Qinsight

Qinsight Atlas

v1.0

Integration Guide

u.trust GP HSM Se-Series

v6.4.0.0

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	2026-07-27
Status	PUBLISHED
Document No.	IG-2026-0068

Table of Contents

1 Introduction

1.1 About This Guide

This document serves as the official integration guide for deploying and configuring Qinsight Atlas with the Utimaco u.trust GP HSM. It provides step-by-step instructions for system administrators to establish a secure, mTLS-authenticated connection between the Qinsight platform and the Utimaco HSM using the Utimaco REST Cryptographic API (RCAPI).

1.2 Target Audience

This guide is intended for Qinsight Atlas and Utimaco Hardware Security Module (HSM) administrators.

1.3 Purpose of the Integration

The primary purpose of this integration is to enable seamless, automated discovery and inventory of hardware-backed cryptographic assets. By integrating Qinsight Atlas with the Utimaco HSM via RCAPI, organizations can:

- Dynamically fetch metadata for keys and certificates stored securely within the HSM.
- Automatically generate a comprehensive Cryptographic Bill of Materials (CBOM) for audit and compliance tracking.
- Continuously monitor cryptographic health, algorithm strength, and key rotation lifecycles - all while ensuring that sensitive private key material never leaves the secure, FIPS-certified boundary of the Utimaco HSM.

1.4 Abbreviations

Abbreviation	Meaning
API	Application Programming Interface
Atlas	Qinsight Atlas cryptographic inventory and policy platform

Abbreviation	Meaning
CBOM	Cryptographic Bill of Materials
CET	Central European Time
CN	Common Name
CXI	Cryptographic eXtended Interface
DB	Database
FIPS	Federal Information Processing Standards
GP HSM	General Purpose Hardware Security Module
HA	High Availability
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
JRE	Java Runtime Environment
MBK	Master Backup Key
mTLS	Mutual Transport Layer Security
P11CAT	PKCS#11 graphical interface tool
PKCS	Public Key Cryptography Standards

Abbreviation	Meaning
PKCS#11	PKCS Part 11: The Cryptographic Token Interface Standard
PKI	Public Key Infrastructure
RCAPI	REST Cryptographic API
REST	Representational State Transfer
RMA	Return Merchandise Authorization
SO	The PKCS#11 cryptographic slot Security Officer
TDE	Transparent Data Encryption
TLS	Transport Layer Security
URL	Uniform Resource Locator

Table 1: Abbrevations

1.5 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press **OK**

Convention	Use	Example
`Monospaced`	Code that is given for explanation or as an example, file paths	`/opt/utimaco/bin`
Italic	References and important terms	See the given sample: *Support - Utimaco Portal*

Table 2: Document conventions

We use special icons to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

This message indicates the expected result after the successful execution of an instruction.

2 Product Overview

2.1 Overview of the Qinsight Atlas

Qinsight Atlas is a Cryptographic Posture Management Platform that discovers, inventories, and analyzes cryptographic assets across the enterprise for quantum readiness and improved crypto agility. Qinsight Atlas connects to the Utimaco HSM to dynamically discover, fetch, and continuously analyze metadata associated with cryptographic keys and certificates to ensure compliance and security visibility.

2.2 Overview of Utimaco u.trust GP HSM

The Utimaco u.trust GP HSM Se-Series is a hardware security module developed by Utimaco IS GmbH. It is a physically protected, specialized computer unit designed to perform sensitive cryptographic tasks and securely manage and store cryptographic keys and data. The u.trust GP HSM can be used as a universal, independent security component for heterogeneous computer systems.

