



Amazon Web Services KMS External Key Store (XKS)

KeyControl Cloud Key Management Vault (HYOK) Integration Guide

2024-02-26

 $\ensuremath{\mathbb{C}}$ 2024 Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction
1.1. Product configuration
1.2. Requirements
1.3. Overview
2. Procedures
2.1. Prerequisites
2.2. Adding an Elastic Load Balancer
2.3. Configure certificates and DNS
2.4. Key Administrators - AWS IAM user
2.5. Create a Cloud Key Management Vault
2.6. Create a CSP Account in the Cloud Key Management Vault
2.7. Create the Key Set
2.8. Create an External Key Store in AWS
2.9. Test the integration
3. Additional resources and related products
3.1. nShield Connect
3.2. nShield as a Service
3.3. Entrust digital security solutions
3.4. nShield product documentation

Chapter 1. Introduction

This guide describes the integration of the Entrust KeyControl Cloud Key Management Vault with Amazon Web Services KMS External Key Store (XKS).

Entrust KeyControl Cloud Key Management Vault provides an External Key Store Proxy inside KeyControl Vault. This feature allows the KeyControl Vault administrator to protect their data within Amazon Web Services (AWS) with 256bit AES keys residing in KeyControl Vault. KeyControl Vault generates the keys and the keys are stored in KeyControl Vault only.

1.1. Product configuration

Product	Version	Certification
KeyControl Vault	10.1.1	FIPS 140-2 Level 1
	10.2	

Entrust has successfully tested the following software version:

1.2. Requirements

To integrate Entrust KeyControl Cloud Key Management Vault and Amazon Web Services KMS External Key Store (XKS), the server must be set up as follows.

- You must have an AWS account with KMS access allowed.
- There is a minimum of 2 KeyControl instances within a cluster. These instances must be accessible through a load balancer, typically realized using Elastic Load Balancer in the AWS environment.

This integration uses a public endpoint connectivity for AWS XKS. The following are required:

- Your external key store proxy must be reachable at a publicly routable endpoint.
- You must obtain a TLS certificate issued by a public certificate authority supported for external key stores. For a list, see https://github.com/aws/aws-kms-xksproxy-api-spec/blob/main/TrustedCertificateAuthorities.
- The subject common name (CN) on the TLS certificate must match the

domain name in the proxy URI endpoint for the external key store proxy. For example, if the public endpoint is https://myproxy.xks.example.com, the TLS, the CN on the TLS certificate must be myproxy.xks.example.com or *.xks.example.com.

• Ensure that any firewalls between AWS KMS and the external key store proxy allow traffic to and from port 443 on the proxy. AWS KMS communicates on port 443 and this value is not configurable.

Familiarize yourself with:

- Entrust KeyControl and AWS External Key Store (XKS) Overview
- The Amazon Web Services KMS External Key Store (XKS) Documentation

1.3. Overview

Entrust KeyControl Cloud Key Management Vault provides an External Key Store Proxy within KeyControl. This feature allows KeyControl administrators to safeguard their data within Amazon Web Services (AWS) using 256-bit AES keys housed in the KeyControl Vault. KeyControl generates the keys, which are exclusively stored in KeyControl.

In this guide:

- BYOK (Bring Your Own Key): This approach involves generating and managing encryption keys within an external key management system, such as the Amazon Web Services Key Management Service (AWS KMS). BYOK allows you to maintain control over your encryption keys while utilizing the services provided by AWS.
- HYOK (Hold Your Own Key): This method takes data security a step further by enabling you to retain absolute control over encryption keys, even when data is processed in cloud environments. With HYOK, the encryption keys are stored outside the cloud provider's infrastructure.

Entrust supports both BYOK and HYOK approaches to data security. This integration is HYOK implementation, ensuring that encryption keys are held within our control while still harnessing the benefits of cloud services.

For more information about the BYOK approach, refer to *Bring Your Own Key for AWS Key Management Service and Entrust KeyControl Integration Guide*.

Chapter 2. Procedures

Integration steps:

- 1. Prerequisites
- 2. Adding an Elastic Load Balancer
- 3. Configure certificates and DNS
- 4. Key Administrators AWS IAM user
- 5. Create a Cloud Key Management Vault
- 6. Create a CSP Account in the Cloud Key Management Vault
- 7. Create the Key Set
- 8. Create an External Key Store in AWS
- 9. Test the integration

2.1. Prerequisites

Before integrating Entrust KeyControl Vault server and AWS External Key Store (XKS), ensure the following:

- Entrust KeyControl Vault server is deployed and configured. For details, see KeyControl Installation.
- Entrust KeyControl Compliance Manager is deployed and configured.

For this integration, the KeyControl Vault servers were deployed using AWS EC2 instances. To learn more about deploying KeyControl Vault in Amazon Web Services, refer to Creating KC Cluster AWS.

However, KeyControl Vault servers can also be deployed outside of AWS EC2, provided they fulfill the requirements outlined in [procedures:::requirements].

2.2. Adding an Elastic Load Balancer

After cluster set-up is complete, you must use AWS elastic load balancing for the KeyControl load balancing.

For more information on AWS ELB, refer to AWS ELB Documentation.

2.2.1. Configure target group

To configure the target group:

- 1. Sign in the Amazon EC2 console.
- 2. In the navigation pane, under Load Balancing, select Target Groups.
- 3. Select Create target group.
- 4. Under Basic configuration:
 - a. Select **Instances** as target type.
 - b. For **Target group name**, enter a name for the new target group.
 - c. For **Protocol**, select **HTTPS**.
 - d. For Port, select 443.
 - e. Select the VPC containing your instances.
 - f. For **Protocol version**, retain the default.

