



Amazon Web Services (BYOK and HYOK)

KeyControl CSP Vault for Cloud Keys Integration Guide

2026/11/06

© Entrust Corporation. All rights reserved.

Private connectivity from KeyControl to AWS (BYOK and HYOK)

This guide makes the **KeyControl CSP Vault for Cloud Keys** call AWS **privately**, over AWS PrivateLink, instead of over the internet. It covers both:

- **BYOK** (bring your own key): KeyControl creates keys and imports the key material into AWS KMS.
- **HYOK** (hold your own key, AWS external key store / XKS): the keys stay in KeyControl and AWS KMS calls KeyControl.

Region used: `us-east-1` (use your own Region everywhere).

What needs to be private

KeyControl calls four AWS services. Each one needs its own VPC endpoint. An endpoint you do not create keeps using the internet.

AWS service	DNS name KeyControl calls	VPC endpoint service name	What KeyControl does with it
KMS	`kms.us-east-1.amazonaws.com`	`com.amazonaws.us-east-1.kms`	Creates and describes keys, imports key material (BYOK), reads key store status (HYOK)
IAM	`iam.amazonaws.com`	`com.amazonaws.iam`	Checks the AWS account and its credentials (`GetUser` , `ListUsers` , `CreateAccessKey`)
EC2	`ec2.us-east-1.amazonaws.com`	`com.amazonaws.us-east-1.ec2`	Lists AWS Regions (`DescribeRegions`)
Systems Manager	`ssm.us-east-1.amazonaws.com`	`com.amazonaws.us-east-1.ssm`	Reads AWS parameters (`GetParameter`)

The call names in the last column were observed in AWS CloudTrail when KeyControl added an AWS account and created keys.

HYOK also needs the other direction (AWS KMS calling KeyControl). That is a separate setup: see *Connect AWS KMS External Key Store (XKS) to KeyControl over AWS PrivateLink*. BYOK does not need it.

```
KeyControl --> private DNS --> VPC interface endpoints (kms, iam, ec2, ssm) --> AWS
(private IPs)  (Step 4)          (Steps 2-3, TCP 443)
```

Before you start

- A VPC with **two private subnets in two different Availability Zones**.
- **VPC DNS settings:** *DNS resolution* and *DNS hostnames* are both **enabled** on the VPC (required for private DNS names).
- If KeyControl runs in your data center, a private connection to the VPC: **AWS Direct Connect** (recommended) or Site-to-Site VPN. The VPC IP range must not overlap with your data center range.
- KeyControl nodes with **private IP addresses only** (no public IPs).
- The IAM user or access key that KeyControl uses for the AWS account.

IAM endpoint limit: AWS supports the IAM interface endpoint only in **US East (N. Virginia)** (and the China Beijing and GovCloud US-West Regions). If your VPC is in another Region, create the IAM endpoint in a US East (N. Virginia) VPC and reach it over AWS Transit Gateway. See the AWS documentation page *Create a VPC endpoint for IAM*.

Step 1. Create a security group for the endpoints

VPC > Security groups > **Create security group**

1. Name: `keycontrol-aws-endpoints`. Select your VPC.
2. Inbound rule: **HTTPS (TCP 443)** from the **VPC CIDR**, and also from your data center range if KeyControl is on-premises.
3. Create.

Why the whole VPC: private DNS applies to the entire VPC. After Step 2 and Step 3, every workload in the VPC that calls KMS, IAM, EC2 or Systems Manager uses these endpoints. If the security group only allowed the KeyControl IP addresses, those other workloads would stop working.

Step 2. Create the KMS, SSM and EC2 endpoints

VPC > Endpoints > **Create endpoint**. Repeat three times:

Name	Service name
`keycontrol-kms`	`com.amazonaws.us-east-1.kms`
`keycontrol-ssm`	`com.amazonaws.us-east-1.ssm`
`keycontrol-ec2`	`com.amazonaws.us-east-1.ec2`

For each endpoint:

1. Type: **AWS services**. Select the service name from the table.
2. VPC: your VPC. Subnets: **both Availability Zones** (one private subnet in each).
3. IP address type: **IPv4**.
4. Security group: `keycontrol-aws-endpoints`.
5. Turn **Enable DNS name on** (private DNS). This is required.
6. Create, and wait until the status is **Available**.

Step 3. Create the IAM endpoint

VPC > Endpoints > **Create endpoint**, in a **US East (N. Virginia)** VPC:

1. Name: `keycontrol-iam`. Type: **AWS services**. Service name: `com.amazonaws.iam`.
2. VPC, both Availability Zones, IPv4, security group `keycontrol-aws-endpoints`, **Enable DNS name** on.
3. Create, and wait until the status is **Available**.

Step 4. Make KeyControl resolve the four names privately

Private DNS only works for DNS queries that go through the VPC resolver.

