when prompted. Sign in again to verify.

For example:



8. Notice the new vault.



2.6. View the Cloud Keys Vault details

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

Vault Details

 \times

AWS-BYOK-KC

AWS BYOK integration with Entrust KeyControl

Туре

Cloud Keys

Created

Jul 30, 2024 03:38:30 PM

Vault URL

Сору

API URL

Copy

Administrator

Admin Name Administrator User Name

Email Notifications Off

2. Select **Close** when done.

Chapter 3. Create a AWS AIM user service account

Entrust KeyControl utilizes an AWS IAM user service account to perform the KMS functionality in BYOK.



In addition to the IAM user service account, the feature to utilize an AWS domain user to perform the KMS functionality is under consideration for a future release of Entrust KeyControl.

The following steps create a customer managed policy in AWS. Then create an IAM user service account with the customer managed policy.

3.1. Create a AWS BYOK service account policy

- 1. Select Services / IAM.
- 2. In the left pane select **Access management** / **Policies**. Then select the **Create policy** icon.
- 3. In the **Specify permissions** window, select the **JASON** icon.
- 4. Copy the following in the **policy editor** window. Then select **Next**



aws	Services Q Search	[Alt+S]	۵	¢	0	۲	-	ADF5-ClaudAdmin/D
Ξ	IAM > Policies > Create policy							
	Step 1 Specify permissions	Specify permissions Info Add permissions by selecting services, actions, resources, and conditions. Build p	ermission st	atemen	ts using	the JSO	N editor.	
	Step 2 Review and create	Policy editor					Vi	sual JSON
		1▼ { 2 "Version": "2012-10-17", 3▼ "Statement": [Edit stateme ServiceAccount
		4 ♥ { 5 "Sid": "ServiceAccountPolicy", 6 "Effect": "Allow",						Add actions
		7▼ "Action": [8 "kms:*", 9 "ec2:DescribeRegions",						Choose a service Q Filter servic
		10 "ssm:GetParameter", 11 "iam:ListUsers", 12 "iam:GetUser",						Included EC2
		13 "iam:CreateAccessKey", 14 "iam:UpdateAccessKey", 15 "iam:ListAccessKeys",						IAM KMS
		16 "iam:DeleteAccessKey" 17], 18 "Resource": "*"						Systems Manage
		19 } 20] 21 }						Available AMP API Gateway

- 5. In the **Review and create** window, enter a name and description.
- 6. In the **Permissions defined for this policy** section, select **KMS**. Then select **Create policy**.

aws	Services Q Search	[Alt+5]
=	IAM > Policies > Create policy Step 1 Specify permissions	Review and create Info Review the permissions, specify details, and taos.
	Step 2 Review and create	Policy details
		Policy name Enter a meaningful name to identify this policy.
		Position rate United to See adjustmenters and +-, genUnited to See See See See See See See See See Se
		Maximum 1,000 characters. Use alphanumeric and '++,,@+_' characters.
		Permissions defined in this policy Into Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM Identity (user, user group, or role), attach a policy to it
		Q, Search <services (55="" 55)<="" actions="" in="" kms="" of="" th=""></services>
		Read (6 of 6)
		DescribeCustomKeyStores All resources None

7. Notice the new policy created.

aws Services Q Search	[Alt+S]
Identity and Access ×	⊘ Policy service-byok-keycontrol created.
Management (IAM)	IAM > Policies
Q Search IAM	Policies (1245) Info
Dashboard	A policy is an object in AWS that defines permissions. Filter by Type
Access management	Q service-byok-keycontrol X All types 1
User groups	Policy name Type
Users	Element of the service-byok-keycontrol Customer managed
Policies	

For further information, refer to the AWS BYOK Service Account Requirements.

3.2. Create AWS AIM user service account

This steps create an AWS IAM user with no console access, a service account, with policy created in Create a AWS BYOK service account policy.