2.3 Joint Value Proposition

By integrating the Qinsight Atlas Cryptographic Posture Management Platform with Utimaco u.trust GP HSM via the REST Cryptographic API (RCAPI), organizations gain complete visibility into their hardware-backed cryptographic assets and can analyze quantum readiness across hardware, cloud, network, code, and the software supply chain. This integration provides a complete picture of the cryptographic estate while ensuring that all keys managed within the HSM are actively monitored, cataloged, and validated against security policies and compliance requirements without compromising the HSM's strict isolation.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

Operating System	Partner Product	Utimaco SecurityServer Version	Utimaco HSM
Linux Ubuntu 22.04	Qinsight Atlas v1.0	SecurityServer v6.4.0.0 with RCAPI v2.1.1	u.trust GP HSM Se-Series; tested with u.trust GP-HSM Simulator v6.4.0.0

Table 3: Tested versions

3.2 Supported Platforms

Qinsight Atlas is environment-agnostic and connects to the Utimaco RCAPI Server over standard network protocols using HTTPS. The Qinsight Atlas client can run in Linux, macOS, containerized, virtualized, and cloud environments, provided that it has network reachability to the RCAPI endpoint.

Platform Category	Supported Environments
Operating systems	Linux Ubuntu 20.04 or 22.04, RHEL 8 or 9, CentOS, and macOS.
Virtualization and containers	Native Docker or containerd environments, Kubernetes clusters, and standard virtual machines such as VMware or UTM.
Cloud environments	Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.

Table 4: Supported platforms

The Utimaco RCAPI Server must run using the provided Docker container. The Qinsight Atlas client can operate from any supported platform as long as HTTPS connectivity to the RCAPI endpoint is available.

3.3 Hardware and Software Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	u.trust GP HSM Se-Series LAN with firmware SecurityServer 6.4.0 or higher
Utimaco PCI-e HSM	u.trust GP HSM Se-Series PCI-e with firmware SecurityServer 6.4.0 or higher

Table 5: List of hardware requirements

Software	Software Requirements
HSM Interface	Utimaco REST Cryptographic API (RCAPI) v2.1.1
HSM Utility	SecurityServer administration tools, including csadm and p11tool2
Partner Product	Qinsight Atlas v1.0 and Qinsight Atlas client environment
Container Runtime	Docker runtime for the utimaco-rcapi-server-jre:v2.1.1 container image
Host Operating System	Ubuntu Linux 22.04 for the tested simulator and RCAPI host environment

Table 6: List of software requirements

3.4 Prerequisites

Before starting the integration, ensure that the Utimaco HSM environment and Qinsight Atlas client environment are prepared and reachable.

- Install and configure the operating system used for the *Tested Versions* .
- Install and start the u.trust GP HSM Se-Series environment. For the tested setup, use the u.trust GP-HSM Simulator v6.4.0.0.
- Replace the HSM default administrator with a dedicated administrator user.

- Create and store the Master Backup Key (MBK) on each HSM according to the SecurityServer documentation.
- Set up and configure the SecurityServer environment according to the SecurityServer documentation for the HSM.
- Set up and configure the PKCS#11 library according to your environment. Refer to the SecurityServer documentation for instructions on setting up and configuring the PKCS#11 library.
- Create the required Security Officer (SO) and Crypto user roles for HSM administration and cryptographic operations.

4 Setting Up Utimaco SecurityServer Software

The following section outlines the procedures required to configure the Utimaco SecurityServer Software.

If you have not already done so, create and request an Utimaco Support Portal Account at https://support.hsm.utimaco.com/support. This will allow you to download the software components needed for this installation.

On Linux:

1. Copy the downloaded software to the appropriate location on the Qinsight machine.
2. Create a `utimaco` folder under the `/opt` directory and create two directories `/opt/utimaco/bin` and `/opt/utimaco/lib`.

```
# mkdir -p /opt/utimaco/bin
# mkdir /opt/utimaco/lib
```

3. Copy the pkcs11 library file `libcs_pkcs11_R3.so` from the Utimaco SecurityServer software to the `/opt/utimaco/lib` directory and make the file executable.

```
cp ~/path_to_application_folder/lib/libcs_pkcs11_R3.so /opt/utimaco/lib
chmod +x /opt/utimaco/lib/libcs_pkcs11_R3.so
```

