Abstract
This document includes feature, installation, and configuration information about HPE Secure Encryption and is for the person who installs, administers, and troubleshoots servers and storage systems. Hewlett Packard Enterprise assumes you are qualified in the servicing of computer equipment and trained in recognizing hazards in products with hazardous energy levels.
# Contents

**Overview** ........................................................................................................................................... 5
  About HPE Secure Encryption .................................................................................................................. 5
  Benefits ................................................................................................................................................... 5
  Solution components ............................................................................................................................... 6

**Planning** .............................................................................................................................................. 11
  Encryption setup guidelines ...................................................................................................................... 11
  Recommended security settings at remote sites ....................................................................................... 11
  Encrypted backups ................................................................................................................................... 11
  Security domains ..................................................................................................................................... 12
  Deployment scenarios ............................................................................................................................... 12
    Remote and local key management requirements ................................................................................... 12

**Configuration** .......................................................................................................................................... 13
  Local Key Management Mode ................................................................................................................ 13
    Configuring the controller (local mode) ............................................................................................... 13
    Express Local Encryption ..................................................................................................................... 15
  Remote Key Management Mode .......................................................................................................... 16
    Configuring Remote Key Management Mode ....................................................................................... 17
    Configuring the controller (remote mode) ............................................................................................. 34

**Operations** .............................................................................................................................................. 37
  Accessing Encryption Manager ............................................................................................................... 37
  Opening Encryption Manager .................................................................................................................. 37
  Logging into Encryption Manager ........................................................................................................... 37
  Managing passwords ............................................................................................................................... 38
    Set or change the Crypto Officer password ....................................................................................... 38
    Set or change the password recovery question .................................................................................. 39
    Set or change user account password ............................................................................................... 39
    Set or change the controller password ............................................................................................... 40
    Suspending the controller password ................................................................................................. 41
    Resuming the controller password ..................................................................................................... 42
  Working with keys ................................................................................................................................... 42
    Changing the Master Encryption Key .................................................................................................. 42
    Rekeying the Drive Encryption Keys .................................................................................................... 43
    Rescanning keys ................................................................................................................................... 44
    Enabling Encryption Key Manager Authentication ......................................................................... 44
    Volatile keys .......................................................................................................................................... 45
  Creating a plaintext volume ....................................................................................................................... 51
  Converting plaintext volumes into encrypted volumes ............................................................................ 54
  Changing key management modes .......................................................................................................... 55
  Enabling/disabling plaintext volumes ..................................................................................................... 56
  Enabling/disabling the firmware lock ...................................................................................................... 57
  Enabling/disabling local key cache .......................................................................................................... 58
  Importing drive sets in Local Key Management Mode .......................................................................... 59
    Importing drives with different Master Keys ....................................................................................... 59

**Maintenance** .......................................................................................................................................... 61
  Controllers ................................................................................................................................................ 61
    Clearing the controller ......................................................................................................................... 61
    Replacing an encrypted controller ....................................................................................................... 61
    Replacing a server while retaining the controller .................................................................................. 61
    Preconfiguring replacement components ............................................................................................ 61
    Flashing firmware ............................................................................................................................... 62
  Drives ....................................................................................................................................................... 62
Overview

About HPE Secure Encryption

HPE Secure Encryption is a controller-based, enterprise-class data encryption solution that protects data at rest on bulk storage hard drives and SSDs attached to a compatible HPE Smart Array Controller. The solution is compatible with the HPE Secure Key Manager, and can operate with or without the presence of a key manager in the environment, depending on individual customer settings.

Secure Encryption provides encryption for data at rest as an important component for complying with sensitive data protection requirements including PCI-DSS, HIPAA/HITECH, Sarbanes/Oxley, and state privacy laws. Secure Encryption secures any data deemed sensitive and requiring extra levels of protection through the application of XTS-AES 256-bit data encryption. Many companies under government regulations require that sensitive privacy data must be secured and uncompromised using NIST-approved algorithms and methodologies for key management. Secure Encryption is validated for FIPS-140-2 Level 2 for Smart Array Px3x controllers supporting encryption. HPE Smart Array Px4x controller validation is in progress. For more information, see the Cryptographic Module Validation Program (CMVP) on the National Institute of Standards and Technology website (http://csrc.nist.gov/groups/STM/cmvp/validation.html).

Secure Encryption requires the following core components:

- ProLiant Gen8 or later server
- Smart Array Controller, version Px3X or later. For a list of currently supported controllers, see "Smart Array Controller ("HPE Smart Array Controller" on page 7)"
- Secure Encryption license, per server
- HPE Smart Storage Administrator, version 1.60 or later
- Compatible SAS/SATA hard drive or SSD
- Compatible storage enclosure

Secure Encryption can operate in Remote Key Management Mode, or Remote Mode, through the use of a separate, clustered, appliance-based server called the HPE Enterprise Secure Key Manager. The HPE ESKM manages all encryption keys throughout the data center. When utilizing the ESKM, the communication path between the ESKM and the Smart Array Controller is established through the HPE iLO interface. The controller communicates with the ESKM as new keys are generated and as old keys are retired. The ESKM acts as a key vault where all keys are managed via a web browser interface. For more information about the ESKM, see "Enterprise Secure Key Manager (on page 9)." For more information about iLO connectivity, see "iLO ("HPE iLO" on page 9)."