- 1. Select **Services** / **IAM**.
- 2. In the left pane select **Access management** / **Users**. Then select the **Create user** icon.
- Enter the user name. Uncheck Provide user access to AWS Management
 Console optional since we are creating a service account. Then select Next.

aws	Services Q Search	[Alt+5] D & O O
	IAM > Users > Create user Step 1 Specify user details	Specify user details
	Step 2 Set permissions	User details
	Step 3 Review and create	User name service-byok-keycontrol The user name can have up to 64 characters: A-Z, a-z, 0-9, and + = , , @ (hyphen) Provide user access to the AWS Management Console - optional If you're providing console access to a person, it's a best practice [2] to manage their access in IAM identity Center. If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keysnaper, user access the identity is (IM yess Lacess more 16]
		Cancel Next

- 4. In the **Set permissions** window, select the **Attach policies directly** radio button.
- In the Permissions policy section, enter the policy created in Create a AWS BYOK service account policy. Check the policy. Then select Next.

aws	Services Q Search	
=	IAM > Users > Create user	
	Step 1 Specify user details	Set permissions Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more 🖸
	Step 2 Set permissions	Permissions options
	Step 3 Review and create	 Add user to group Add user to an existing group, or create a new group, We recommend using groups to manage user Copy all group memberships, attached managed policies, and inline policies from an existing user. Attach policies directly Attach policies directly Attach and policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
		Permissions policies (1/1247) Create policy Create policy C
		Filter by Type Q. service-byok-keycontrol X All types 1 match
		Policy name [2] Image: Type V Attached entities V
		Customer managed 0

 In the Review and create window, go to section Tags - optional and select Add new tag if required by your organization. Enter the key-value pair. Then select Create user.



Some organizations uses tags manage IAM users key. Check your organization's policies.

For example:

aws	Services Q Search	[Alt+S]		D 4	0 4	۲	•		 _
=	Step 1 Specify user details	Review and create Review your choices. After you create the user, you can view and download	d the autogenerated password, if enabled.						
	Step permissions	User details							
		User name service-byok-keycontrol	Console password type None			R	equire passw o	ord reset	
		Permissions summary							< 1 >
		Name 🖸	▲ Туре			∇	Used as		▽
		service-byok-keycontrol	Customer managed				Permissi	ons policy	
		Tags - optionot Tags are key-value pairs you can add to AWS resources to help identify, organize, Key Q Add new tag Vau can add up to 49 more tags.	or search for resources. Choose any tags you want to Value - optional X	associate wi	th this user.		×	Remove	

7. Notice the new user created.

aws	Services	Q s	earch			[Alt+S]		D	¢	0	۲	•
Ide Ma	ntity and Acc nagement (IA	ess M)	×	<u>iam</u> > 1	Users							
Q	Search IAM			An IAM	S (1) Info user is an identity with long-term of iearch	redentials that is used to i	nteract with AWS in an accoun	t.				
	ess management				User name	▲ Path	▼ Group! ▼	Last acti	vity	⊽	MFA	⊽ Pa
Usei	r groups				service-byok-keycontrol	/	0	-			-	-
Use	rs											
Role	25											

- 8. Select the new user. Then select the **Security credentials** tab.
- 9. In the Access keys (0) section, select the create access key icon.
- 10. In the Access key best practices & alternatives window, select the Third party service radio button. Check I understand the above recommendation and want to proceed to create an access key. Then select Next.



Entrust KeyControl gives you the ability to rotate the access keys. You can set the rotation schedule later on, in Create an AWS CSP account.

aws	Services Q Search	(Alt+5)	Ð	\$	0	⊚ •	,
=	IAM > Users > service-byok-keycor	ntrol > Create access key					
	Step 1 Access key best practices & alternatives	Access key best practices & alternatives Info Anoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.					
	Step 2 - optional	Use case					
	Step 3 Detrieve arress keus	Command Line Interface (CLI) You plan to use this access key to enable the AWS CLI to access your AWS account.					
	Refrieve access keys	O Local code You plan to use this access key to enable application code in a local development environment to access your AWS account.					
		O Application running on an AMS compute service You plan to use this access key to enable application code running on an AMS compute service like Amazon EC2, Amaz					
		• Third-party service You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.					
		Application running outside AWS You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.					
		Other Your use are is not listed here.					
		Atternative recommended As a best practice, use temporary security credentials (IAM roles) instead of oreating long-term credentials like access keys, and don't create AWS acco	unt root user ac	cess keys	s. <u>Learn n</u>	nore 🖸	
		Confirmation Confi					
					Ca	ncel Next	Ĩ

 In the Set description tag - optional window, enter a description tag if desired. Then select Create access key.