4. Copy the `csadm` and `p11tool2` files from the Utimaco SecurityServer software to the `/opt/utimaco/bin` directory and make both files executable.

```
# cd ~/path_to_application_folder
# cp csadm p11tool2 /opt/utimaco/bin
# chmod +x /opt/utimaco/bin/csadm /opt/utimaco/bin/p11tool2
```

5. Create the directory `/etc/utimaco`. Locate the Utimaco PKCS#11 configuration file in your SecurityServer directory, `Software\Linux\Crypto_APIs\PKCS11_R3\sample`. Copy the Utimaco PKCS#11 configuration file `cs_pkcs11_R3.cfg` to the `/etc/utimaco` directory.

```
# mkdir /etc/utimaco
# cd ~/path_to_application_folder/Software/Linux/Crypto_APIs/PKCS11_R3/sample
# cp cs_pkcs11_R3.cfg /etc/utimaco
```

On Windows:

On Windows, `cs_pkcs11_R3.cfg` will be automatically created and available in the `C:\ProgramData\UtimacoPKCS11_R3` folder as part of the SecurityServer software installation. Edit the `cs_pkcs11_R3.cfg` file and make the appropriate changes to the file. A sample `cs_pkcs11_R3.cfg` file is mentioned below:

```
library = C:\oracle\extapi\64\hsm\utimaco\6.1.1.0\cs_pkcs11_R3.dll
 slot = 0
 pin = Oracle123
 [Global]
 # For Unix:
 Logpath = /tmp
 # For Windows:
 # Logpath = C:/ProgramData/Utimaco/PKCS11_R3
 # Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
 Logging = 1
 # Prevents expiring session after inactivity of 15 minutes
 KeepAlive = true
 # Set the Device to connect with
 #[CryptoServer]
 # Device specifier
 Device = <HSM_IP>
```

For detailed guidance on commands and their parameters, please refer to the Utimaco SecurityServer documentation. The device could be a u.trust GP HSM Se-Series, available in either PCIe or LAN form factors. Depending on the type, the device configuration line will follow one of these formats:

- **LAN-based HSM:** Device = 288@ipaddress
- **PCIe-based HSM:** Device = /dev/cs2.0

Select the appropriate format based on your specific hardware setup.

`library` specifies the path where the cs_pkcs11_R3.dll file is located.

`Slot` indicates the slot number associated with the created USER.

`Pin` represents the password assigned to the USER.

To simplify your testing process, it's recommended that you enable the PKCS#11 log file by adjusting the logging settings. Specifically:

- Set the `LogPath` to a writable directory (not a specific file).
- Set the `Logging` log level to 1 for basic logging. Increase it to 4 for more detailed output during testing.

This will generate a log file named `cs_pkcs11_R3.log` within the specified `LogPath` directory. Reviewing this log can help with troubleshooting if you encounter issues. Once testing is complete, it's advisable to reduce `Logging` log level to 1 or 2 to limit output to only critical or important messages.

5 Setting Up Qinsight Atlas RCAPI

1. Start the Utimaco Simulator: in the UTM Ubuntu 22.04 VM, execute the `cs_sim.sh` script to start the u.trust GP HSM simulator
2. Prepare mTLS certificates: generate a `server.key` and `server.crt` to secure the RCAPI connection to the VM.
3. Provision the RCAPI User: using the Utimaco `csadm` tool, generate an RSA private key and register the RCAPI user to the HSM with the `rsasign` mechanism.
4. Run the RCAPI Server: load the `utimaco-rcapi-server-jre:v2.1.1` Docker container alongside the simulator in the VM, ensuring it connects to the simulator instance and mounts the generated mTLS certificates.

6 Network and Security Configurations

- **mTLS** is strictly enforced. Qinsight must present the client certificate during the TLS handshake to the VM.
- The Qinsight Scanner must have network access to the VM hosting the RCAPI server on **port 8443 (TCP)**. Firewall rules must allow inbound traffic on this port.
- The RCAPI Docker container must be able to reach the local Utimaco Simulator process running in the VM.

7 Integration Steps on Utimaco u.trust GP HSM

The following section outlines the procedures required to configure both the Utimaco HSM and Partner Product components for seamless integration.