- **KeyControl runs inside the VPC:** nothing to do. Go to Step 5.
- **KeyControl runs in your data center:**
  1. Route 53 > Resolver > **Inbound endpoints** > **Create inbound endpoint**. Select your VPC, both Availability Zones, and a security group that allows **TCP and UDP 53** from your DNS servers. Note the two endpoint IP addresses.
  2. On your data center DNS server, add a **conditional forwarder** for each of these names, pointing to the two inbound endpoint IP addresses:
     - `kms.us-east-1.amazonaws.com`
     - `ssm.us-east-1.amazonaws.com`
     - `ec2.us-east-1.amazonaws.com`
     - `iam.amazonaws.com`

Step 5. Check the DNS answers

From a KeyControl node (or a host that uses the same DNS server):

```
for n in kms.us-east-1.amazonaws.com ssm.us-east-1.amazonaws.com \
         ec2.us-east-1.amazonaws.com iam.amazonaws.com; do
  echo "$n -> $(dig +short $n | tr '\n' ' ')"
done
```

Every name must return **private** addresses (for example `10.x`, `172.16-31.x`, `192.168.x`) from your VPC range. A public address means the endpoint or the forwarder for that name is missing.

Step 6. Check that KeyControl's calls are private

1. In KeyControl, run actions that talk to AWS:
   - **Select a key set** on the CloudKeys tab: KeyControl calls EC2 (`DescribeRegions`).
   - **Create or enable a CloudKey** (BYOK or HYOK): KeyControl calls KMS.
   - **Add the AWS account** (CSP account) or create a key set or CloudKey: KeyControl also calls Systems Manager (`GetParameter`) and IAM (`GetUser`, `ListUsers`, `CreateAccessKey`).
   - **Rotate the account's access key**: KeyControl calls IAM. This creates a new access key, so do it only in a test account.
2. In AWS open **CloudTrail > Event history**. Set the filter to **User name** = the IAM user that KeyControl uses. IAM events appear in the **US East (N. Virginia)** Event history.
3. Open the events from KeyControl (user agent starts with `Boto3`). Every event for `kms`, `iam`, `ec2` and `ssm` must show:
   - a **private** `sourceIPAddress` (your KeyControl node IP), and
   - a `vpcEndpointId` (`vpce-...`).

A public `sourceIPAddress` with no `vpcEndpointId` means that call still goes over the internet.

You can also list them with the AWS CLI and `jq`:

```
aws cloudtrail lookup-events --region us-east-1 \
  --lookup-attributes AttributeKey=Username,AttributeValue=<keycontrol-iam-user> \
  --max-items 200 --query "Events[].CloudTrailEvent" --output json \
 | jq -r '.[] | fromjson | select(.userAgent|startswith("Boto3"))
          | [.eventSource,.eventName,.sourceIPAddress,(.vpcEndpointId // "-")] | @tsv' \
 | sort | uniq -c | sort -rn
```

Step 7. Test BYOK and HYOK

- **BYOK:** create a key set and a CloudKey in KeyControl and upload it to AWS. Check in CloudTrail that `CreateKey`, `GetParametersForImport` and `ImportKeyMaterial` also show a private source IP and a `vpcEndpointId`.
- **HYOK:** complete the XKS PrivateLink guide, then run an encrypt and decrypt with the XKS key.

Step 8. Remove internet access last

Only after Steps 5 to 7 pass, remove the nodes' public IP addresses and any internet route (NAT or firewall rule). Run the Step 6 actions and the BYOK and HYOK tests again. Anything that stops working points to a missing endpoint or DNS name.

Quick checklist

- [ ] VPC DNS resolution and DNS hostnames enabled
- [ ] Four endpoints **Available** with **Enable DNS name** on: kms, ssm, ec2 (Region) and iam (US East N. Virginia)
- [ ] Endpoint security group allows TCP 443 from KeyControl
- [ ] Data center DNS forwards the four names to the Route 53 inbound endpoint (if KeyControl is not in the VPC)
- [ ] `dig` returns private addresses for all four names
- [ ] CloudTrail shows a private source IP and a `vpcEndpointId` for every KeyControl call
- [ ] BYOK and HYOK tests pass before internet access is removed

Troubleshooting

Symptom	Cause	Fix
`dig` returns a public address	Conditional forwarder missing, or endpoint private DNS is off	Add the forwarder (Step 4); turn on **Enable DNS name** on the endpoint
Cannot turn on private DNS	VPC DNS resolution or DNS hostnames disabled	Enable both on the VPC
Calls time out	Endpoint security group blocks the caller	Allow TCP 443 from the VPC CIDR (and your data center range) in the endpoint security group (Step 1)
CloudTrail shows a public source IP for `iam`	IAM endpoint missing, or VPC not in US East (N. Virginia)	Create the IAM endpoint (Step 3) or use Transit Gateway
Adding the AWS account fails after internet access is removed	One of iam, ec2 or ssm endpoints or DNS names is missing	Re-check Steps 2 to 5 for all four services
BYOK upload fails, XKS works	KMS name resolves publicly from KeyControl	Fix the `kms` DNS forwarder (Step 4)