The following additional components are required for operating Secure Encryption in Remote Mode:

- Integrated Lights Out (iLO) Advanced or Scale Out Edition license, per ProLiant server
- Enterprise Secure Key Manager

Secure Encryption can also operate without an attached key management solution through Local Key Management Mode, or Local Mode.

Benefits

Broad encryption coverage

- Encrypts data on both the attached bulk storage and the cache memory of Smart Array Controllers
- Supports any hard drive or SSD in the Smart Drive portfolio for ProLiant Gen8 or later servers or the Supported Storage Enclosures

**High availability and scalability**
- Scales to meet individual data privacy requirements
  - Server counts up to 25,000
  - Millions of drives
  - Millions of encryption keys
- The ESKM supports High Availability Clustering, from 2-8 nodes.

**Simplified deployment and management**
HPE Smart Storage Administrator configures the cryptographic features of Secure Encryption, and manages the controller and other direct-attached storage devices

**Helps users meet compliance regulations**
- The ESKM is FIPS 140-2 Level-2 validated, certificate #1922
- The HPE Smart Array Gen8 Pxn family of controllers is FIPS 140-2 Level-2 validated; certificate #2375
- The HPE Smart Array Gen9 Pxn controllers P244br, P246br, P440, P441, and P741m are FIPS 140-2 Level-1 validated; certificate #2506

**Solution components**

**HPE Smart Storage Administrator**
The HPE SSA is a configuration and management tool for HPE Smart Array controllers. Starting with HPE ProLiant Gen8 servers, HPE SSA replaces ACU with an enhanced GUI and additional configuration features.

The HPE SSA exists in three interface formats: the HPE SSA GUI, the HPE SSA CLI, and HPE SSA Scripting. Although all formats provide support for configuration tasks, some of the advanced tasks are available in only one format.

Some HPE SSA features include the following:
- Supports online array capacity expansion, logical drive extension, assignment of online spares, and RAID or stripe size migration
- Provides diagnostic and SmartSSD Wear Gauge functionality on the Diagnostics tab
- For supported controllers, provides access to additional features.

For more information about HPE SSA, see the Hewlett Packard Enterprise website ([http://www.hpe.com/servers/ssa](http://www.hpe.com/servers/ssa)).

**Minimum requirements**
For minimum operating system requirements to run any SSA format, see the Hewlett Packard Enterprise website ([http://www.hpe.com/info/ossupport](http://www.hpe.com/info/ossupport)).

Minimum video requirements to run the SSA GUI include a minimum monitor resolution of 1024x768 and 16-bit color. The GUI supports the following browsers:
- Mozilla Firefox 9.0 or later
- Microsoft Internet Explorer 8.0 or later
- Google Chrome
HPE Smart Array Controller

Secure Encryption is supported on HPE Smart Array PX3X and PX4X controllers, and on HX4X HPE Smart HBAs operating in RAID mode.

For more information about controllers supporting Secure Encryption, see the Hewlett Packard Enterprise website (http://www.hpe.com/servers/smartarray).

For more information about Smart Array controllers, see the appropriate Smart Array controller user guide on the Hewlett Packard Enterprise website (http://www.hpe.com/info/smartstorage-docs).

Encryption features

Most Secure Encryption features and security settings are available through HPE Smart Storage Administrator. Additional features for Remote Mode deployments are available through Enterprise Secure Key Manager and Integrated Lights Out (iLO).