Settings in this	section can't be changed after the target group is created.
Choose a tar	get type
 Instand Instand Instand 	ces Supports load balancing to instances within a specific VPC. Facilitates the use of Amazon EC2 Auto Scaling 🔀 to manage and scale your EC2 capacity.
O IP add	resses Supports load balancing to VPC and on-premises resources. Facilitates routing to multiple IP addresses and network interfaces on the same instance. Offers Resibility with microservice based architectures, simplifying inter-application communication. Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.
C Lambd	la function Facilitates routing to a single Lambda function. Accessible to Application Load Balancers only.
O Applica	ation Load Balancer Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC. Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.
Target group	name
A maximum of	32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.
Protocol HTTPS VPC Select the VPC	Port V I I I I I I I I I I I I I I I I I I
keycontrolt	est-vpc
 Protocol vers HTTP1 Send reque HTTP/2. HTTP2 Send reque but gRPC-s 	ion ests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or ests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, specific features are not available.
gRPC Send reque	ests to targets using gRPC. Supported when the request protocol is gRPC.

5. Under Health checks:

- a. For Health check protocol, select HTTPS.
- b. Retain the default settings for other properties.

Health checks The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.
Health check protocol HTTPS Health check path Use the default path of */* to ping the root, or specify a custom path if preferred.
Up to 1024 characters allowed.
Advanced health check settings

- 6. Select Next.
- 7. On the **Register Targets** page, complete the following steps. This is an optional step for creating the load balancer. However, you must register this target if you want to test your load balancer and ensure that it is routing traffic to this target.
 - a. For **Available instances**, select the two KeyControl instances.
 - b. For **Port for the selected instances**, enter **443**, and select **Include as pending** below.
 - c. Select Create target group.

Available instances (2)															
Filter resources	s by property or value														< 1
Instance ID	· · · ·	Name	♥ Stat	tus	♥ Secur	ity groups	w Zone	v Subnet I							
i-0a218fd98	8e961c245	aws-xks-keycontrol-nod	e-1 Ø#	tunning	test		us-east-1a	subnet-0	a461						
i-0a9b910cc	cfbf357ab	aws-xks-keycontrol-nod	e-2 ØR	Running	test		us-east-1a	subnet-0	a469c						
								0 selected							
							Ports for th	selected instances							
							Ports for rou	ing traffic to the selected instar	205.						
							443								
							443 1-65535 (w)	rate multiple ports with comm	40						
							443 1-65535 (w)	rate multiple ports with comm clude as pending below							
							443 1-65535 (sej 1 2 selections are now per	rate multiple ports with comm clude as pending below ing below. Include more or regist	n)						
view targets							443 1-65535 (au 1 2 selections are now per	rate multiple ports with comm clude as pending below ing below. Include more or regist	n)						
iew targets							443 1-65535 (asj 2 selections are now per	rate multiple parts with comm clude as pending below ing below. Include more or regist	n)						
view targets Fargets (2)							443 1-65555 (say 2 telections are now per	irate multiple ports with conve clude as pending below ing below, include more or regist	a)						Remove all pend
riew targets Targets (2) All	 Q. Filter resource 	zes by property or value					443 1-65535 (ar 2 telections are now por	rate multiple parts with conve clude as pending below ing below. Include more or regist	n)						Remove all pend
riew targets Fargets (2) All serve	Q Filter resource Health statu	zes by property or volue	Instance ID		v		443 1-65535 (au 2 soluctions are new per	nate multiple parts with correct clude as pending below ing below, include more ar regist	n) targets when ready. State	v Security gro	25 🖤	Zone	♥ Subset IC		Remove all pend
Targets (2) All remove		ces by property or value a v v	Instance ID +Oa218fd		7	Name ave-ski-keycentoik-tode-1	445 1-65335 far 2 subschere en now per	cate multiple ports with some clude as pending below ing boles, include more or regist Port V 443	n) tarspets when ready. State ORunning	v Security gro test	5 ¥	Zone us-east-1a	v Subset 10 subset-00	a469i	Remove all pend

2.2.2. Create an Elastic Load Balancer

To create an Elastic Load Balancer:

1. Sign in to the Amazon EC2 console.

- 2. On the navigation bar, select a region for your load balancer. You must select the same region that you used for your EC2 instances.
- 3. In the navigation pane, under Load Balancing, select Load Balancers.
- 4. Select Create Load Balancer.
- 5. Select Application Load Balancer, select Create.



- 6. Under Basic configuration:
 - a. For Load balancer name, enter a name for your load balancer.
 - b. For Scheme, select Internet-facing.
 - c. Retain the IP address type default.

Basic configuration
Load balancer name Name must be unique within your AWS account and can't be changed after the load balancer is created.
test
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.
Scheme Info Scheme can't be changed after the load balancer is created. Intermet-facing An intermet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more C Intermal An internal load balancer routes requests from clients to targets using private IP addresses.
IP address type Info Select the type of IP addresses that your subnets use. O IPV4 Recommended for internal load balancers.
Dualstack Includes IPv4 and IPv6 addresses.

- 7. Under Network mapping:
 - a. For **VPC**, select the VPC that you used for your EC2 instances.

- b. For **Mappings**, select at least two Availability Zones and one subnet per zone.
- c. For each Availability Zone that you used to launch your EC2 instances, select the Availability Zone and then select one public subnet for that Availability Zone.
- d. You must select at least one Availability Zone that was used when launching your instances.

Network mapping Info The load balancer routes traffic to targets in th	e selected subnets, and in accordance with your IP address settings.	
VPC Info Select the virtual private cloud (VPC) for your t the load balancer is created. To confirm the VP	argets or you can create a new VPC 🚺. Only VPCs with an internet gateway are enabled for sele C for your targets, view your target groups 🚺.	ection. The selected VPC can't be changed after
keycontroltest-vpc vpc-036ec5bi IPv4: 10.0.0.0/16	Ŧ	C
Mappings Info Select at least two Availability Zones and one s balancer or the VPC are not available for select	ubnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability	ability Zones that are not supported by the load
✓ us-east-1a (use1-az2)		
Subnet		
subnet-0ea469d	keycontroltest-subnet-public1-us-east-1a 🔻	
IPv4 address		
Assigned by AWS		
✓ us-east-1b (use1-az4)		
Subnet		
subnet-0358a1d1	keycontroltest-subnet-public2-us-east-1b 🔻	
IPv4 address Assigned by AWS		

- 8. Under Security groups:
 - a. For **Security group**, select the default security group for the VPC that you selected in the previous step. Alternatively, you can select a different security group.
 - b. Ensure that the security group includes rules that allow the load balancer to communicate with registered targets on both the listener port and the health check port.
 - c. You must include the VPC source in the inbound rule to allow access to all ports or the port you are using as a listener.

