



Hewlett Packard Enterprise



Interoperable

- Supports OASIS KMIP, NIST, and Hewlett Packard Enterprise standards
- Supports a growing range of Hewlett Packard Enterprise tape, disk, network, cloud, and desktop partner data protection products and solutions
- Upgradeable to new software releases
- **HPE Security ArcSight FlexConnector** for ESKM to enable external **SIEM support**

Secure

- Hardened server appliance designed as a FIPS 140-2 Level 2 cryptographic module (validation in progress) and with a Level 3 HSM option
- All software is included, preinstalled, digitally signed, and verified at startup
- Keys are always encrypted at-rest and in-motion; SSL/TLS encrypted communications
- Strong mutual certificate authentication available for client access to keys
- Local Certificate Authority as an option

Scalable

- Clusters span and serve multiple data centers, across geographic locations
- Supports tens of thousands of encryption clients and millions of keys

Reliable

- High-availability clustering, 2–8 nodes
- Performs automatic key replication, client load-balancing, and failover
- Fault-tolerant hardware with mirrored internal disks, dual power supplies, dual network ports, and redundant cooling

Manageable

- Secure remote administrator access to assign roles and privileges
- Scheduled backups and log rotations
- SNMP alerts and SIEM log monitoring

HPE Enterprise Secure Key Manager v5

Manage business-critical application encryption keys for HPE and OASIS KMIP clients

Enterprise data protection

Protecting sensitive information with data encryption

Organizations across all industry and public sectors are increasingly challenged to protect their sensitive information such as cardholder data, patient records, personally identifiable information, and intellectual property from threats such as unauthorized insider access, accidental disclosure, and theft by a range of hostile outsiders.

Auditors and regulators, due to privacy policy mandates, often require encryption of sensitive data-at-rest as a minimum standard of care and security best practice. When sensitive data at rest is encrypted, the risks of loss and audit failure that can damage business reputation and result in financial penalties, are reduced.

Key management is essential

When encryption is used to protect data at rest, strong and secure **key management** practices with automated policy enforcement are needed to manage, protect, and serve encryption keys over the life of the data. If encryption keys are compromised, data is compromised or lost, and business continuity is impacted. Finally, if an organization cannot prove that data and keys were managed and protected under verifiable security controls, it will fail compliance audits.

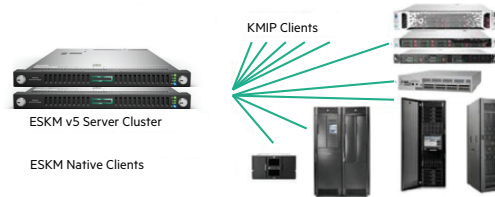
Product overview

HPE Enterprise Secure Key Manager (ESKM) provides a centralized key management hardware-based solution for unifying and automating an organization's encryption key controls by creating, protecting, serving, and auditing access to encryption keys for secure, reliable administration.

HPE ESKM supports the OASIS Key Management Interoperability Protocol (KMIP) versions 1.0 through 1.3, enabling the broadest range of data protection applications and solutions from HPE and partners. A client Software Development Kit (SDK) is also available to partners and customers to enable native protocol ESKM integrations.

ESKM is designed as a turnkey solution: an independent lab-validated secure server appliance. Standard capabilities include high-availability clustering and failover, secure key database, key generation and retrieval services, identity and access management for administrators and encryption devices, secure backup and recovery, local Certificate Authority, and signed audit logging for compliance attestation.

HPE Enterprise Secure Key Manager—v5



ESKM high-availability cluster with enrolled client systems

Software

Unified, secure, scalable encryption key management services

- Automate and enforce organizational data protection and compliance policies
- Secure encryption key generation, creation, protection, serving, auditing for enrolled clients
- Supports multiple key algorithms use cases, encryption client devices
- Capacity for >2 million keys, >25,000 clients, and 8 HPE ESKM nodes per distributed cluster

Strong auditable security

- Security hardened Linux[®]-based server appliance; all software is digitally signed
- All keys and backups are encrypted both at rest and in motion
- Granular control of key management access to key owners and across administrator defined key-sharing groups
- Certificate-based mutual client-server authentication, secure administration, and audit logging
- ESKM 5.0 is designed to FIPS 140-2 Level 2 (validation in process) or as a Level 3 option
- Locking front bezel, dual pick-resistant locks for security officer dual control

Reliable continuous access to business-critical encryption keys

- Supports mirrored internal storage, dual networks, dual power, and redundant cooling
- Native multisite high-availability clustering, encryption keys replicated securely and transparently to all nodes
- Comprehensive monitoring, recovery, scheduled backup, and restore functionality

Management

- Web browser GUI and Command Line Interface supported
- SSL/TLS and SSH for secure administrator remote access
- Terminal interface (serial RS-232C) for initial installation setup

Cryptography and security

Supports (in FIPS mode): AES (128, 192, 256), 3-key Triple DES, HMAC, and RSA (2048/3072/4096) key types. Designed for NIST SP 800-131A, and FIPS 140-2 Level 2 and Level 3 requirements. Conforms with KMIP 1.0 through 1.3 specifications.