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic key management</td>
<td>Encryption keys are automatically created, saved, and deleted by Smart Array Controllers without the need for user intervention or management when logical drives are created or deleted.</td>
<td>For more information, see &quot;Encryption Algorithms (on page 87).&quot;</td>
</tr>
<tr>
<td>Compliance</td>
<td>Secure Encryption has been designed to meet NIST-approved standards. The ESKM has completed FIPS 140-2 Level-2 validation, certificate #1922. Secure Encryption helps enterprises comply with the data privacy and protection requirements associated with the U.S. Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Acts.</td>
<td></td>
</tr>
<tr>
<td>Controller key cache</td>
<td>Smart Array Controllers can optionally store all keys required at boot time inside the controller, enabling the server to survive a variety of network outages.</td>
<td>Remote Mode only</td>
</tr>
<tr>
<td>Controller password</td>
<td>Protects the server in the event of theft by applying a secondary password upon boot to lock down the controller.</td>
<td>For more information, see &quot;Set or change the controller password (on page 40).&quot;</td>
</tr>
<tr>
<td>Dynamic Encryption</td>
<td>Enables smooth transitions between local and remote modes, the conversion of plaintext data to encrypted data, and rekey services for both data and key wraps.</td>
<td></td>
</tr>
<tr>
<td>Encryption keys</td>
<td>Data is protected using a series of keys that provide layered protection at the volume and drive levels. The solution utilizes XTS-AES 256-bit encryption.</td>
<td></td>
</tr>
<tr>
<td>Enterprise Secure Key Manager</td>
<td>The ESKM unifies and automates an organization’s encryption controls by securely creating, protecting, serving, controlling, and auditing access to encryption keys.</td>
<td>Remote Mode only. For more information, see &quot;HPE Enterprise Secure Key Manager (&quot;Enterprise Secure Key Manager&quot; on page 9).&quot;</td>
</tr>
<tr>
<td>ESKM key search</td>
<td>Individual Drive Encryption Keys are visible by serial number identification on the ESKM to enable unique tracking and management from a central location. The ESKM supports query by serial number, server name, bay number, PCI slot, and date.</td>
<td>Remote Mode only. For more information, see &quot;Running queries (on page 72).&quot;</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Firmware lock</td>
<td>Prevents controller firmware from being updated unintentionally or by</td>
<td>For more information, see &quot;Enabling/disabling the firmware lock (on page 57).&quot;</td>
</tr>
<tr>
<td></td>
<td>unauthorized personnel.</td>
<td></td>
</tr>
<tr>
<td>Hardware-based encryption</td>
<td>Utilizes the Smart Array Controller hardware to accelerate all cryptographic</td>
<td>For more information about Smart Array controllers, see the website (<a href="http://www.hpe.com/servers/smartarray">http://www.hpe.com/servers/smartarray</a>).</td>
</tr>
<tr>
<td></td>
<td>algorithms when securing data and keys.</td>
<td></td>
</tr>
<tr>
<td>Integrated Lights Out (iLO)</td>
<td>iLO Management is a comprehensive set of embedded management features</td>
<td>Remote Mode only. For more information, see &quot;iLO (&quot;HPE iLO&quot; on page 9).&quot;</td>
</tr>
<tr>
<td></td>
<td>supporting the complete lifecycle of the server, from initial deployment,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>through ongoing management, to service alerting and remote support. iLO is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>provided on all ProLiant Gen8 and later servers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>iLO 4 Advanced or Scale Out editions v1.40 or later connect and auto-register</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with the ESKM. iLO provides key exchange support between the Smart Array</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controller and the ESKM to enable pre-boot support for OS disk encryption.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Audit support is provided for all key management transactions.</td>
<td></td>
</tr>
<tr>
<td>Instant volume erase</td>
<td>Provides ability to instantly, cryptographically erase logical volumes</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>without having to delete the volume first.</td>
<td></td>
</tr>
<tr>
<td>Key rotation support</td>
<td>Supports the rekeying of all keys utilized by the controller to enable a</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>robust key rotation strategy.</td>
<td></td>
</tr>
<tr>
<td>Local Key Management Mode</td>
<td>Focused on single server deployments where there is one Master Encryption</td>
<td>For more information, see &quot;Local Key Management Mode (on page 13).&quot;</td>
</tr>
<tr>
<td></td>
<td>Key per controller that is managed by the user. In Local Mode, all volumes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>still have their own unique key for data encryption.</td>
<td></td>
</tr>
<tr>
<td>One-way encryption</td>
<td>As a security feature, data volumes cannot be converted back to plaintext</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>after the volume is encrypted. Restoration of data is required to revert</td>
<td></td>
</tr>
<tr>
<td></td>
<td>back to plaintext.</td>
<td></td>
</tr>
<tr>
<td>Pre-deployment support</td>
<td>Supports the ability to preconfigure all cryptographic security settings</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>while in a server, then store the powered-off controller for later use while</td>
<td></td>
</tr>
<tr>
<td></td>
<td>retaining the settings securely.</td>
<td></td>
</tr>
<tr>
<td>Remote Key Management Mode</td>
<td>Designed for enterprise-wide deployments with the Smart Array Controller.</td>
<td>For more information, see &quot;Remote Key Management Mode (on page 16).&quot;</td>
</tr>
<tr>
<td></td>
<td>It requires the Enterprise Secure Key Manager to manage all keys related to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>encryption deployments. All keys are managed automatically between the Smart</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Array Controller, iLO and the ESKM.</td>
<td></td>
</tr>
<tr>
<td>Security reset function</td>
<td>The feature clears all secrets, keys, and passwords from the controller,</td>
<td>For more information, see &quot;Clearing the encryption configuration (on page 84).&quot;</td>
</tr>
<tr>
<td></td>
<td>and places the controller’s encryption configuration in a factory new state.</td>
<td></td>
</tr>
</tbody>
</table>
HPE SmartCache

HPE SmartCache can be used in conjunction with Secure Encryption. SmartCache enables solid state drives to be used as caching devices for hard drive media. Data can be accessed from the solid state drive instead of hard drives. Data stored on the SmartCache drive utilizes the same encryption methods and keys as the originating volume where the data is permanently stored, extending protection to the SmartCache drives.