12. In the Retrieve access key window, select Download .csv file to download a file containing the Access key and Secret access key. Save these keys. You will need them to Create an AWS CSP account. Then select Done.

aws	Services	Q Search		[Alt+S]	ک	\$	@ @	•	-
Ξ	Access key created the onl	eated y time that the secret access	i key can be viewed or downloaded.	You cannot recover it later. However,	you can create a new a	iccess key a	any time.		
	IAM > User	service-byok-keyconti	ol > Create access key						
	Step 1 Access key be alternatives	st practices &	Retrieve access k	Keys Info					
	Step 2 - optione Set descriptio	n In tag	Access key If you lose or forget your secret acc	cess key, you cannot retrieve it. Instead, crea	ate a new access key and m	nake the old	key inactive	2.	
			Access key	Secret access ke	еу				
	Retrieve acce	ess keys	0	0	100 at 12		Hide	2	
			Access key best praction	ces					
			Never store your access Disable or delete access Enable least-privilege p Rotate access keys regu For more details about manag	s key in plain text, in a code repository s key when no longer needed. permissions. Jlarly. ging access keys, see the best practice	y, or in code. es for managing AWS a	ccess keys.			
							Dov	vnload .csv file	Done

Chapter 4. Integrate BYOK for AWS Key Management Service and Entrust KeyControl

4.1. Create an AWS CSP account

- 1. Sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
- 2. Select the **CSP Accounts** tab.
- 3. In the **Actions** pull down menu, select **Add CSP Account**.
- 4. In the Add CSP Account window, enter the Name and Description.
- 5. In the Admin Group pull-down menu, select Cloud Admin Group.
- 6. In the **Type** pull-down menu, select **AWS**.
- 7. In the **AWS Access Key ID** text box, enter the **Access key** created in Create AWS AIM user.
- 8. In the **AWS Secret Access Key** text box, enter the **Secret access key** created in Create AWS AIM user.
- 9. In the **Default region**, choose your AWS region. Then select **Continue**.

		Add CSP Account	>
Details	Schedule		
Name *			
AWSBYO	KKeyControl		
Description			
AWS BYC	CK integration wit	h Entrust KeyControl	11.
Admin Grou	ib *		
Cloud Adr	min Group		~
Туре *			
AWS			~
AWS Acces	s Key ID *		
AWS Secre	t Access Key *		
Default Reg	jion 🚯		
10.044	to respond to the	6.1	~
Cancel			Continue

10. In the **Schedule** tab, enter your organization's standard rotation schedule for the access keys. Then select **Apply**.

	Add CSP Account	×
Details Schedule		
Define a schedule for which	access keys are rotated.	
Rotation Schedule *		
O Never O Define Sche	dule	
Every 7	days 🗸 (max limit is 1096 days)	
Cancel		Apply

11. Notice the newly created CSP account.

ENTRUST KeyControl Vault for Cloud P	Keys			AWS-BYOK-KC 🚢 Administrator 🔹
	This vault is not c	onnected to KeyControl Compliance Manager.	Connect Now	
Actions - Key Sets CloudKeys C	CSP Accounts			Refresh 🕽
CSP Account Name	Y Description Y	Admin Group ~	Key Set ~	Туре ~ ≡
AWSBYOKKeyControl	AWS BYOK integration with Entrust KeyControl	Cloud Admin Group		AWS

4.2. Create a key set in KeyControl

- 1. sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
- 2. Select the **Key Sets** tab.
- 3. In the Actions pull down menu, select Create Key Set.
- 4. In the Choose the type of keys in this key set: window, select AWS Key.
- In the Create Key Set window, enter a Name and Description. In the Admin Group pull-down menu, select Cloud Admin Group. Then select Continue.

For example:

		Crea	te Key Set	×
Details	CSP Account	HSM	Schedule	
Name *				
AWSBYO	KKeyControl			
Description				
AWS BYC	OK integration with	KeyContro	<u>bl</u>	11.
Admin Grou	tb *			
Cloud Ad	min Group			~
Cancel				Continue

 In the CSP Account tab, select the CSP account created in Create an AWS CSP account. Check Use as External Key Store to allow Entrust KeyControl to encrypt and decrypt the KMS keys. Then select Continue.

	Create Key Set							
Details	CSP Account	HSM	Schedule					
CSP Accour Choose an e	nt * xisting CSP Account	t or add a r	ew one to use with this Key S	et.				
AWSBYO	KKeyControl			~				
+ Add CSP A	Account							
External Ke	y Store							
Enabling exte	ernal key store allow	s KeyCont	ol to encrypt and decrypt KMS	S keys.				
🗌 Use as E	External Key Store							
Cancel				Continue				

7. In the **HSM** tab, check **Enable HMS** if an HSM is configured. Then select **Continue**.

For example:

		Cre	ate Key Se	Create Key Set							
Details	CSP Account	HSM	Schedule								
A Thei can	re is no HSM config be enabled in the	gured. HS Key Set.	M needs to be	configured in Settings before it							
Enable I If checked, the Cloudkeys in Cancel	HSM ⊨ HSM linked to KeyCo this Key Set	ontrol will b	e used for gener	ating cryptographic material for Test Connection Contin	ue						

See Integrating with an HSM for additional information.

