Enterprise Secure Key Manager

Enterprise Secure Key Manager v8.50.0

Release Notes

utimaco®

Imprint

Copyright 2022	Utimaco IS GmbH Germanusstr. 4 D-52080 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	8.50.0
Date	2023-04-26
Status	
Document No.	

Table of Contents

1 Description

These Release Notes outline the functional changes and enhancements for the Enterprise Secure Key Manager (ESKM) appliance. This software update for the ESKM v8 appliances is available at no charge to the customers with a current ESKM support agreement. Please contact Technical Support (p. 17) for software download access or support renewal assistance.

Supersedes

ESKM v8.42.0 — software version 8.43.0

1.1 Product models

Enterprise Secure Key Manager 8.50.0 (ESKM v8.50.0) appliance

1.2 Operating systems

Hardened embedded Linux OS

1.3 Languages

International English

2 Enhancements to the ESKM v8 appliance

2.1 Software v8.50.0 feature updates

- New WebUI support for Google Cloud External Key Manager
- Upgraded OpenSSL to OpenSSL 3.0.8
- Upgraded OpenSSH to OpenSSH 9.1
- ESKM now supports KMIP v3.0
- Virtual ESKM now supported on Hyper-V and KVM hypervisors
- New REST logging category for REST and Cloud logs
- Custom attribute support in REST API
- Fixed vulnerabilities and defects

For upgrading from ESKM v8.1, please follow the instructions in ESKM User Guide (ESKM Appliance overview > Upgrading from a previous ESKM version).

Please refer FIPS mode changes in ***ESKM 8.50.0 User Guide*** for the new restrictions related FIPS mode.

2.2 Software v8.43.0 feature updates

Software v8.43.0 feature updates can be summarized as follows:

- Bring Your Own Key (BYOK) support for Microsoft Azure CSP.
- New WebUI interface for BYOK Cloud integration.
- Support for Google Cloud External KMS integration.
- Fixed vulnerabilities and defects.

2.3 Software v8.42.0 feature updates

Software v8.42.0 feature updates can be summarized as follows:

- Key import via REST API.
- Certificate signing via REST API.
- Random number generation via REST API.
- Get Custom attributes via REST API.
- Local user last access time update for REST API operations.
- Upgraded httpd and SNMP packages.
- Fixed vulnerabilities and defects.

2.4 Software v8.41.0 feature updates

Software v8.41.0 feature updates can be summarized as follows:

- Signing and verification via REST API.
  - Supported Key Algorithms: RSA-2048, RSA-3072, RSA-4096
  - Supported Padding: PSS, PKCS1
  - Supported Hashing Algorithms: SHA-256, SHA-512
- Hashing support via REST API.
  - Supported Algorithms: MD5, SHA-1, SHA-256, SHA-512
- KMIP Object creation via ESKM Management Console.
- Two NIC support for older vESKM releases via upgrader.
- What's New option in the ESKM Management Console.
- Fixed vulnerabilities and defects, including:
  - CVE-2022-0778

2.5 Software v8.4 feature updates

Software v8.4 feature updates can be summarized as follows:

- NIC Teaming support in ESKM appliances.
- Data Encryption and Decryption via REST API.
- LAN HSM support in ESKM L2 appliance.
- SSH public key authentication support for schedule backups.
- Enabled option to initiate schedule backups manually.
- Enabled option to download ESKM license usage and device information.
- Local user license type restricted for the following:
    - Server
    - KMIP
    - KMS
    - Custom
- SNMP trap and system log for scheduled backup failure.
- Updated Log4j version for vulnerability fixes (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832).
- Bug Fixes.

2.6 Software v8.3.2 feature updates

Software v8.3.2 feature updates can be summarized as follows:

- Fixed vulnerabilities and defects, including:
    - Log4j Vulnerability.

2.7 Software v8.3.1 feature updates

Software v8.3.1 feature updates can be summarized as follows:

- Bug fixes including
  - Key operation via REST is not disabled when all the enrolled HSMs are offline.

2.8 Software v8.3 feature updates

Software v8.3 feature updates can be summarized as follows:

- REST API support for basic ESKM key operations.
- Server configuration support for REST and HSM Web UI.
- Service commands for REST service management.
- Bug fixes including
  - Intermediate CA signed certificates are not working for syslog TLS.
  - FIPS level is displayed incorrectly for custom key queries.
  - Disable the key operations via REST API when all the enrolled HSMs are offline to restrict the key operations.

2.9 Software v8.2 feature updates

Software v8.2 feature updates can be summarized as follows:

- Database support for ESKM users and groups
- Support for additive restore of ESKM users and groups
- Improved replication log messaging
- Reliability improvement for ESKM users/groups replication
- Bug fixes

2.10 Software v8.1 feature updates

Software v8.1 feature updates can be summarized as follows:

- New Utimaco hardware for ESKM FIPS level 2 appliance

- Added support for FIPS level 3 and level 4 ESKM appliances
- Improved cluster scalability and performance
- LCD based first time configuration support
- Support for HSM CLI commands
- Upgraded OpenSSH
- Fixed vulnerabilities and defects, including
    - Remove DH ciphers in SSH Kex algorithms
    - Updated the operating system packages
    - ESKM connecting to unknown addresses after setting a DNS server
    - ESKM is not responding through both NIC IPs when NIC2 IP is added without connecting ethernet cable
    - Failure in sending ESKM backups via SCP
    - Error in renaming ESKM CA name
    - IP authorization rules are not working

2.11 Software v8.0 feature updates

Software v8.0 feature updates can be summarized as follows:

- First virtual ESKM release with OVA deployment image
- Initial 60 day trial period for vESKM installation
- Post trial licensing support for production environment
- Support for external HSM support (General purpose and CP5)
- New WebUI interface for HSM configuration
- Improved Security features
    - Disk Encryption
    - XFS file system
    - Stronger encryption algorithms

3 Workarounds

3.1 Cluster Join Failure

Symptom: If more than one DNS server is configured in ESKM, the cluster join operation may fail.