Physical characteristics and ports

Full configuration weight: 32.8 lb (14.8 kg)
 Overall dimensions 30.87 x 19.01 x 1.69 in. (78.4 x 48.3 x 4.3 cm)
 1U rack mount; dual locking front bezel, FIPS Level 2 physical security and Level 3 HSM option, and rack mount rail kit included
 2 autosensing 10/100/1000BASE-T (Ethernet) RJ-45 ports
 1 RS-232C serial console port, 1 video port

Processor, memory, and disk

Processor: Intel[®] Xeon[®] 6-core E5-2620 v3 2.4+ GHz
 Memory: 32 GB PC4-2133P; 15 MB L3 Cache
 Disk controller: HPE Smart Array P440ar
 Disks: Dual RAID-1 (mirror) 600 GB SAS, encrypted
 Cooling: 7 High Ambient Temperature Fans

Environment

Operating temperature 50°F to 95°F (10°C to 35°C) at sea level
 Altitude up to 10,000 ft. (3050 m) with a derating of maximum operating temperature of 1.0°C per 305 m (1.8°F per every 1000 ft.) above sea level; no direct sustained sunlight
 Operating relative humidity 10% to 90%, 82.4°F (28°C) maximum wet bulb temperature, noncondensing
 Non-operating/Storage temperature -22°F to 140°F (-30°C to 60°C); maximum change 20°C/hr (36°F/hr)
 Non-operating/Storage relative humidity 5% to 95%, 101.7°F (38.7°C) maximum wet bulb, noncondensing

Electrical and thermal characteristics

Maximum heat dissipation 290 BTU/hr (305.95 kJ/hr);
 Voltage 100–240 VAC auto-ranging, Frequency 50/60 Hz; Idle power 85 W, Maximum power 135 W
Note: Idle power is the actual power consumption of the device with no ports connected or active.
 Each HPE ESKM node ships with dual redundant power supplies and two (2) IEC C13 to C14 power cords intended for rack mounting with dual PDUs and UPS for highest availability. HPE ESKM nodes may also be powered using two (2) regional power cords connecting to receptacles on separate branch circuits for highest availability.

Ordering options for HPE ESKM v5 software and servers



ESKM 3.x to 4.0 Upgrade Kit for a single node server LTU C8Z65AA

Software upgrade kit and LTU for one ESKM server. Free upgrade to version v5 software on ESKM 3.0 or 3.1 appliances after kit installation.



ESKM v5 single node server M6H81AA (Level 2) or M6H83AA (Level 3)

One ESKM v5 server node. Includes all hardware, accessories, preinstalled software, and documentation. Production clusters should be configured with a minimum of 2 and maximum of 8 nodes.