8. In the **Schedule** tab, select a **Rotation Schedule** matching the selection made during Create an AWS CSP account. Then select **Apply**.

		Create Key Set					
Details	CSP Accoun	t HSM	Schedule				
efault Clou otation Sc	udKey rotation s	chedule pres	ented during CloudKey crea	tion.			
efault Clou otation Sc Other	udKey rotation s	chedule pres	ented during CloudKey crea	tion.			
efault Clou otation Sc Other Every	udKey rotation s hedule * 7	chedule pres days ►	ented during CloudKey creat	tion.			

9. Notice the newly created key set.

For example:

ENTRUST KeyControl Vault for Cloud Key				AWS-BYOK-KC 🛛 📤 Administrator 👻
	This vault is not c	connected to KeyControl Compliance Manager.	Connect Now	
Actions - Key Sets CloudKeys CS	P Accounts			Refresh ${\cal G}$
Key Set Name Y	Description ~	Admin Group ~	Туре ~	Keys ~ \equiv
AWSBYOKKeyControl	AWS BYOK integration with KeyControl	Cloud Admin Group	AWS	0

For further information, refer to Creating a Key Set in the KeyControl online documentation.

Chapter 5. Test the integration

5.1. Create a cloud key in KeyControl

- 1. Sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
- 2. Select the **CloudKeys** tab.
- 3. In the **Key Set** pull-down menu, select the key set created in Create a key set in KeyControl. In the **Region** pull-down menu, select your region.

For example:

E N	ITRUST	KeyControl Vault for Clou	ud Keys		CLOUDKEYS
				This vault is not connec	ted to KeyCon
Actions -	Key Sets	CloudKeys	CSP Accounts		
Key Set: *	AWSBYOKKey	Control (AWS)	✓ Region: *	~	



Multi-region keys will be supported in a future release of Entrust KeyControl.

- 4. In the **Actions** pull down menu, select **Create CloudKey**. The **Create CloudKey** window appears.
- 5. In the **Details** tab, enter the **Name** and **Description**. Then select **Continue**.

Create CloudKey

×

Details	Purpose	Access	Schedule	
Type Key Set Region	AWS AWSBYC)KKeyContro	pl	
Name *	KKeyControl			
Description	Artey Control			
AWS BYC	OK integration	with Entrust	KeyControl	
Cancel				Continue

 In the Purpose tab, select from the Purpose and Algorithm pull-down menus. Then select Continue.

	×			
Details	Purpose	Access	Schedule	
Choosing a	purpose will d	letermine the	e key type and algorithm selec	ction
Purpose *				
Symmetri	c Encrypt and	decrypt		~
Algorithm *				
AES-256				~
Cancel				Continue

7. In the **Access** tab, select the service account created in Create AWS AIM user in box the **Administrator** and **Users** text box. Then select **Continue**.

For example:

Create CloudKey					2		
Details	Purpose	Access	Schedule				
Administrators Choose users (AWS IAM users) who should have administrative rights to the key.							
service-by	service-byok-keycontrol × Add an Administrator						
Users							
Choose user	s (AWS IAM us	sers) who car	n use key to enc	rypt/decrypt.			
service-by	ok-keycontrol	× Add a U	User				
Cancel					Continue		

8. In the **Schedule** tab, select your **Rotation Schedule** and **Expiration** date. Then select **Apply**.

For example:

	Create CloudKey			>		
Details	Purpose	Access	Schedule			
Rotation Schedule * Define a schedule for which the CloudKey will be rotated.						
Inherit from keyset (Once 7 days)			~			
Expiration * Define when	the CloudKey	should be exp	bired.			
O Never	O Choose a	date				
Cancel				Apply		

9. Notice the newly created cloud key.

ENTRUST KeyControl Vault for Cloud Keys		International State	AWS-BYOK-KC 🛛 🏝 Administrator 👻					
	This vault is not connected to KeyControl Compliance Manager.	Connect Now						
Actions - Key Sets CloudKeys CSP Accounts			Refresh ${\cal G}$					
Key Set • AWSBYOKKeyControl (AWS) V Region: • V								
CloudKey Name ~	Description ~	Expires ~	Cloud Status 🖲 🗧					
AWSBYOKKeyControl	AWS BYOK integration with Entrust KeyControl	Never	AVAILABLE					

10. Verify the cloud key is visible in the AWS Key Management Service (KMS).

Key Management × Service (KMS)	KMS > Customer managed keys > Key ID:	en er an er en en en en er	Kay actions 💌 Edit
AWS managed keys Customer managed keys	General configuration		
Custom key stores AWS CloudH5M key stores External key stores	Allas AWSBYOKKeyControl ARN D	Status Enabled Description AWS BYOK integration with Entrust KeyControl	Creation date Sep 03, 2024 10:59 EDT Regionality Single Region

For further information, refer to Creating a CloudKey in the KeyControl online documentation.