Workaround: Please configure only one DNS server and try to join the cluster.

3.2 User Configuration Change is not Replicated When the ESKM v8 Appliance is under a Heavy Load

Symptom: When a local ESKM v8 appliance is under a heavy load, any user configuration change is not replicated to a remote node.

Workaround: Manually perform the user configuration change on the remote node.

3.3 Unable to start KMIP server after restoring a backup

Symptom: A KMIP server will not start when a backup that has a specific IP address for the KMIP server configuration is restored onto an ESKM v8 appliance that has a different IP address.

Workaround: After restoring the backup, restart the ESKM v8 appliance, and manually edit and save the KMIP server settings. This action causes the KMIP server IP field to be reset to ALL.

3.4 Multiple KMIP server restart events

Symptom: When an ESKM v8 appliance belonging to a cluster is configured to use a server certificate that is not present on the other ESKM v8 appliances in the cluster, the other ESKM v8 appliances will continuously attempt to restart their KMIP servers. This condition occurs only when either SNMP or SYSLOG is enabled on the ESKM v8 appliances in the cluster.

Workaround: Add the server certificate to all ESKM v8 appliances in the cluster, and then manually restart the KMIP server.

3.5 Management console windows do not display correctly

Symptom: After upgrading an ESKM appliance, the Management Console windows may not display correctly.

Workaround: Clear the web browser's cache, and connect to the ESKM Management Console again.

3.6 Unable to Connect to ESKM via Remote CLI

Symptom: When disabling all SSH algorithms on the ESKM v8 appliance, the SSH Administration service will stop. As a result, the ESKM will no longer be accessible via remote CLI, even after enabling the cipher suites.

Workaround: Manually start the SSH Administration service via the web based Management Console.

4 Known Issues

This section describes the issue(s) that users of ESKM may encounter.

4.1 CA certified via KMIP certify operation does not have "X509v3 Authority Key Identifier" extension

Description

KMIP certify operation can be used to certify intermediate CAs with ESKM. In ESKM 8.50 or higher, the signed CA certificate does not have the X509v3 extension "Authority Key Identifier".

5 Installation instructions

Follow the software installation procedure provided in the *ESKM v8.50.0 Installation and Replacement Guide* for the ESKM appliance.

Follow the software installation procedure provided in the *vESKM v8.50.0 Deployment Guide* for the virtual ESKM.

6 Compatibility/Interoperability

ESKM v8 requires at least OpenSSH version 7.6 or PuTTY version 0.70 to successfully establish an SSH session.

ESKM v8 supports KMIP and is continuously being tested with various KMIP clients. ESKM is demonstrated in the yearly OASIS Interop test and has previously been certified under the SNIA KMIP Conformance Test program. See the OASIS and SNIA websites for additional references:

https://www.oasis-open.org/committees/kmip/

https://www.snia.org/forums/SSIF/kmip/results

The SSIF KMIP Conformance Test Program has been retired effective September 1, 2017.

Execute the KMIP Query operation to determine the KMIP capabilities and protocol mechanisms supported by ESKM v8.

A client-side Software Developer Kit (SDK) is also available to Utimaco Partners and customers to enable native ESKM client integrations.

Existing clients that use the ESKM SDK to communicate with the ESKM v8 appliance must be recompiled with SDK version 2.0. Consult Technical Support (p. 17)or specific client product documentation for minimum client versions supported by the ESKM v8 hardware and software.

The Key Management Services (KMS) server does not service requests when an ESKM node, operating in FIPS mode, is subsequently configured to use a non-FIPS-compliant server certificate. Customers who restore data from ESKM 2.x and earlier versions can no longer use the certificates and key sizes (for example, 1024-bit RSA) that are considered non-FIPS-approved in ESKM 3.0 and above when operating in FIPS mode.

Utimaco recommends to upgrade to the latest OpenSSH version or Putty version for establishing an SSH session with ESKM.

6.1 Determining current software version

Check your current software version using the Management Console.

To access the console on your web browser, go to:
<https://<IPv4> address of the server>:<port number of the GUI>

The default web administration port number is **9443**.

Upon successful login[1], you can check the software from two locations:

- From the **Home** tab, in the **System Summary** section, the **Software Version** field identifies the installed software version.
- From the **Device** tab, in the **Maintenance** menu on the left of the screen, select **System Information & Upgrade**. In the **Device Information** section, the **Software Version** field identifies the installed software version.

In addition, you also can use the CLI command `show software all`.

[1] If you cannot connect to the Management Console, ensure that:

- Your browser version supports TLS.
- The address you are using is connected via HTTPS, not HTTP.
- The port number is correct; the default is 9443, but it could have been changed during setup.

7 Technical Support

If you have any questions about licensing, upgrading, or technical content, please contact Utimaco Technical Support:

- E-mail: support-atalla@utimaco.com[1]
- Telephone: 800-500-7858 (U.S.A.) +1-916-414-0216 (International)
- Website: https://support.utimaco.com/

7.1 Open source files

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is included in the ESKM v8 User Documentation. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Utimaco.

7.2 Effective date

April 2023

1 mailto:support-atalla@utimaco.com