Security groups Info A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group 🔀							
Security groups Select up to 5 security groups C test sg-034600: X VPC: vpc-036ec5b2-							

- 9. Under Listeners and routing:
 - a. For **Protocol**, retain the default setting.
 - b. For **Port**, retain the default setting.
 - c. For **Default action**, select the **Forward to** action and select the target group that you created and registered.
 - d. Keep the **Add-on services** and **Load balancer** tags unchecked and left as default.

This configures a listener that accepts HTTP traffic on port 80 and forwards traffic to the selected target group by default.

Listeners and routing Info Listener is a process that checks for connection requests using the port and pro o its registered targets.	stocol you configure. The rules that you define for a listener determine how the load bal	ancer routes requests
▼ Listener HTTP:80		Remove
Protocol Port Default acti HTTP V: 80 Forward to 1-65535 Create target	on Info Select a target group ▲ tt Q	C
Listener tags - optional Consider adding tags to your listener. Tags enable you to categorize your AW Add listener tag You can add up to 50 more tags.	In use S test HTTPS Target type: Instance, IPv4	
Add listener		

- 10. Review your configuration and select **Create load balancer**. A few default attributes are applied to your load balancer during creation. You can view and edit them after creating the load balancer.
- 11. Select Create load balancer.

est Internet-facing IPv4	• test sg-0346003	VPC vpc-036ec5b2 keycontroltest-vpc • us-east-1a subnet-0es469d5 keycontroltest-subnet-public1-us- east-1a • us-east-1b subnet-0358a1d1a keycontroltest-subnet-public2-us- east-1b	HTTP:80 defaults to Target group not defined
Add-on services Edit		Tags Edit	
Attributes G Certain default attributes	will be applied to your load balancer. You can	view and edit them after creating the load	balancer.

After you receive the notification confirming the successful creation of your load balancer, follow the steps below to verify the status of your instances and test the load balancer.

EQ 2 Ladibilitations							
Load balances (1/1) C Actions • Create load balances (2/1) Easts: Load bilances (2/1) Easts: Load bila							
Q. Indimensional by diffuence of the general sector of the							
😰 Name v DNS name v State v VPCID v Availability.Zones v Type v Date created							
v test	Active vpc-036ec5b <u>2 Availability Zones</u> applicate	an June 13, 2023, 14:26 (UTC-04:00)					
Load balancer: test Details Listeners Network mapping Security Monitorin Details Details Entering Monitorin	Load balancer: test = 2000 2000 2000 2000 2000 2000 2000 2						
Laad balancer type Application Scheme Internet-fading	Status ØAche Hotad ane Z35500	VPC Image: Constraint of the second sec	IP address type IPv4 Date crosted June 13, 2023, 14/26 (JJT, OK00)				
Load balancer ARN G arrcawsclasticloadbalancingus-east-1:594691249913:loadbalancer/app/test	Laad balance ASN Dis constrained of the State of the Stat						

- 1. After you are notified that your load balancer was created successfully, select **Close**.
- 2. In the navigation pane, under **Load Balancing**, select **Target Groups**.
- 3. Select the newly created target group.
- 4. Select **Targets** and verify that your instances are ready.

If the status of an instance is **Initial**, the instance is either in the process of being registered or has not passed the minimum number of health checks to be considered healthy. Wait until the status of at least one instance is **Healthy**. For example:

Detai	Details Targets Monitoring Health checks Attributes Tags							
Regi	Registered targets (2) C Deregister Registere targets (2) C The reparate to monotoria value (1)							
	Instance ID	v Name	v Port	v Zone	▼ Health status	v Health status details		
	i-0a218fd5	aws-xks-keycontrol-node-1	443	us-east-1a	⊘ healthy			
	i-0a9b910c	aws-xks-keycontrol-node-2	443	us-east-1a	⊘ healthy			

2.3. Configure certificates and DNS

For the successful set-up of AWS External Key Store (XKS), note that the DNS record and TLS certificate relate to the Fully Qualified Domain Name (FQDN) of the load-balanced endpoint utilized for accessing the service. This is distinct from the KeyControl instances.

Ensure the KeyControl Vault server possesses a publicly accessible IP address and that a DNS record is in place for the designated common name within the public DNS server.



Amazon recommends a round-trip time latency of under 35 milliseconds between the AWS region and the KeyControl.

You must obtain a TLS certificate issued by a public certificate authority supported for external key stores. For a list, see https://github.com/aws/aws-kms-xksproxy-api-spec/blob/main/TrustedCertificateAuthorities

To ensure seamless access across the cluster nodes, you must install the TLS certificate on all nodes of the cluster, especially if users plan to access the cluster through other nodes. If an Elastic Load Balancer (ELB) is part of the set-up, the certificate handling process will differ. When using an ELB, the TLS certificate must be managed according to ELB requirements.

- 1. In the KeyControl Appliance Management:
 - a. Navigate to **Cluster > Servers**.
 - b. Select the server to install the certificate.
 - c. Select Actions > Install Certificate. The Install Custom SSL Certificate dialog appears.
 - d. Locate and select the SSL Certificate file.
 - e. Locate and select the CA certificate chain file.
 - f. Select **External** for the Web server.
 - g. Select Install Certificate.