SmartCache provides the following features:

- Accelerates application performance
- Provides lower latency for transactions in applications
- Supports all operating systems, without the need for changes

SmartCache requires a SmartCache license. For more information, or to obtain a license, see the Hewlett Packard Enterprise website (http://www.hpe.com/servers/smartcache).

HPE iLO

iLO Management is a set of embedded management features that support the complete life cycle of the server, from initial deployment, to ongoing management, to service alerting and remote support.

The iLO subsystem is a standard component of HPE ProLiant servers that simplifies initial server setup, server health monitoring, power and thermal optimization, remote server administration, and key exchanges between the ESKM and the Smart Array Controller. The iLO subsystem includes an intelligent microprocessor, secure memory, and a dedicated network interface. This design makes iLO independent of the host server and its operating system. This system provides client credentials, registration to the key management database, key management, encryption activation, and audit support for the devices within the platform.

For the full implementation of HPE Secure Encryption with the ESKM, HPE iLO Advanced or HPE iLO Scale Out editions are required to connect and auto-register with the ESKM. iLO provides key exchange support between the Smart Array Controller and the ESKM to enable pre-boot support for OS disk encryption. Audit support is provided for all for key management transactions.

For more information about iLO, see the Hewlett Packard Enterprise website (http://www.hpe.com/info/ilo).

Enterprise Secure Key Manager

Enterprise Secure Key Manager acts as a secure, reliable repository for keys used by HPE Secure Encryption. In Remote Key Management Mode, iLO connects to the ESKM using username/password and digital certificate authentication to securely store and retrieve keys. Each iLO must be registered as an ESKM user by an administrator, or Crypto Officer, of the ESKM for access to be granted. If a user is registered and has the necessary permissions, the ESKM accepts requests and provides keys to the
As standard practice, communication with the ESKM is configured for SSL to ensure the security of the connection and authorized access to keys.

The ESKM keys and users can be organized into different groups depending on the policies set by an administrator. These groups determine whether a particular user can retrieve a particular key, and supports both key sharing and separation for multi-tenant and hosted service provider environments.

**Characteristics**

- Used only in Remote Mode, requiring a network connection
- Supports high-availability clustering of 2-8 ESKM nodes for automatic replication and failover
- Provides key services to iLO clients using username and password, certificate authentication, or both
- Communicates using SSL encryption to ensure the security of the connection and authorized access to keys
- Provides reliable, secure access to business-critical encryption keys
- Supports audit and compliance requirements, including PCI-DSS and HIPAA/HITECH
- Provides scalability for multiple data centers, thousands of clients, and millions of keys
- Uses a FIPS-140-2 Level 2 validated secure appliance which supports the latest NIST cryptographic guidance

**ESKM and key management**

The Smart Array Controller manages keys by separating them into the following categories:

- Keys stored off-controller on the ESKM
- Keys stored on the drive media
- Keys stored on the controller

The separation of keys helps ensure the safety of the data residing on the drives, the portability of the drives, and the ability to manage keys in a centralized manner. The controller uses the ESKM to back up a segment of its keys using an encryption method that protects the keys from exposure in plaintext.

**Licensing**

Depending on when you initially set up Secure Encryption, licensing is based on the number of servers requiring encryption, or is on a per-drive basis. If configuring after June 2015, you will need one Secure Encryption license (C9A82AAE) per server. Once configured, Secure Encryption applies to all storage devices internally or externally attached to the Smart Array controllers in the server.

Though you are required to purchase an entitlement license for each server to authorize use, HPE Smart Storage Administrator does not require that you input a license key to enable encryption via a configuration change in the controller and iLO.

In addition to a physical Enterprise Secure Key Manager, Secure Encryption operating in Remote Key Management Mode requires the following licenses:

- Integrated Lights Out (iLO), Advanced or Scale Out edition, version 1.4 or later
- One Enterprise Secure Key Manager Client License per ProLiant server
Planning

Encryption setup guidelines

When setting up Secure Encryption, consider the information described in the following table.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Options</th>
<th>Deciding factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption mode</td>
<td>• Local Key Management Mode</td>
<td>Choose Local Key Management Mode when:</td>
</tr>
<tr>
<td></td>
<td>• Remote Key Management Mode</td>
<td>• Data is stored at a site without network access.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In a small deployment center or lab</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Manual key management is available.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Choose Remote Key Management Mode when:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Using a large number of servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A network is available between the ESKM and a server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Automatic key management is preferred, including backups and redundancy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configurations</td>
</tr>
<tr>
<td>Plaintext volumes</td>
<td>• Allow</td>
<td>Allow future plaintext logical drives when:</td>
</tr>
<tr>
<td></td>
<td>• Disallow (default)</td>
<td>• Drive migration might occur to a non-encrypting controller.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data is not privacy-sensitive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information, see &quot;Enabling/disabling plaintext volumes (on page 56).&quot;</td>
</tr>
<tr>
<td>Key naming conventions</td>
<td>Master Encryption Keys are customizable.</td>
<td>Create a specific naming convention when managing multiple keys and multiple servers.</td>
</tr>
</tbody>
</table>

Recommended security settings at remote sites

For added security, Hewlett Packard Enterprise recommends the following configuration when operating Secure Encryption at remote sites outside the main data center.