5.2. Create a cloud key in AWS Key Management Service

- In AWS, navigate to Services > Key Management Service > Customer managed keys. Then select the Create key icon.
- In the Configure key window, select the Key type and Key usage. Then expand the Advance options and select the Key material origin. For Regionality select the Single-Region key radio button. Then select Next.

compare key	Configure key	
Step 2 Add labels	Key type Help me choose 🖸	
Step 3 Define key administrative permissions	Symmetric A single key used for encrypting and decrypting data or generating and verifying HMAC codes	ting and iges, or
Step 4 Define key usage permissions	Key usage Help me choose [2]	
Step 5 Review	Encrypt and decrypt Use the key only to encrypt and decrypt data. Generate and verify MAC Use the key only to generate and verify hash message authentication codes (HMAC).	-based
	 Advanced options 	
	Key material origin Key material origin is a KMS key property that represents the source of the key material when creating the KMS key. Help m	e choose 💽
	KMS - recommended MVS KMS creates and manages the key material for the KMS key. Vou create and import the key material for the	he KMS ke
	AWS CloudHSM key store AWS KMS creates the key material in the AWS CloudHSM Cluster of your AWS CloudHSM key store. The key material for the KMS key is in an ext manager outside of AWS.	ernal key
	Regionality	Help me
	Create your KMS key in a single AWS Region (default) or create a KMS key that you can replicate into multiple AWS Regions.	
	Create your KMS key in a single AWS Region (default) or create a KMS key that you can replicate into multiple AWS Regions: choose \mathcal{C}' Single-Region key Never allow this key to be replicated into other Regions	



Multi-region keys will be supported in a future release of Entrust KeyControl.

3. In the Add labels window, enter the Alias and Description. Then select Next.

Services Q Search	[Alt+S]
KMS > Customer managed keys	> Create key
Step 1 Configure key	Add labels
Step 2 Add labels	Alias You can change the alias at any time. Learn more 🔀
Step 3 Define key administrative permissions	Allas AW5BYOKKeyControlCloud
Step 4 Define key usage permissions	Description - optional You can change the description at any time.
step s Review	Description AW5 BYOK integration with Entrust KeyControl
	Tags - optional
	You can use tags to categorize and identify your KMS keys and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. Learn more 🗹 This key has no tags.
	Add tag You can add up to 50 more tags.
	Cancel Previous Next

 In the Define key administrative permissions window, enter the service account name created in Create AWS AIM user and select it. In the Key deletion section, check Allow key administrators to delete this key. Then select Next.

For example:

aws	Services Q Search	[Alt+S]
=	KMS > Customer managed keys > Step 1 Configure key	Create key Define key administrative permissions
	Step 2 Add labels	Key administrators (1/57) Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this conside. Learn more [2]
	Step 3 Define key administrative permissions	Q. service-byok-keycontrol X 1 matches < 1 Imatches V Path V Type V
	Step 4 Define key usage permissions	Service-byok-keycontrol / User
	Step 5 Review	Key deletion
		✓ Allow key administrators to delete this key.
		Cancel Previous Next

5. In the **Define key usage permissions** window, enter the service account name created in Create AWS AIM user and select it. Then select **Next**.

aws	Services Q Search	[Alt+\$]
=	KMS > Customer managed keys > Cre	eate key
	Step 1 <u>Configure key</u>	Define key usage permissions
	Step 2 Add labels	Key users (1/57) Select the IAM users and roles that can use the KMS key in cryptographic operations. Learn more 🗗
	Step 3	Q service-byok-keycontrol X 1 matches < 1 >
	Define key administrative permissions	✓ Name ♥ Path ♥ Type ♥
	Step 4	Service-byok-keycontrol / User
	Define key usage permissions	Other AWS accounts
	Review	Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. Learn more 🗹
		Add another AWS account
		Cancel Previous Next