Prerequisites and limitations	Requires verification of prior ESKM 3.0 or 3.1 server purchase and a current ESKM support agreement.	Single nodes are generally recommended only for ESKM low production, test and development environments, and for expansion of production clusters. FIPS 140-2 Level 2 and Level 3 appliances can not be mixed in a cluster or physically upgraded.								
Hardware	Includes a mirror pair of disk drives pre-imaged with ESKM 4.0 software with free upgrade to v5 software.	Single node ESKM server. Includes two power supplies and IEC-IEC power cords, null modem serial cable, 1U rack mounting hardware kit, and two sets of keys to the locking bezel.								
Documentation	Includes "Read Me First" card and document CD with user guide, installation guide, and release notes.	Includes "Read Me First" card and document CD with user guide, installation guide, and release notes.								
Software	ESKM 4.0 software is included and pre-installed on disks. Software upgrades to ESKM version 5.x are available free via electronic software delivery for each unit under a current Hewlett Packard Enterprise support contract.	ESKM v5 software is included and pre-installed on the server node. Software upgrades to ESKM version 5.x are available free via electronic software delivery for each unit under a current Hewlett Packard Enterprise support contract.								
Server LTU	Includes ESKM 4.0 software LTU for one existing single server node.	Includes ESKM v5 software LTU for a single server node.								
Client LTU	Existing ESKM client licenses are preserved. Additional clients require additional client licenses, which may be purchased in any desired quantity (see table below).	Each ESKM v5 single node server includes one preinstalled ESKM client license. Additional clients require additional client licenses, which may be purchased in any desired quantity (see table below).								
	<table border="1"> <thead> <tr> <th>Order item#</th> <th>Client license item description</th> </tr> </thead> <tbody> <tr> <td>M6H94AAE</td> <td>HPE ESKM 1-9 Per Client (C Class) E-LTU</td> </tr> <tr> <td>M6H94AAE</td> <td>HPE ESKM 1-9 Per Client (D Class) E-LTU</td> </tr> <tr> <td>M6H97AAE</td> <td>HPE ESKM 1-9 Per Client (G Class) E-LTU</td> </tr> </tbody> </table>	Order item#	Client license item description	M6H94AAE	HPE ESKM 1-9 Per Client (C Class) E-LTU	M6H94AAE	HPE ESKM 1-9 Per Client (D Class) E-LTU	M6H97AAE	HPE ESKM 1-9 Per Client (G Class) E-LTU	
Order item#	Client license item description									
M6H94AAE	HPE ESKM 1-9 Per Client (C Class) E-LTU									
M6H94AAE	HPE ESKM 1-9 Per Client (D Class) E-LTU									
M6H97AAE	HPE ESKM 1-9 Per Client (G Class) E-LTU									
Support services	ESKM server node to be upgraded must be covered under an existing support agreement.	Support services must be ordered at the same time as a single node ESKM server order.								
Installation services	ESKM installation or startup, upgrade, migration, and training services are available. Please contact your Hewlett Packard Enterprise sales representative or reseller.	ESKM installation/startup, upgrade, migration, and training services are available. Please contact your Hewlett Packard Enterprise sales representative or reseller.								



ESKM 4.0/4.1—FIPS certificate #2598
ESKM 5.0—validation pending for Level 2
ESKM 5.0 Level 3 (validated).

Resources

Learn more about
HPE Enterprise Security
Products, Services, and Solutions
hpe.com/software/DataSecurity

Find ESKM product details
and related products at
hpe.com/software/eskm

Contact your local
Hewlett Packard Enterprise
Sales Representative
DataSecurity.globalsales@hpe.com

Worldwide Technical Support
Data Security Support
DataSecurity.atalla.support@hpe.com
U.S. only: +1-800-500-7858
Outside U.S.: +1-916-414-0216



HPE ESKM is Common Criteria Evaluation
Assurance Level 2+ (CC EAL2+) certified



Sign up for updates

Unify data security and secure key management controls for all your sensitive data

HPE Enterprise Secure Key Management helps protect sensitive information such as payment cardholder data, customer and employee records, electronic health records, intellectual property, cloud-hosted data, and national security and defense information with strong encryption key management.

ESKM helps organizations to comply with regulatory audits including Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA) or Health Information Technology for Economic and Clinical Health (HITECH), Graham Leach Bliley (GLBA), Sarbanes-Oxley (SOX), state and international privacy laws, national security regulations, and in addition supports internal policies, controls, and audits.

ESKM supports the OASIS KMIP standard, and a growing portfolio of Hewlett Packard Enterprise and partner encryption solutions, for protecting sensitive data at rest across storage and server media, including cloud applications.

ESKM scales easily to support large enterprise solutions across multiple geographically distributed data centers, tens of thousands of encryption clients, and millions of keys.

ESKM supports NIST, KMIP, and PCI standards and recommendations for cryptography, security, key lifecycle management and interoperability, and audit. The appliance is available as a FIPS 140-2 Level 2 validated cryptographic module or with a Level 3 HSM option to protect root secrets.

HPE Security and Services

HPE Enterprise Security

HPE Security helps organizations protect their business-critical digital assets by building security into the fabric of the enterprise, detecting and responding to advanced threats, and safeguarding continuity and compliance to effectively mitigate risk. With an integrated suite of market-leading **products, services, threat intelligence** and **security research**, HPE Security empowers organizations to balance protection with innovation to keep pace with today's idea economy. Find out more about HPE Security at hpe.com/us/en/solutions/protect-digital.html.

HPE Security Services

HPE ESP Global Services take a holistic approach to building and operating cyber security and response solutions and capabilities that support the cyber threat management and regulatory compliance needs of the world's largest enterprises. We use a combination of operational expertise—yours and ours—and proven methodologies to deliver fast, effective results, and demonstrate ROI. Our proven, use case-driven solutions combine market-leading technology together with sustainable business and technical process executed by trained and organized people.

Learn more at

hpe.com/software/eskm

hpe.com/software/DataSecurity

© Copyright 2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Intel Xeon is a trademark of Intel Corporation in the U.S. and other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. All other third-party trademark(s) is/are the property of their respective owner(s).

4AA6-5089ENW, October 2016, Rev. 2