Install Custom SSL Certificate

Certificate	Private Key
SSL Certificate:	ServerCertificate.crt Clear Preview Certificate needs to be in base64 encoded pem format.
CA Certificate:	ChainBundle2.crt Clear Preview Certificate needs to be in base64 encoded pem format.
Web server	External Internal Choose which web server to install the custom certificate.
Close	Install Certificate

2. After installation, restart the Web service

🜔 ENTRUST	KeyControl Appliance Management	CUISTER AUGTLOG ALERTS SETTINGS	•
Actions - pde	Online	★ ip-10- internal 10.0.9.88	
	Online	ip-10-0 internal 10.0.2.14	
Name:		🖈 ip-10-0- ternal	
Status:		Online	
Authenticated:		Yes	
Domain:		Appliance Management Admin Group	
IP Address:		10.0.9.88	
Certificate:		Internal Web server: Default	
		External Web server: Defaul Restart Web Service	

3. Confirm the installation. The External Web server will now show as **Custom** for the certificate.

Name:	★ ip- ec2.internal
Status:	Online
Authenticated:	Yes
Domain:	Appliance Management Admin Group
IP Address:	
Certificate:	Internal Web server: Default External Web server: Custom
Encryption Status:	No rekey is in progress

4. You can validate the certificate using https://entrust.ssllabs.com/ or a similar tool. For example:





If you are not able to verify the server hostname, ensure that any firewalls between AWS KMS and the external key store proxy allow traffic to and from port 443 on the proxy.

2.4. Key Administrators - AWS IAM user

To enable the integration, you must designate an IAM user as a Key Administrator. This user is required to generate an access key that will be used in a later step.

This user must have permissions to manage and use the KMS key for cryptographic operations.

- 1. Sign in to the AWS Management Console.
- 2. Search for the Identity and Access Management (IAM) service and select it.
- In the IAM console, select Access Management in the left tab and then select Users.
- Create a new user or use an existing user to generate an access key. In this example integration, a new user named xks-user is created as the Key Administrator.

IAM > Users							
Users (4) Info An IAM user is an identity with long-term cred	lentials that is used to inte	eract with AWS in an ac	count.			2 Delete	Add users
Q xks-user				×	1 match		< 1 > 🕲
User name \bigtriangledown	Groups 🗢	Last activity 🗢	MFA	\bigtriangledown	Password a… ▽	Active key age	\bigtriangledown
xks-user	users and Administrator	오 1 hour ago	None		오 24 hours ago	🕑 24 hours ago	

5. In the user settings, select **Create access key** and select **third-party service**.

2005 III Services Q. Search		(Atris) B 4	0 Gk	bul 🕶 🕴 A
Identity and Access X Management (IAM)	IAM 🏷 Users 🗲 keycontroltestuser	> Create access key		
Q. Search IAM	Step 1 Access key best practices & alternatives	Access key best practices & alternatives Avoid using long-term conformation like access legs to improve your accurdy. Consider the following use cases and alternatives.		
Access management User groups	Step 2 - optional Set description tag	C Command Line Netrofice (12.8) Nay jales to use this access tays to enable the ABS CL/15 access pair ABS accurat.		
Users Roles Policies	Sep 5 Retrieve access keys	Local code too junctions buy to enable application code its a local devolutioner environment to access pure fill's assumed.		
Identity providers Account settings		O Application contribution on AM AMS computer service they plant to use this access key to enable application inder noneing on an AMS computer service like Amazon EC2, Ama		
Access reports Access analyzer Archive rules		The dyperty service The plant bases have a third-perty application or service that monitors or managery par AMS wisacres.		
Analyzers Settings Crodential report		Application number particle MMS Toppington to an the access large the analysis and accessing as an expendition hast, or to are a local XMS clerk or the Approx MMS plaque.		
Organization activity Service control policies (SCPs)		C Other This vasion can be not literative.		
Related consoles		Attenuative recommended As a best practice, one temporary security condensials (IAM roles) instead of creating long-term condensials like access logs, and durit create RMS account noet access logs, Learn more C		
AWS Organizations 🕑		I understand the above recommendation and want to proceed to create an access key.	uncel N	level .

6. Create the access key.

Services Q Search		[Alt+S] D 🗘 Ø Global 🔻
Identity and Access × Management (IAM)	IAM > Users > keycontroltestu	ser 🖒 Create access key
	Step 1 Access key best practices &	Set description tag - optional
Q Search IAM	alternatives	The description for this access key will be attached to this user as a tag
Dashboard	Step 2 - ontional	and shown alongside the access key.
Access management	Set description tag	Description tag value
User groups		Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.
Users	Step 3 Retrieve access keys	keycontroltestkey
Roles		Maximum 256 characters. Allowed characters are letters, numbers, spaces
Policies		representable in UTF-8, and: : / = + - @
Identity providers		
Account settings		Cancel Previous Create access key



Ensure that you securely store the Access ID and Secret Access Key, as they are required for accessing and managing your AWS resources.

2.5. Create a Cloud Key Management Vault

The KeyControl Vault appliance supports the following types of vaults:

- Cloud Key Management Vault for cloud keys such as BYOK and HYOK.
- **KMIP Vault** Vault for KMIP Objects.
- **PASM** Vault for objects such as passwords, files, SSH keys, and so on.
- **Database** Vault for database keys.
- Tokenization Vault for tokenization policies.
- VM Encryption Vault for encrypting VMs.

To create a Cloud Key Management Vault:

- 1. Sign in to the KeyControl Vault Server Appliance Manager.
- 2. Open the drop-down menu and select **Vault Management**.

SECROOT 💄	
Help	F
API Documentation	
Vault Management	
Logout	

The KeyControl Vault Management interface appears.

ENTRUST KeyControl Vault Management		Lescroot v SWITCH TO: Applicance Management ?
Vaults Each vault has unique authentication and management		Settings
	+	
	Let's get started!	
	+ Create Vault	

3. Select Create Vault.

The Create Vault page appears.

