AWS
Hold Your Own Key (HYOK)

Integration Guide

CryptoServer HSM

utimaco®

Imprint

Copyright 2026	Utimaco IS GmbH Krefelder Straße 220 52070 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-05-21
Status	PUBLISHED
Document No.	IG-2026-0043

Table of Contents

1 Introduction

More and more companies are moving into the cloud; some even apply a “cloud first” strategy. If public clouds such as Amazon Web Services (AWS) are used, data must be protected sufficiently, also to meet legal requirements. Such protection can be achieved with encryption. Necessary encryption keys could be stored in the cloud, for example in the key management systems of the cloud providers. However, in doing so, companies will give up control of their keys, it might be difficult to migrate the keys to another provider, and multi-cloud strategies are impossible.

Hosting your own keys is a viable alternative, especially if you already own an HSM. Then, a VPN tunnel between your cloud installation and the on-premise HSM can be created, and the applications running in the cloud can perform cryptographic operations using the local HSM. Depending on the internet connectivity of your company, higher latency must be considered.

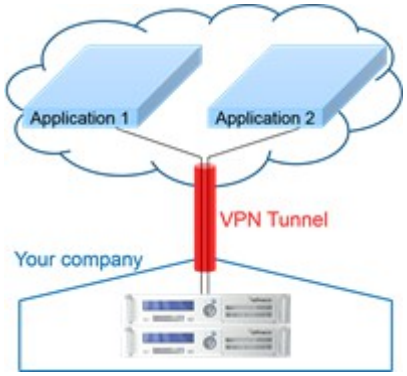

Figure 1 : VPN tunnel

In this scenario, you have full control of your HSM, including physical access required e.g., for key ceremonies. Moreover, your in-house applications can also have access to the HSMs. Last but not least, the full feature set of Utimaco CryptoServer HSMs is available, including applications written with CryptoServer SDK or CryptoScript and running on - and thus protected by - the HSM.

This integration guide shows how to set up such a HYOK scenario with AWS. We assume that the reader is familiar with AWS and has already set up a Virtual Private Cloud (VPC). Also, the reader should be familiar with installing the Utimaco SecurityServer software and with using the CryptoServer HSM.

2 VPN Setup

Setting up the Virtual Private Network (VPN) connection requires work in AWS and locally. Before starting, please check that you have a gateway device that was tested by AWS (see VPC Network Administrator Guide) or that it supports IKE and IPsec. Detailed VPN setup is beyond this integration guide; please ask your networking staff for further assistance.

2.1 AWS Setup

Setup on AWS is described very well in the VPC User Guide. In short, you have to create a customer gateway, create a virtual private gateway, enable route propagation, and finally create the VPN connection. If your only intention is to connect one or more on-premise HSMs to the AWS VPC, you can rely on static routing and you do not need to enable inbound access in AWS. For static routing, enter the internal IP address or address prefix of your HSM(s) during VPN connection setup. For debugging purposes using the ping command, you might want to enable incoming ICMP in the VPC security group.

2.2 Local Setup

After the creation of the VPN connection, download the VPN configuration for your gateway device, if listed. Otherwise, download the generic configuration since it will contain all the parameters needed. If your gateway was tested by AWS, you can find detailed configuration examples in the AWS Network Administrator Guide. Your gateway might even provide a function to import the AWS configuration directly for auto-configuration.

In case you cannot download a VPN configuration for your gateway and you do not find configuration examples, open the generic configuration file in a text editor and configure your local gateway accordingly. The “Outside IP Address” of the Virtual Private Gateway is the public IP address of AWS your local gateway is connecting to. Typically, you have to set up IKE and IPsec with the given pre-shared key for authentication. Note that the given authentication algorithms as well as the Diffie-Hellman/Perfect Forward Secrecy groups represent a minimal configuration only. We recommend to use at least SHA-256 for authentication (if not combined with the encryption algorithm AES-GCM) and Diffie-Hellman group 14 (MODP 2048).

2.3 Connection Check

After the VPN connection has been established, the HSM can be accessed from an AWS Virtual Machine (VM). For the rest of the document, we assume that the environment variable

`CRYPTOSERVER` is set to the IP address of the HSM, reachable via the VPN. Then, running `csadm getstate` should return status information of the CryptoServer.

3 Additional Security

Since SecurityServer release 4.10, the CryptoServer HSM can also authenticate against the user/host application. Thus, your application running in an AWS VM can be sure to talk to the right HSM. To enable this feature, export the public HSM authentication key to a file:

›_ Console

```
csadm GetHSMAuthKey > hsmkey.txt
```

We recommend to perform this operation on-premise, as close as possible to the HSM, and to copy the resulting file to the VM. On the VM, set the environment variable `CS_AUTH_KEYS` to the file path.

Now, each time an application wants to authenticate against the HSM, the HSM also needs to authenticate against the application (“mutual authentication”). You can check by renaming or moving the file or by changing the **CSxxxxxx** number in the file - an error will occur when you try `csadm Login…`.

4 Conclusion

Setting up a HYOK scenario with AWS is usually simple and straightforward. The creation of a VPN tunnel between your company and AWS is independent from the HSM; and once the tunnel has been established the HSM can be reached via IP as if it was on local network. Mutual Authentication provides additional security for such remote connection scenarios.

5 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.