Create users SO (Security Officer) and USR (the Crypto user) and initialize a slot.

The slot must be initialized using the p11tool2.

First, create the SO using p11tool2. Then, using the p11tool2 command, initialize the Slot you want to use and the slot user, as shown below.

- `# ./p11tool2 slot=<slot no.> Label=<token label> Login=ADMIN,ADMIN.key InitToken=<SO pin>`

Initialize the SO user.

- `# ./p11tool2 slot=<slot no.> LoginSO=<SO pin> InitPin=<Cryptouser pin>`

8 Integration Steps on Qinsight Atlas

1. Ensure the Qinsight client possesses the `server.crt`, `server.key`, and the generated RCAPI user's private key.
2. Configure the Qinsight scanner to point to the RCAPI server endpoint hosted on any VM/ Host Machine (`https://<Utimaco_host_machine_ip>:8443`).
3. Qinsight authenticates against the `/hsm/cryptography/v1/users/login` endpoint using the RCAPI user credentials and retrieves a Bearer token.

9 Key/Token Management (MKEK, HMAC, SO/Admin users)

RCAPI v2.1.1 authenticates Qinsight purely using the RSA private key assigned to the RCAPI user. Qinsight uses this dedicated RCAPI user to not only discover and fetch existing keys but also to securely create new cryptographic keys directly within the HSM simulator. Security Officer (SO) tasks are segregated and performed out-of-band via `csadm`.

10 Verification and Testing

10.1 Functional Testing

1. Trigger the discovery scan from Qinsight Atlas.
2. Verify that Qinsight authenticates with RCAPI and retrieves a Bearer token.
3. Fetch key attributes from the HSM simulator via RCAPI and confirm that the expected cryptographic objects are visible in Qinsight Atlas.

10.2 Performance Benchmarks

Operations performed through the RCAPI server demonstrate low latency for key fetching and creation tasks.

10.3 Logs and Validation Steps

10.3.1 PKCS#11 Logs

Enabling PKCS#11 logging to facilitate easier testing and troubleshooting is recommended. This can be done by configuring the **Logging Loglevel** and **LogPath** parameters in the configuration file.

- **LogPath** should point to a writable directory (not a specific file) where log files can be stored.
    - Set it to 1 for basic logging.
    - For detailed testing and debugging, increase the level to 4.

The generated log file will be named `cs_pkcs11_R3.log` and located in the directory specified by **LogPath**. Reviewing this log file can help identify and resolve issues that arise during testing.

Once testing is complete, it is advisable to reduce the **Logging Loglevel** to 1 or 2 to limit logging to only critical or important messages, thereby optimizing performance and reducing unnecessary log data.

10.3.2 Qinsight Atlas Logs

Review Docker container logs for the RCAPI Server. Additionally, Qinsight client logs will capture detailed HTTP response codes.

11 Optional Features

11.1 Advanced Features

Automated Key Discovery & CBOM Generation: Qinsight goes beyond basic integration by actively scanning the Utimaco HSM (via RCAPI) to dynamically generate a Cryptographic Bill of Materials (CBOM). This provides a comprehensive, real-time inventory of all cryptographic assets, algorithms, and key sizes residing within the hardware boundary.

Security Policy Validation & Rotation Tracking: Qinsight automatically analyzes the fetched HSM metadata to identify weak or vulnerable cryptographic algorithms (e.g., quantum-vulnerable RSA/ECDSA, small key sizes) and tracks key rotation lifecycles, alerting administrators if keys managed by the Utimaco HSM fall out of enterprise compliance or internal policies.

11.2 High Availability / Redundancy

While the current integration was developed and verified against the u.trust-GP-HSM-Simulator v6.4.0.0 in a standalone VM, production environments can achieve High Availability by deploying the RCAPI Server behind a load balancer pointing to a physical Utimaco HSM cluster.