- Firmware lock enabled ("Enabling/disabling the firmware lock" on page 57)
- Controller password enabled ("Set or change the controller password" on page 40)
- Plaintext volumes disabled ("Enabling/disabling plaintext volumes" on page 56)
- Local Key Cache disabled ("Enabling/disabling local key cache" on page 58)

Applies to Remote Key Management Mode only

Encrypted backups

At system startup, all encrypted data-at-rest becomes accessible to the host system in unencrypted form via the controller and the appropriate keys. This method of startup allows the system to boot into an operating system installed on an encrypted volume. As a result, encrypted backups are not available, and all data appears unencrypted when accessed from the host system and placed on tape. Software or hardware utilizing an independent encryption feature is not impacted by Secure Encryption.
Security domains

A security domain is a blueprint for separating out different groups of servers or key management escrows where access to a set of keys is inhibited by the structure of the various domains. The best mechanisms for establishing separate security domains are either through the use of separate ESKM or via the use of groups within the ESKM. Unique groups provide a software mechanism for each server to partition off their key sets from one server to another. Groups are created on the ESKM and assigned to a server via the HPE iLO Key Manager page. For more information, see "Remote Key Management Mode (on page 16)."

Deployment scenarios

Remote and local key management requirements

Use the table below to determine which encryption mode is right for you.

<table>
<thead>
<tr>
<th>Mode parameters</th>
<th>Local Key Management Mode</th>
<th>Remote Key Management Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of servers</td>
<td>&lt;99 (recommended)</td>
<td>100 or more</td>
</tr>
<tr>
<td>ESKM available</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Integrated Lights Out (iLO)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Advanced or Scale Out License</td>
<td></td>
<td></td>
</tr>
<tr>
<td>available</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement to escrow keys</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Manual tracking of keys</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Configuration

Local Key Management Mode

Local Key Management Mode, or Local Mode, is a solution designed for small to medium-size data centers using few encrypting controllers. The solution utilizes a paraphrase password, or Master Encryption Key name, to set the security on the controller and enable encryption. The Master Encryption Key must be tracked independently of the controllers in case the controller needs replacement or drive migration is required among controllers with different passwords. In local mode, the Master Key name is considered a cryptographic secret and should be protected as such. Key creation and management is maintained at the local controller level without the use of a key manager.

Characteristics

- Requires physical paraphrase password management, such as writing and storing Master Key information in a notebook or computer file
- Utilizes one paraphrase password-derived 256-bit key to encrypt a unique, per-volume XTS-AES 256-bit data encryption key

Prerequisites

- An installed Smart Array Controller compatible with Secure Encryption
- A valid Secure Encryption license for each server to be encrypted. This license must be purchased, but it does not need to be input into HPE Smart Storage Administrator.
- HPE Smart Storage Administrator v1.60.xx.0 and later
- ProLiant Gen8 or later server

Configuring the controller (local mode)

**IMPORTANT:** Hewlett Packard Enterprise recommends that you keep a record of the Master Encryption Keys when encryption is configured in Local Mode. The local Master Encryption Key is not displayed by any available tool or firmware because it is considered a cryptographic secret by FIPS 140-2. Secure Encryption design follows the NIST architecture requirements and does not allow Hewlett Packard Enterprise to assist in the recovery of a lost Master Encryption Key.

To configure Secure Encryption using command line or scripting methods, see the HPE Smart Storage Administrator user guide.

To configure the controller to operate in Local Key Management Mode:

1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Click **Perform Initial Setup**.

The following screen appears.

3. Complete the following:
   - Under **Setup Type**, select **Full Setup**.
   - Under **New Password**, enter and then re-enter the Crypto Officer password in the fields provided.
   - Under **Encryption Mode**, select either:
     - **Enable and Allow Future Plaintext Volumes**: Allowing future plaintext volumes still requires authentication by the Crypto Officer or the User before a plaintext volume can be created.
     - **Enable and Disallow Future Plaintext Volumes**: This option prevents the creation of new plaintext volumes on the controller. This setting can be changed later by the Crypto Officer. Selecting this option does not prevent the migration of a set of drives with existing plaintext volumes to the controller.
   - Under **Key Management Mode**, select **Local Key Management Mode**.
Enter the Master Key name in the field provided. The Master Encryption Key name must be between 10 and 64 characters.

4. Click OK.

5. A warning appears, prompting the user to record the Master Encryption Key. Click Yes to continue.

6. If you have read and agree to the terms of the EULA, select the check box and click Accept.

7. A summary screen appears, indicating the controller has been successfully configured for encryption use. Click Finish to continue.