- 4. On the Create Vault page:
 - a. For Type, select Cloud Key Management.
 - b. Enter a **Name** for the vault.
 - c. Provide a **Description** for the vault.
- 5. Under **Administration**:
 - a. Enter the **Admin Name** who will be responsible for the vault.
 - b. Enter a valid **Admin Email** address.

Create Vault
A vault will have unique authentication and management.
Type Choose the type of vault to create
Cloud Key Management
Name*
AWS-XKS
Description
AWS XKS
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 *
Admin Email *
Create Vault Gancel

6. Select Create Vault.

If you set up an administrator email address when you logged in for the first time, a temporary password is mailed to that address. This is the password you must use when you sign in for the first time to Vaults space in KeyControl.

If you did not set up an email configuration when you logged in for the first time, a password is shown in the Vault Details when you create a Vault for the first time. You must make a note of the password at this time, as it will not be included in the Vault Details afterwards.

7. Select **Close**.

The newly created vault is displayed in the **Vaults** dashboard.

	RUST	KeyControl Vault Manageme	nt	
Vaults Each vault has u	nique authentica	tion and managemen	nt	
Total Vault	61			
AWS-XKS	Cloud Key KS	Management		

8. To view the details of a vault, hover over the vault and select **View Details**.

Vault Details	×
AWS-XKS AWS-XKS	
Type Cloud Key Management	
Created Jun 13, 2023 10:44:24 AM	
Vault URL	
Сору	
API URL	
Сору	
Administrator	

Close

To edit the details of a vault:

- 1. Hover over the vault and select **Edit**.
- 2. Make the required changes and select **Apply**.

Vaults Each vault has unique authentication and management	
Edit Vault	
Type Cloud Key Management	
Name*	
AWS-XKS	
Description	
AWS-XKS	
Max. 300 characters	
Administrator	
Apply Cancel	🛱 Delete Vault

2.6. Create a CSP Account in the Cloud Key Management Vault

To create a CSP Account in the Cloud Key Management Vault:

- 1. Sign into the newly created vault.
- 2. Select Cloud Keys > CSP Accounts > Actions > Add CSP Account.

ENTRUST KeyControl Vault for Cloud Key Management	CLOUDKEYS SECURITY AUDIT LOG A		aws-xks 💄 🔹 👻
Actions - Key Sets CloudKeys CSP Accounts			Refresh ${f C}$
Add CSP Account	in Group ~	Key Set ~	Type ~ =

There are no CSP Accounts to show. Please add one from Actions.

The Add CSP Account dialog appears.

- 3. In the **Details** page:
 - a. For **Name**, enter a name for the CSP account.
 - b. Add a **Description**.
 - c. For Admin Group select Cloud Admin Group.
 - d. For **Type** select **AWS**.
 - e. Enter the AWS Access Key ID and AWS Secret Access Key from earlier.
 - f. Select the target region as the default region.
 - g. Select Continue.

Add CSP Account	×
Details Schedule	
Name *	
aws_csp	
Description	
aws_csp	
Admin Group •	
Cloud Admin Group	~
Type *	
AWS	~
AWS Access Key ID *	
AKIAYU5S4K3	
AWS Secret Access Key *	
Wef8bWtYphaG2unb623HT	
Default Region 0	
US East (N.Virginia) us-east-1	~
Cancel	Continue

4. In the **Schedule** page:

- a. Select the required Rotation Schedule.
- b. Select **Apply**.

	Add CSP Account	×
Details	Schedule	
Define a sch	edule for which access keys are rotated.	
Rotation Sch	nedule *	
Never	O Define Schedule	
Cancel		Apply

2.7. Create the Key Set

To create the Key Set:

1. Under CloudKeys, select Key Sets > Create a Key Set Now.

EN1	RUST	KeyContro Vault for Clo	ol Dud Key Management	c	CLOUDKEYS	SECURITY	AUDIT LOG	ALERTS	SETTINGS	AWS-XKS	🐣 jadonm	lichael.dejes 🔻
Actions -	Key Sets	CloudKeys	CSP Accounts									Refresh ${\cal G}$
				There a	are cui Create	rrently a Key Se	no Key et Now	Sets				

2. Select **AWS Key** for the type of keys in key set.



The Create Key Set dialog appears.

- 3. In the **Details** page:
 - a. Enter a **Name**.
 - b. Enter a **Description**.
 - c. For Admin Group, select Cloud Admin Group.
 - d. Select Continue.

		Cre	ate Key Set	×
Details	CSP Account	HSM	Schedule	
Name *				
aws_xks_	keyset			
Description				
<u>aws_xks</u>	kevset			li
Admin Grou	tb *			
Cloud Ad	min Group			~
Cancel				Continue

- 4. In the CSP Account page:
 - a. For **CSP Account**, select the <u>aws_csp</u> account created earlier.
 - b. Select Use as External Key Store.
 - c. Make a note of the XKS credentials, as these are required later.
 - d. Select **Continue**.

		Cre	eate Key Set	×
Details	CSP Account	HSM	Schedule	
CSP Accou Choose an e	nt * existing CSP Accoun	it or add a i	new one to use with this Key Se	ət.
aws_csp				~
+ Add CSP	Account			
External Ke	ey Store			
Enabling ext	ernal key store allov	vs KeyCon	trol to encrypt and decrypt KMS	8 keys.
Use as E Access Ke Secret Access	External Key Store ey ID: X526QQ6ZN cess Key: **********	****		
Copy an	d add this Access	Key ID and	I Secret Access Key to your A	AWS KMS Portal
Cancel				Continue

- 5. In the **HSM** page:
 - a. Optionally select **Enable HSM**.
 - b. Select Continue.

	Create Key Set							
Details	CSP Account	HSM	Schedule					
A The Man	A There is no HSM configured. HSM needs to be configured in Appliance Management, before it can be enabled in the Key Set.							
Enable I If checked, the this Key Set.	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				

To set up an HSM linked to KeyControl, follow the installation and set-up instructions in the *Entrust KeyControl nShield HSM Integration Guide*.