6. In the **Review** window, select **Finish**.

aws	Services Q Search		[Alt+S]		
=	KMS > Customer managed keys > Creaters Step 1 Configure key	Review			
	Step 2 Add labels	Key configuration			
	Step 3 Define key administrative permissions Step 4 Define key usage permissions Step 5 Review	Key type Symmetric Origin AWS KMS To cannot change the key com Alias and description Alias AWSBYOKKeyControlCloud	Key spec SYMMETRIC_DEFAI Regionality Single-Region key	JLT / is created. Description AWS BYOK integra	Key usage Encrypt and decrypt
		Tags			
		Кеу	Val	ue	
			No di No tags to	ata display	

7. Notice the new key in the AWS KMS.

aws Services Q Search	[Alt+	sj D. 🔶 Ø 🚳 🔹 🔹	ADTS Claubhains, Talles Ranning antications go ethical April	•
Key Management × Service (KMS)	KMS > Customer managed keys > Key ID:	45 78da 4420-8205-9milar127x94	Key actions 🔻 Edit	() ()
AWS managed keys Customer managed keys Custom key stores	General configuration			
AWS CloudHSM key stores External key stores	Alias AWSBYOKKeyControlCloud ARN	Status Enabled Description AWS BYOK integration with Entrust KeyControl	Creation date Sep 03, 2024 14:37 EDT Regionality Single Region	
	Key policy Cryptographic configuration	Tags Key rotation Aliases		

To import the cloud key in KeyControl:

- 1. Sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
- 2. Select the **Key Sets** tab. Then select the key set created in Create a key set in KeyControl.
- 3. In the Actions pull down menu, select **Import CloudKeys**. The **Import Cloud Keys** window appears.
- 4. Select your region. Then select Import.



- 5. Select the CloudKeys tab and select Refresh.
- 6. Verify the imported key is visible in the Entrust KeyControl cloud keys vault.

ENTRUST KeyControl Vault for Cloud Keys		TTS SETTINGS	AWS-BYOK-KC 📤 Administrator 🝷
	This vault is not connected to KeyControl Compliance Manager.	Connect Now	
Actions - Key Sets CloudKeys CSP Accounts			Refresh C
Key Set: * AWSBYOKKeyControl (AWS) V Region: *	×		
CloudKey Name ~	Description ~	Expires ~	Cloud Status 🚯 🗮
AWSBYOKKeyControl	AWS BYOK integration with Entrust KeyControl	Never	AVAILABLE
AWSBYOKKeyControlCloud	AWS BYOK integration with Entrust KeyControl	Never	AVAILABLE

For further information, refer to Importing CloudKeys in the KeyControl online documentation.

5.3. Remove a cloud key in KeyControl

- 1. Sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
- 2. Select the **CloudKeys** tab.
- 3. In the **Key Set** pull-down menu, select the key set created in Create a key set in KeyControl. In the **Region** pull-down menu, select your region.
- 4. Select the key to be removed from the cloud.
- In the Actions pull down menu, select Remove from Cloud. The Remove from Cloud dialog appears.

 Type the name of the key in the Type CloudKey Name text box. Then select Remove.

For example:

For example:

	Remove from Cloud	×
	Removing the key from the cloud will remove the key material from the KM An application will no longer be able to use this key from the cloud. KeyControl Vault will keep a copy of the key. This copy can always be	1S.
	uploaded back to the cloud.	
Are you	sure you want to remove the following CloudKey from the cloud?	
Clou	udKey AWSBYOKKeyControl	
Key	ld	
Type C	loudKey Name *	
AWS	BYOKKeyControl	
Cano	Ren	nove

7. Notice the key **Cloud Status** becomes **NOT AVAILABLE**.

			AWS-BYCK-KC 🛛 💄 Administrator 🝷	
	This vault is not connected to KeyControl Compliance Manager.	Connect Now		
Actions - Key Sets CloudKeys CSP Accounts			Refresh ${\cal G}$	
Key Set • AWSBYOKKeyControl (AWS) V Region: •				
CloudKey Name ~	Description ~	Expires	Cloud Status 🕄 🗮	
AWSBYOKKeyControl	AWS BYOK integration with Entrust KeyControl	Never	NOT AVAILABLE	
AWSBYOKKeyControlCloud	AWS BYOK integration with Entrust KeyControl	Never	AVAILABLE	

8. Verify the key **Status** changed in AWS KMS.

aws Services Q Search	[Alt+S]	ַם ¢ 0 ¢	
Key Management ×	KMS > Customer managed keys > Key ID:	AND THE OWNER DESIGNATION	0
Service (KMS)	00717104-6400-4145-4744		Key actions 🔻 Edit
AWS managed keys Customer managed keys	General configuration		
Custom key stores			
AWS CloudHSM key stores	Alias	Status Rending import	Creation date
External key stores	AWSBTOKKeycontrol	rending import	5eb 05, 2024 10.59 ED1
	ARN	Description	Regionality
	Ð	AWS BYOK integration with Entrust	Single Region
	and there are any total and the	KeyControl	
	and of the state fragments of the		
	Key policy Cryptographic configuration	Key material Tags Aliases	
	cryptographic configuration	Rey material Tags Allases	

For further information, refer to Removing a CloudKey from the Cloud in the KeyControl online documentation.