8. The Encryption Manager screen appears with updated Settings, Accounts and Utilities options.

   IMPORTANT: Hewlett Packard Enterprise recommends setting up a password recovery question and answer after initial configuration. If the Crypto Officer password is lost and a recovery question and answer have not been set, you will need to erase and reconfigure all Secure Encryption settings in order to reset the Crypto Officer password. For more information, see "Set or change the password recovery question (on page 39)."

   To configure Secure Encryption using command line or scripting methods, see the HPE Smart Storage Administrator user guide.

Express Local Encryption

About Express Local Encryption

   IMPORTANT: Express Local Encryption configures Secure Encryption in Local Key Management Mode. Once configured, you will not have a Crypto Officer password.

   IMPORTANT: Express Local Encryption uses a randomly-generated Master Encryption Key. Features requiring the input of a Master Encryption Key, such as migrating volumes to a new controller, will not be available while Express Local Encryption is enabled.

Express Local Encryption configures the controller with predetermined encryption settings and a randomly-generated Master Encryption Key. Once configured, encryption settings changes will not be possible without clearing the encryption configuration.

Express Local Encryption enables the following:

- Controller encryption
- Local Key Manager Mode
- Random crypto password, not recoverable
- Random master key name, not recoverable
- Future plaintext volumes not allowed

Setting up Express Local Encryption

1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Click **Perform Initial Setup**. A new window appears.

3. Under **Setup Type**, select **Express Local Encryption**. Once selected, all other encryption setup options disappear. Click **OK** to continue.

4. A warning appears. Click **Yes** to continue.

5. If you have read and agree to the terms of the EULA, select the check box and click **Accept**.

6. The **Encryption Manager** screen appears with updated **Settings**, **Accounts** and **Utilities** options.

**Remote Key Management Mode**

重要提示：**Enterprise Secure Key Manager** 必须已经安装并配置好以运行在远程模式下的安全加密。更多信息，请参阅"配置 ESKM（第 17 页）"。

在远程密钥管理模式下，密钥在控制器和 ESKM 之间进行导入和导出。ESKM 中提供了冗余的、安全的存储，且控制器能够连续访问这些密钥。要使控制器和 ESKM 进行密钥交换，必须建立网络连接。控制器不具有直接的网络访问能力。ilo 提供了必要的网络访问，以支持控制器和 ESKM 之间的密钥交换。ilo 在网络连接期间和操作系统运行期间都保持系统活跃，且控制器和 ESKM 之间的密钥交换本身就在 AUX 电源上。这些密钥在 ilo、ESKM 之间交换时都是被安全处理的。

为每台要加密的服务器购买有效的安全加密许可证是必需的。此许可证必须购买，但不需要输入到 HPE Smart Storage Administrator 中。

**特性**

- 高容量密钥存储
• Keys are kept in separate storage from servers to protect against physical removal
• Requires network availability and a remote key management system

Configuring Remote Key Management Mode

**IMPORTANT:** Secure Encryption and other encryption client products must be coordinated for a successful installation and configuration. It is recommended to refer to each product's user guide to ensure proper installation and encryption protection.

To configure Secure Encryption to operate in Remote mode:

1. Configure the ESKM ("Configuring the ESKM" on page 17). For more information about installation, configuration and operation of the ESKM, see the Enterprise Secure Key Manager user guide and the Installation and Replacement guide.
2. Connect iLO to the ESKM.
3. Install HPE SSA. For more information, see the HPE Smart Storage Administrator user guide.
4. Configure the Smart Array Controller.

Configuring the ESKM

1. Log in to the ESKM ("Logging in to the ESKM" on page 17).
2. Create initial user accounts ("Adding a user" on page 17).
   a. Create an account called **DeployUser**.
   b. Create an account called **MSRUser**.
3. Create a group ("Adding a group" on page 19).
4. Assign the user account for hosting Master Encryption Keys to the group created in step 3 ("Assigning a user to a group" on page 21).
5. Create a Master Encryption Key to be used by the controller ("Creating a Master Key" on page 24). Be sure to set the owner of the key to the user account created to host the Master Encryption Key created in Step 2b.
6. Place the Master Encryption Key in the group created in step 3 ("Placing a key in a group" on page 26).

Logging in to the ESKM

1. Open a new browser window and enter the IPv4 address and web administration port number using https. The port is user-configurable. The default port is 9443.
   **Example:** https://11.12.13.14:9443
2. Log in using administrator credentials.

Adding a user

**IMPORTANT:** Passwords must contain at least five different characters. Passwords cannot:
- Contain only whitespace
- Resemble a phone number, dictionary word or reversed dictionary word
- Be based on the username associated with the password

The deployment user is the first user account created. It allows iLO to connect to the ESKM and begin using keys. Subsequent standard user accounts are assigned Master Encryption Keys.