6. In the **Schedule** page:

E

- a. For Rotation Schedule, select your required CloudKey rotation.
- b. Select **Apply**.

Create Key Set				×	
Details	CSP Account	HSM	Schedule		
Default Clo Rotation Sc	udKey rotation sch hedule *	edule pres	ented during Cloudk	Key creation.	
Never					~
Cancel					Apply

2.8. Create an External Key Store in AWS

To create an External Key Store in AWS:

- 1. Sign in to the AWS console and navigate to Key Management Service (KMS).
- 2. In the left panel, select **Custom key stores** > **External key stores**.
- 3. For **Key store name**, enter the required name.
- 4. Select Create external key store.

aws Services Q Search	[Alt+S] D 🗘 Ø N. Virginia ▼ ADFS-Administrator/
Key Management × Service (KMS)	KMS > External key stores
AWS managed keys Customer managed keys	External key stores (0) Info Key store actions Create external key store Q. Find key stores
Custom key stores AWS CloudHSM key stores External key stores	Custom key store na V Custom key store ID V Proxy connectivity V Connection state V No external key stores Unable to find any external key stores in this account and Region. Create external key store Create external key store

The Create external key store page appears.

- 5. Under **Custom key store name**, provide a descriptive name for the external key store.
- 6. Under **Proxy connectivity**:
 - a. Select Public endpoint.
 - b. For **Proxy URI endpoint**, enter the Proxy URI endpoint in the following format:

https://<FQDN of Load Balanced Endpoint>

Substitute <FQDN of Load Balanced Endpoint> with the fully qualified domain name of the load-balanced endpoint utilized for accessing the service, distinct from any of the KeyControl instances.

eate external key store	
ustom key store name	
y store name	
-xks	
y store name must be unique in your AWS account and Region.	
Public endpoint Select this option to use a public endpoint to communicate with the external key store proxy.	VPC endpoint service Select this option to use a VPC endpoint service to communicate with the external key store proxy.
Public endpoint Select this option to use a public endpoint to communicate with the external key store proxy. oxy URI endpoint	VPC endpoint service Select this option to use a VPC endpoint service to communicate with the external key store proxy.

- 7. Under **Proxy configuration**:
 - a. Leave Proxy URI path prefix empty.
 - b. For **Proxy credential: Access key ID**, enter the previously-saved proxy access key ID.
 - c. For **Proxy credential: Secret access key**, enter the previously-saved proxy secret access key.
 - d. Select Create external key store.

Proxy URI path prefix - optional	
/example/path/prefix	/kms/xks/v1
Proxy URI path prefix must have between 9 and 117	characters. Valid characters are a-z, A-Z, 0-9, /, - (hyphen), and _ (underscore)
Proxy credential: Access key ID The ID of the secret access key in the authentication of	credential established on your external key store proxy.
JPEUXYIU75NF5TCR	
Access key ID must have between 20 and 30 characte	ers. Valid characters are uppercase A-Z and 2-7
Proxy credential: Secret access key The secret access key in the authentication credential	l established on your external key store proxy.
•••••	
Secret access key must have between 43 and 64 char.	acters. Valid characters are a-z, A-Z, 0-9, /, +, and =

A details page for the new external key store appears.

aws iii Services Q Search	[Alt+S]			N. Virginia • ADFS-Administrator/Jadon/Hichael.DeJesus@entrust.com @ edc-dps
Key Management × Service (KMS)	⊘ Successfully created external key store -sks with ID cks-36015c191	⊗ ₀ ∆₀ ⊗₂ ⊙₀ ⊖∘ ∨		Connect key store
AWS managed keys Customer managed keys V Custom key stores AWS CloudHSM key stores External key stores	KMS > Extend key sters > dx-34011 -XKS General configuration			Key store actions v Counte a KMS key in this key store
	Cutom key store ann aks Cutom key store (D C da-S6015.1918b)	Connection state Disconnected Castom key store External key store	Creation date Aug 21, 2023 16:28 EDT	r

- 8. Select **External key stores** to view all external key stores.
- 9. Select **Key store actions** > **Connect** to connect to the external key store.

KMS > External key stores					
External key stores (1/2) Info			[Key store actions 🔺	Create external key store
Q Find key stores				Edit	
				Connect	
Custom key store name		▼ Proxy connectivity	♥ Connec	Disconnect	⊽
• vics	🗇 cks-36015c191	Public endpoint	Disconr	Delete	
0	🗇 cks-6503c336	Public endpoint	Disconn	rected	

10. Wait for the Connection state to display as **Connected**.

KMS > External key stores				
External key stores (1/2) Info			Key store actions v Create extern	I key store
Q. Find key stores				
Custom key store name	マ Custom key store ID	マ Proxy connectivity	▼ Connection state	~
O -xks	🗗 cks-36015c191	Public endpoint	Connected	

- Return to KeyControl Cloud Key Management Vault and select CLOUDKEYS > CloudKeys.
- 12. Select the Key Set created earlier along with the Region.

() EN	ITRUST	KeyControl Vault for Clor	l ud Key Manage	ment		CLOUDKEYS	SECURITY	AUDIT LOG		ANKS XXXS 🛦
Actions -	Key Sets	CloudKeys	CSP Accou	nts						Refresh C
Key Set: •	aws_xks_keyset	(AWS-XKS)	∨ Re	ion: *	US East (N. Virginia) us-east-1 🔹 🗸					

There are no Cloudkeys to show. Please create one from Actions.

×

13. Select Actions > Create CloudKey.

The Create CloudKey dialog appears.

- 14. In the **Details** page:
 - a. For **Name**, enter a name for the CloudKey.
 - b. Enter a **Description**.
 - c. Select Continue

Create CloudKey

Details	Access	Schedule		
Туре	AWS		-	
Key Set	aws_xk	s_keyset		
Region	us-east-	-1		
Name *				
keycontro	l-test-cloudk	ey		
Description				
keycontro	l-test-cloudk	ey		
Cancel				

- 15. In the **Access** page:
 - a. For **Administrators**, select AWS IAM users who will have administrative rights.
 - b. For **Users**, select AWS IAM users who will be able to use the key to encrypt/decrypt.
 - c. Select Continue.