5.4. Delete a cloud key in KeyControl

- 1. Sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
- 2. Select the **CloudKeys** tab.
- 3. In the **Key Set** pull-down menu, select the key set created in Create a key set in KeyControl. In the **Region** pull-down menu, select your region.
- 4. Select the key to be deleted.
- 5. In the **Actions** pull down menu, select **Delete CloudKey**. The **Delete CloudKey** dialog appears.
- Select a time in Define when the CloudKey should be permanently deleted. Then select Delete.

For example:

 Delete CloudKey
 ×

 The deletion of the following CloudKey will not take effect immediately. However the key will be removed from the cloud and the key will not be available to use by any application.

 CloudKey
 AWSBYOKKeyControl

 Keyld
 Define when the CloudKey should be permanently deleted.

7	$\hat{\cdot}$	days		
Cancel				

7. Notice the key Cloud Status becomes PENDING DELETE.

ENTRUST KeyControl Vault for Cloud Keys			AWS-BYOK-KC 🛛 📤 Administrator 🝷
	This vault is not connected to KeyControl Compliance Manager.	Connect Now	Success ×
Actions - Key Sets CloudKeys CSP Accounts			Cloudkey deleted Successfully
Key Set: • AWSBYOKKeyControl (AWS) V Region: •	×		
CloudKey Name ~	Description	Expires ~	Cloud Status 🖲 🗧
AWSBYOKKeyControl	AWS BYOK integration with Entrust KeyControl	Never	PENDING DELETE
AWSBYOKKeyControlCloud	AWS BYOK integration with Entrust KeyControl	Never	AVAILABLE

Delete

8. Verify the key **Status** changed in AWS KMS.

eral configuration	44-322s2balle110	Key actions 🔻 Edit
eral configuration		
YOKKeyControl	Status Pending deletion Description AWS BYOK integration with Entrust KeyControl	Creation date Sep 03, 2024 10:59 EDT Scheduled deletion date Sep 10, 2024 17:05 EDT
nality Region		
	YOKKeyControl	Status Pending deletion Description AVS BYOK integration with Entrust KeyControl

For further information, refer to Deleting a CloudKey in the KeyControl online documentation.

5.5. Cancel a cloud key deletion in KeyControl

- 1. Sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
- 2. Select the **CloudKeys** tab.
- 3. In the **Key Set** pull-down menu, select the key set created in Create a key set in KeyControl. In the **Region** pull-down menu, select your region.
- 4. Select the key who's scheduled deletion is going to be cancelled.
- 5. In the **Actions** pull down menu, select **Cancel Deletion**. The **Cancel Deletion** dialog appears.
- 6. Select Yes, Cancel Deletion.



7. Notice the key Cloud Status becomes NOT AVAILABLE.

ENTRUST KeyControl Vault for Cloud Keys		100 🔅 RTS SETTINGS	AWS-BYOK-KC 🛛 📥 Administrator 🝷
	This vault is not connected to KeyControl Compliance Manager.	Connect Now	Success
Actions - Key Sets CloudKeys CSP Accounts			CloudKey deletion cancelled Successfully
Key Set: • AWSBYOKKeyControl (AWS) V Region: •			
CloudKey Name ~	Description	Expires ~	Cloud Status 🖲 📃
AWSBYOKKeyControl	AWS BYOK integration with Entrust KeyControl	Never	NOT AVAILABLE
AWSBYOKKeyControlCloud	AWS BYOK integration with Entrust KeyControl	Never	AVAILABLE

8. Verify the key Status changed in AWS KMS.

aws Services Q Search		•
Key Management $ imes$ Service (KMS)	KMS > Customer managed keys > Key ID:	(غ) (ه)
AWS managed keys Customer managed keys	General configuration	
 Custom key stores AWS CloudHSM key stores External key stores 	Allas Creation date AWSBYOKKeyControl Pending import Sep 03, 2024 10:59 EDT ARN Description Regionality Image: Control AWS BYOK integration with Entrust Single Region	
	Key policy Cryptographic configuration Key material Tags Aliases	

- Back in Entrust KeyControl, In the Actions pull down menu, select Upload to Cloud. The Upload to Cloud dialog appears.
- 10. Select **Upload**.