To add a user:

1. Log in to the ESKM ("Logging in to the ESKM" on page 17).
2. Click the **Security** tab.

3. Click **Local Users & Groups**.

4. Under **Local Users**, click **Add**.

**User and Group Configuration**

**Local Users**

<table>
<thead>
<tr>
<th>Username</th>
<th>KMIP-Enabled</th>
<th>User Administration Permisssion</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeployUser</td>
<td>✔</td>
<td>□</td>
</tr>
</tbody>
</table>

1 - 1 of 1
The dialog above shows a deploy user being added. The following fields appear.

5. Complete the following fields:
   - Username
   - Password
   - Confirm Password
   - If this is the deployment user account, select the **User Administration Permission** and **Change Password Permission** check boxes.
   - If this is a standard user account, leave the **User Administration Permission** and **Change Password Permission** check boxes empty.
   - Leave the **Enable KMIP** check box empty.

6. Click **Save**.

Adding a group

Groups enable you to organize a set of servers together and restrict access only to a specific set of users.
To add a group:

1. Log in to the ESKM ("Logging in to the ESKM" on page 17).
2. Click on the Security tab.
3. Click Local Users & Groups.
4. Under Local Groups, click Add.

5. Enter the group name in the Group entry field.

6. Select ESKM in the Group Type field.

7. Click Save.

Assigning a user to a group

1. Log in to the ESKM ("Logging in to the ESKM" on page 17).
2. Click on the **Security** tab.

3. Click **Local Users & Groups**.
4. Under **Local Groups**, select the group name and click **Properties**.

A new window appears, listing the group properties.

5. Click **Add**.
6. Enter the Username in the field provided.

Local Group Configuration

Properties

Local Group Properties

<table>
<thead>
<tr>
<th>Group:</th>
<th>Sample_Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Type:</td>
<td>ESKM</td>
</tr>
<tr>
<td>Group Sub-type:</td>
<td>Users</td>
</tr>
</tbody>
</table>

Back

User List

Filtered by _ _ _ _ where value contains _ _ _ _

Username

Save  Cancel

7. Click Save.

Creating keys

About keys

Master keys are used to wrap the drive keys and are stored on the ESKM in remote mode. In general, one master key is used for a group of servers that provide similar functionality or belong to a specific department. This allows you to swap the drives among the servers. Depending on your environment, you can create one master key for a server, a project, a department, or for an entire deployment.

The ESKM does not differentiate between key types such as Master Encryption Key or Drive Encryption Key. If creating a Master Encryption Key, Hewlett Packard Enterprise recommends applying a specific Master Encryption Key naming convention to distinguish the Master Key from all other keys created in the ESKM. You should have one Master Key for each iLO.

Creating a Master Key

1. Log in to the ESKM ("Logging in to the ESKM" on page 17).
2. Click the **Security** tab.

3. From the left side panel, expand the **Keys** menu, and then click **Create Keys**.
The following screen appears.

Security » Keys » Create Keys

Key and Policy Configuration

Create Key

4. Under the section Create Key, complete the following:
   - **Key Name**: Enter the preferred key name.
     The name must consist only of US-ASCII letters, numbers, or the underscore or hyphen characters, and must be between 8 and 64 characters. The minimum character length is required by the Smart Array controller, not by the ESKM.
   - **Owner Username**: Enter the name of the user account to be paired with the key. If creating the Master Encryption Key, do not assign keys to the deployment user account.
   - **Algorithm**: Select AES-256.
     - Select the **Exportable** checkbox. Leave the remaining fields as the default values.

5. Click Create. You will receive a notification that the key was created successfully.

Placing a key in a group

A key must be assigned a group in order to enable access by iLO. To place a key in a group, do the following:

1. Run a key query and locate the key created ("Running a key query" on page 26).
2. Assign the key to a group ("Assigning a key to a group" on page 29).

Running a key query

1. Log in to the ESKM ("Logging in to the ESKM" on page 17).
2. Click the **Security** tab.

3. From the left side panel, expand the **Keys** menu and click **Query Keys**.
The following screen appears.

4. Click **Add**.

The following screen appears.

5. Complete the following fields:
   a. Query Name
   b. Query Type
   c. Description

6. Click **Next**.
The following screen appears.

7. Under **Create Query**, complete the following:
   a. **Query Name**: Enter a query name here. Your query will be saved for future use.
   b. **Choose Keys Where** drop down menu: select **Owner**, or **Key Name**. Two additional **Choose Keys Where** fields appear.

8. Complete the following fields:
   a. Field 1: Leave as default.
   b. Field 2: Leave as default.
   c. Field 3: Enter the user account name associated with the Master Key, or the Master Key name, depending on your selection for **Choose Keys Where**.

9. Click **Save and Run Query**. A results screen appears, displaying the Master Key name.

Assigning a key to a group
1. Log in to the ESKM ("Logging in to the ESKM" on page 17).
2. Run a key query for the preferred key ("Running a key query" on page 26).
3. Select the key, and then click **Properties**.