		Cre	ate CloudKey	×
Details	Access	Schedule		
Administrate Choose user	ors 's (AWS IAM u	users) who shou	Id have administrative rights to the key.	
xks-user	× Add an A	dministrator		
Users	. ANC IAM.		an lass to an an attal and a	
Ks-user Add a User				
Cancel			Cont	inue

- 16. In the **Schedule** page:
 - a. For Rotation Schedule, select a rotation schedule for the CloudKey.
 - b. For **Expiration**, select the required condition.
 - c. Select **Apply** to finish the process.

		Cre	ate CloudKey ×			
Details	Access	Schedule				
Rotation Sc Define a sch	hedule * edule for whic	ch the CloudKey	will be rotated.			
Inherit from keyset (Never)						
Expiration * Define when	Expiration • Define when the CloudKey should be expired.					
Never	⊖ Choose a	a date				
Cancel			Apply			

After the XKS CloudKey is created in KeyControl, a KMS key pointer is automatically created in AWS KMS with a key alias that matches the KeyControl CloudKey name. This KMS key pointer can be utilized by AWS services to encrypt or decrypt user objects.

17. Return to AWS KMS > **Customer managed keys** to find the created CloudKey.

Key Management X Service (KMS)	1045 > Customer managed keys			
AWS managed keys Customer managed keys Custom key stores AWS Chustol Mere storer	Customer managed keys (17) Q. / Elser logs by properties or lags: https://www.superties.or.lags https://www.superties.or.lags https://www.superties.or.lags Segmented X Gar Hiter			Key actions Create key < 1
External key stores	Allases ∇ Key10 ∇ Status bescentrel.test-cloudies 750/01/2.01/04.46(0) Enabled	Key type Summetric	Key spec Symmetric Decallet	Key usage
	C NEXTREMENTATION NEXT 100-000-000-000-000-000-000-000-000-000	aynnillethe	STIMETING_DEMOLT	end ypt and sed ypt

18. Select either the **Aliases** or **Key ID** hyperlink for the CloudKey.

A details page for the CloudKey appears.

19. Select Cryptographic configuration.

Note that under **Custom key store**, the **Custom key store name** appears and the **Custom key store type** as listed as **External**.

20. Under General configuration, copy the AWS KMS ARN for a later step.

KMS > Customer managed keys > Key ID: 7a59c8c9-9c3b-4194- 7a59c8c9-9c3b-4194-a6e0-	te .			Key actions 🔻 Edit		
General configuration	General configuration					
Allas *GSt-CloudRey ⊘ ANN copied ↑ armawskmsus-cesti-1594691246913key/7z595clc9-9c10-4194-	Status Enabled Description keycontrol-test-cloudkey		Creation date Aug 21, 2023 16:38 EDT Regionality Single Region			
Key policy Cryptographic configuration Tags Aliases						
Cryptographic configuration						
Key Type Symmetric	Origin External key store	Key Spec ① SYMMETRIC_DEFAULT	Key Usage Encrypt and decrypt			
Custom key store						
Custom key store ID Custom ke	Custom key store name xks		Custom key store type External key store			
Connection state Connected	Creation date Aug 21, 2023 16:28 EDT					
External key						
External key ID Of of dbadd-1098-41b4-b50ceast-1.keycontrol-test-clour	dkey					

2.9. Test the integration

To test the integration:

- 1. Sign in to the AWS Console and access **S3** services.
- 2. From the left panel, select **Buckets** and then select **Create bucket**.

Amazon S3 X	Amazon 53 > Buckets			
Buckets Access Points	Account snapshot Storage lens provides visibility into stora	ge usage and activity trends. Learn more 🔀		View Storage Lens dashboard
Object Lambda Access Points Multi-Region Access Points Batch Operations	Total storage Pending	Object count O Pending	Average object size O Pending	You can enable advanced metrics in the "default-account-dashboard" configuration.
IAM Access Analyzer for S3 Block Public Access settings for	Buckets Info Buckets are containers for data stored in S3.	Learn more 🖸		Copy ARN Empty Delete Create bucket

The Create bucket page appears.

- 3. Under General configuration:
 - a. For Bucket name, enter the required name for the bucket.
 - b. Select an appropriate **AWS Region**.

Bucket name	
xks-user-test	
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket nami	ing 🔼
AWS Region	
US East (N. Virginia) us-east-1	

4. Under Object Ownership, select ACLs disabled.



5. Under Bucket Versioning, set Bucket Versioning to Disable.

Bucket Versioning Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and rest every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user action and application failures. Learn more 🖸	ure S
Bucket Versioning Disable Enable 	

6. Under **Default encryption**:

- a. For Encryption type, select Server-side encryption with AWS Key Management Service keys (SSE-KMS).
- b. For AWS KMS key:
 - i. Select Enter AWS KMS key ARN.
 - ii. Paste the AWS KMS ARN from the previously created CloudKey.
- c. For **Bucket Key**, select **Enable**.
- d. Select **Create bucket** to complete the process.

Default encryption Info Server-side encryption is automatically applied to new objects stored in this bucket.
Encryption type Info Server-side encryption with Amazon S3 managed keys (SSE-S3)
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
O Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS) Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page. 2
AWS KMS key Info
O Choose from your AWS KMS keys
O Enter AWS KMS key ARN
AWS KMS key ARN Your KMS key must be in the us-east-1 Region, where this bucket is being created. am:aws:kms:us-east-1:5946912 key/7a59c8c9-9c3b-4194- Create a KMS key [2] Format (unity key fill; amawskms:region>: <account-id>:allas/callas-name> Bucket Key Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Lear more C MSL Lear more C O Disable</account-id>
Enable
Advanced settings
③ After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.
Cancel Create bucket

The bucket is created.