11.3 Scalability Recommendations

As Qinsight Atlas connects via the Utimaco REST Cryptographic API (RCAPI), the integration is inherently stateless at the application layer and highly horizontally scalable. To accommodate large-scale enterprise environments with high cryptographic discovery volumes, we recommend:

- Horizontal Scaling of RCAPI Servers: Deploy multiple instances of the `utimaco-rcapi-server-jre` Docker container across different host machines.
- Load Balancing: Place a standard Layer 7 / TCP Load Balancer (such as NGINX or HAProxy) in front of the RCAPI Docker containers.
- HSM Clustering: Ensure the backend u.trust GP HSM Se-Series is configured in a cluster (HA group). The RCAPI instances will automatically leverage the Utimaco hardware's built-in synchronization.

12 Troubleshooting

12.1 Common Issues and How to Resolve Them

Issue	Resolution
Cannot fetch keys	Ensure `CXI_GROUP` is properly configured for the simulator slot.
Login Failure	Check RSA private key file and passphrase.
Connection Timeout	Ensure port `8443` is open using `ufw allow 8443/tcp`.

Table 7: Common issues

13 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 Straße 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.

14 Appendices

14.1 References

Title	Description	Document/Link
Utimaco SecurityServer Documentation	Product documentation for installation, administration, client software, HSM configuration, and operational guidance for u.trust GP HSM / SecurityServer.	Refer to the official Utimaco documentation portal or the documentation package delivered with the SecurityServer release.
Utimaco REST Crypto API (RCAPI) Documentation	API reference and operational guidance for REST-based cryptographic services, user authentication, TLS configuration, and key/token access through RCAPI.	Refer to the RCAPI documentation delivered with the RCAPI package used for this integration.
Qinsight Atlas Documentation	Partner documentation for configuring Atlas cryptographic discovery, inventory collection, CBOM generation, policy validation, and HSM integration workflows.	Refer to the Qinsight Atlas product documentation provided by Qinsight.

Table 8: References

14.2 Glossary

Term	Description
Atlas	Qinsight Atlas, the cryptographic posture management platform used to discover, inventory, and assess cryptographic assets exposed through the integration.

Term	Description
CBOM	Cryptographic Bill of Materials. An inventory of cryptographic objects, algorithms, certificates, and related metadata used for governance and risk assessment.
HSM	Hardware Security Module. A dedicated security device used to protect cryptographic keys and perform cryptographic operations in a controlled environment.
mTLS	Mutual Transport Layer Security. A TLS configuration in which both client and server authenticate each other using certificates.
RCAPI	Utimaco REST Crypto API. The REST interface used by Atlas to access cryptographic services and key/token information from the Utimaco SecurityServer environment.
SecurityServer	Utimaco SecurityServer / u.trust GP HSM used as the HSM platform for this integration.
SO	Security Officer. The administrative role responsible for HSM and user management tasks such as provisioning users and assigning permissions.
Token	A logical cryptographic container or object namespace exposed through the HSM/RCAPI environment and discovered by Atlas.

Table 9: Glossary

14.3 Command Summary (CLI commands used)

Command	Purpose
`./csadm Dev=$HSM_IP:$HSM_PORT GetState`	Start the SecurityServer simulator
`csadm Dev=$HSM_IP:$HSM_PORT GetState`	Verify HSM connectivity
`csadm Dev=$HSM_IP:$HSM_PORT UserAdd`	Create or verify RCAPI user
`openssl req -newkey rsa:2048 -nodes -keyout atlas-client.key -out atlas-client.csr`	Generate client certificate material
`openssl x509 -req -in atlas-client.csr -CA ca.crt -CAkey ca.key -out atlas-client.crt`	Sign the client certificate
`docker run -d --name rcapi -p 8443:8443 ...`	Start the RCAPI container
`docker ps`	Check RCAPI container status
`docker logs rcapi`	Review RCAPI logs
`curl -k https://<rcapi-host>:8443/`	Test RCAPI HTTPS reachability
`curl --cert atlas-client.crt --key atlas-client.key https://<rcapi-host>:8443/<token-endpoint>`	Request or validate Bearer token access

Table 10: Command summary