	Upload to Cloud	×
Once the key is uploaded	t to the cloud it will be available for applications	to use.
CloudKey Key Id	AWSBYOKKeyControl	
Region		
Cancel		Upload

11. Notice the key Cloud Status becomes AVAILABLE.

ENTRUST KeyControl Vault for Cloud Keys		10 Internet Settings	AWS-BYOK-KC 🛛 📥 Administrator 🍷
	This vault is not connected to KeyControl Compliance Manager.	Connect Now	
Actions - Key Sets CloudKeys CSP Accounts			Refresh ${f C}$
Key Set: • AWSBYOKKeyControl (AWS) V Region: •	·		
CloudKey Name ~	Description	Expires ~	Cloud Status 🖲 📃
AWSBYOKKeyControl	AWS BYOK integration with Entrust KeyControl	Never	AVAILABLE
AWSBYOKKeyControlCloud	AWS BYOK integration with Entrust KeyControl	Never	AVAILABLE

12. Verify the key **Status** changed in AWS KMS.

aws Services Q Search	[Alt+5] 🖸 🗛 🔞 🔹 🔹	•
Key Management X	KMS > Customer managed keys > Key ID:	١
Service (KMS)	Key actions ▼ Edit	0
AWS managed keys Customer managed keys Custom key stores	General configuration	
AWS CloudHSM key stores External key stores	Alias AWSBYOKKeyControl ARN Description AWS BYOK integration with Entrust KeyControl Control Creation date Sep 03, 2024 10:59 EDT Regionality Single Region	
	Key policy Cryptographic configuration Key material Tags Aliases	

For further information, refer to Canceling a CloudKey Deletion in the KeyControl online documentation.

5.6. Rotate a cloud key in KeyControl

- 1. Sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
- 2. Select the **CloudKeys** tab.
- 3. In the **Key Set** pull-down menu, select the key set created in Create a key set in KeyControl. In the **Region** pull-down menu, select your region.
- 4. Select the key to be rotated.
- 5. Scroll down, select the **Details** tab, and select the **Rotate Now** icon.

ENTRUST KeyControl Vault for Cloud Keys				AWS-BYOK-KC 📥 Administrator =
AWSBYOKKeyControl	AWS BYOK integration with Entrust KeyControl		Never	AVAILABLE
AWSBYOKKeyControlCloud	AWS BYOK integration with Entrust KeyControl		Never	AVAILABLE
Details Sharing Tags Varsions				C Sync Now
Name:	AWSBYOKKeyControl			
Key Id:				
Description:	AWS BYOK integration with Entrust KeyCon	trol		
Cloud Status 3 :	AVAILABLE			
Key Source:	KEYCONTROL			
Key Set:	AWSBYOKKeyControl			
Algorithm:	AES-256			
Кеу Туре:	Symmetric			
Purpose:	Symmetric Encrypt and decrypt			
Default Region:	OF CARLON Program in cash			
Rotation Schedule:	Every 1 week			
	Rotate Now			
Key Upload Date:	09/03/2024			

6. Verify that the key has been rotated in AWS KMS.

aws Services Q S	earch			D	Alt+S]		۵	¢	0 0	0	•	-	-	-	-	•	
Key Management × Service (KMS)	×	<u>kms</u> >	Customer managed keys													٢	
		Cus	stomer managed keys (13)											Currente		9	
AWS managed keys Customer managed keys		٩	Filter keys by properties or tags									K	y actions 🔻	Create	©		
Custom key stores AWS CloudHSM key stores External key stores After I		Aliases	~	Key ID	⊽	Status		Key typ	e	▼ Key	spec 🚯	Key usa	ge				
	Before	۰ 🗘	-		00f17c84-4a0	<u>00-</u>	Enabled		Symmet	tric	SYM	METRIC_DE	Encrypt	and decrypt			
	After	\$ 0	AWSBYOKKeyControl		110626cd-a90	d7	Enabled		Symmet	tric	SYM	METRIC_DE	Encrypt	and decrypt			

Chapter 6. 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 7. Additional resources and related products

- 7.1. nShield Connect
- 7.2. nShield as a Service
- 7.3. KeyControl
- 7.4. KeyControl BYOK
- 7.5. KeyControl as a Service
- 7.6. Entrust products
- 7.7. nShield product documentation