Buckets (1) Info Buckets are containers for data stored in S3. Learn more Q. Find buckets by name	Ø		C Copy ARN Empty Delete	Create bucket
Name	AWS Region		▼ Creation date	~
O xks-user-test	US East (N. Virginia) us-east-1	Bucket and objects not public	August 21, 2023, 16:45:00 (UTC-	-04:00)

7. Select the hyperlink for the bucket.

A details page for the bucket appears.

- 8. Select Objects.
- 9. To test the encryption, select **Upload**.

xks-user-test Info					
Objects Properties Per	missions Metrics Management Access	Points			
Objects (0) Objects are the fundamental entities store	ed in Amazon S3. You can use Amazon S3 inventory to get a lis 	st of all objects in your bucket. For others to access your objects, your Delete Actions ▼ Create folder	need to explicitly grant them permissions. Learn more	ß	
Q. Find objects by prefix				<	1 > 💿
Name	▲ Туре	▼ Last modified	⊽ Size	▼ Storage class	~
		No objects You don't have any objects in this bu In Upload	cket.		

The **Upload** dialog appears.

10. Select Add files.

Upload Info				
Add the files and folders y 33 REST API. Learn more	You want to upload to S3. To u	upload a file larger than 160GE	3, use the AWS CLI, A	WS SDK or Amazor
Drag an	d drop files and folders you wa	ant to upload here, or choose <i>i</i>	Add files or Add fold	er.
Files and folders All files and folders in this	(O) table will be uploaded.	Remove	Add files	Add folder
Q Find by name				< 1 >
Name	▼ Folder	⊽ Туре	▼ Size	∇
	N You have not cho	o files or folders sen any files or folders to uplo	ad.	

11. Locate and select an image to upload.

The file is added to the list of available images.

12. Select the check box for the image file and select **Upload**.

REST API. Learn more 🖸	load here, or choose Ad	d files or Add folder.
Files and folders (1 Total, 28.0 KB) All files and folders in this table will be uploaded.	Remove	Add files Add folder
Q Find by name	7 Type	✓ 1
Entrust-Image.png -	image/png	28.0 KB
Entrust-Image.png - Destination	image/png	28.0 KB

In this example, the Entrust-Image.png file was added and can be selected and

uploaded.

The newly uploaded image is listed within the bucket.

Upload: status					Close
O The information below will no longer be available after you navigate away from the	is page.				
Summary					
Destination s3://xks-user-test	Succeeded ② 1 file, 28.0 KB (100.00%)		Failed () 0 files, 0 B (0%)		
Files and folders Configuration					
Files and folders (1 Total, 28.0 KB)					
Q. Find by name Name Folder	▽ Type ▽	Size 🗢	Status	▼ Error	< 1 > v
	image/png	28.0 KB	Succeeded	-	

13. Select the new image and select **Open** to view it.

xks-user-test Info					
Objects Properties P	Permissions Metrics Management	Access Points			
Objects (1) Objects are the fundamental entities st	tored in Amazon S3. You can use Amazon S3 inventory [2]	to get a list of all objects in your bucket. For others to ren [2] Delete Actions V	o access your objects, you'll need to explicitly Create folder	grant them permissions. Learn more 🔀	
Q Find objects by prefix					< 1 > @
✓ Name	▲ Туре		⊽ Size		⊽
Image: Contract of the second seco	png	August 21, 2023, 16:47:4	1 (UTC-04:00)	28.0 KB Standard	

The image starts in a browser window.



- 14. Return to KeyControl Cloud Key Management Vault and select **CLOUDKEYS** > **CloudKeys**.
- 15. Select the CloudKey and then select **Actions** > **Disable CloudKey**.

Actions - Key Sets CloudKeys CSP Accounts				Refresh 🕽
Create CloudKey set (AWS-XKS) V Region: US East (N. Virginia Disable CloudKey	us-east-1 🗸			
Delete CloudKey	P Description V	Expires	Cloud Status ()	≡
keycontrol-test-cloudkey	keycontrol-test-cloudkey	Never	AVAILABLE	

The CloudKey is disabled.

ENTRUST KeyControl Vault for Cloud Key Management		LERTS SETTINGS		aws-xks 🔒 🗸
Actions - Key Sets CloudKeys CSP Accounts Key Set: • avs_xks_keyset (AWS-XKS) • Region: • US East (N. Virginia) (s-east-1 V			Success X CloudKey Disabled Successfully
CloudKey Name ~	Description	 Expires 	 Cloud Status () 	=
keycontrol-test-cloudkey	keycontrol-test-cloudkey	Never	DISABLED	

16. Return to the AWS S3 bucket and attempt to open the uploaded image.

The image is not viewable as the CloudKey was disabled.

← → C ☆ ■ xks-	user-test.s3.us-east-1.amazonaws.com/Entrust-Image.png	?response-content-disposition=inline&X-Amz-Security-Token=IQoJb3JpZ2luX
This XML file does not appea	r to have any style information associated with it. The	document tree is shown below.
▼ <error> <code>KMS.DisabledExcept <message>arn:aws:kms:us</message></code></error>	tion •east-1:59469 :key/7a59c8c9-9c3b-4194-	is disabled.

17. Re-enable the **CloudKey** in the KeyControl CloudKey Management Vault.

	Enable CloudKey	×
By Enabling the follow	wing CloudKey, the key will become enabled and available to use.	
CloudKey	keycontrol-test-cloudkey	
Keyld	7a59c8c9-9c3b-4194-	
Cancel	Enable	

- 18. Return to the AWS S3 bucket.
- 19. Open the uploaded image again. It is now viewable.



This concludes the integration process.

Chapter 3. Additional resources and related products

- 3.1. nShield Connect
- 3.2. nShield as a Service
- 3.3. Entrust digital security solutions
- 3.4. nShield product documentation