4. A new **Key and Policy Configuration** screen appears. Click the **Permissions** tab.

5. Under **Group Permissions**, complete the following:
a. In the **Group** field, enter the **Group** name created previously.
b. Under **Export**, select **Always**.
c. Under **Full**, leave deselected (default).
6. Click **Save**. The screen will refresh and list the group permissions.

### Configuring iLO

Integrated Lights Out (iLO) manages key exchanges between the ESKM and the Smart Array controller. iLO initially uses user credentials with administrative privileges created on the ESKM to automatically register and create a private, unique, MAC address-based username account for all key exchanges. The administrative account is termed the deployment user account. All iLO accounts can be viewed in the ESKM under Users And Groups and take the form iLO-MAC Address. The iLO-specific account is placed in the group indicated in the group field on the iLO Key Manager page. If the group does not exist, iLO creates one and places the account in that group along with all future keys generated.

### Prerequisites

- The ESKM must be configured with a deployment user. For more information, see "Configuring the ESKM (on page 17)."
- iLO must be installed and operating properly with the appropriate iLO-supporting license.

For more information on installing and configuring iLO, including scripting and command line methods, see the Hewlett Packard Enterprise website ([http://www.hpe.com/info/ilo/docs](http://www.hpe.com/info/ilo/docs)).

### Connecting iLO to the ESKM

If you intend to use a second ESKM for a redundant key repository, complete the fields under **Secondary Key Server** and select the **Enable Enterprise Secure Key Manager Redundancy** check box. Hewlett Packard Enterprise strongly recommends a redundant pair of ESKM devices in a cluster configuration.

To connect iLO to the ESKM:
1. Log in to iLO using your server’s credentials.
2. From the left side panel, expand the **Administration** menu and select **Key Manager**.
The **Enterprise Secure Key Manager** configuration page appears.

### Key Manager Servers

**Primary Key Server**
- **Address**: Enter the primary IP address of the ESKM in the *Address* field.
- **Port**: Enter the primary port number of the ESKM in the *Port* field. This port number should match the value on the ESKM, located on the **Device** tab under **KMS Server Settings**. SSL should be enabled on the ESKM as well.

**Secondary Key Server**
- **Address**: Enter the secondary IP address of the ESKM in the *Address* field.
- **Port**: Enter the secondary port number of the ESKM in the *Port* field.

**Require Redundancy**
- Select the **Require Redundancy** check box. This option enables iLO to verify that encryption keys are copied to all configured key servers. For configurations with a primary and secondary key server, Hewlett Packard Enterprise recommends enabling this option.

4. Click **Apply**. A confirmation message appears.

---

1. Under **Key Manager Servers**, complete the following:

2. **Primary Key Server**:
   - Enter the primary IP address of the ESKM in the *Address* field.
   - Enter the primary port number of the ESKM in the *Port* field. This port number should match the value on the ESKM, located on the **Device** tab under **KMS Server Settings**. SSL should be enabled on the ESKM as well.

3. **Secondary Key Server**:
   - Enter the secondary IP address of the ESKM in the *Address* field.
   - Enter the secondary port number of the ESKM in the *Port* field.

4. **Select the Require Redundancy check box. This option enables iLO to verify that encryption keys are copied to all configured key servers. For configurations with a primary and secondary key server, Hewlett Packard Enterprise recommends enabling this option.**

5. **Click Apply**. A confirmation message appears.
5. Under Key Manager Configuration, enter the group name created previously in the ESKM in the Group field.

6. Under ESKM Administrator Account, complete the following fields using the deployment username and password created earlier on the ESKM.
   a. Login Name: Enter the deployment account username.
   b. Password: Enter the deployment account password.

7. Click Update ESKM. A confirmation screen appears, indicating the configuration was saved and connected successfully.

Configuring the controller (remote mode)

To configure Secure Encryption using command line or scripting methods, see the HPE Smart Storage Administrator user guide.

To configure the controller to operate in Remote Key Management Mode:

1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Click Perform Initial Setup.
A new screen appears.

3. Complete the following:
   - Under **Setup Type**, select **Full Setup**.
   - Under **New Password**, enter and then re-enter the Crypto Officer password in the fields provided.
   - Under **Encryption Mode**, select either:
     - **Enable and Allow Future Plaintext Volumes**: Allowing future plaintext volumes still requires authentication by the Crypto Officer or the User before a plaintext volume can be created.
     - **Enable and Disallow Future Plaintext Volumes**: This option prevents the creation of new plaintext volumes on the controller. This setting can be changed later by the Crypto Officer. Selecting this option does not prevent the migration of a set of drives with existing plaintext volumes to the controller.
   - Under **Key Management Mode**, select **Remote Key Management Mode**.
   - Enter the **Master Key** name created on the ESKM in the field provided.

4. Click **OK**.
5. A EULA screen appears. If you have read and agree to the terms of the EULA, select the check box and click **Accept**.

6. A summary screen appears, indicating the controller has been successfully configured for encryption use. Click **Finish** to continue.

7. The **Encryption Manager** home screen appears with updated **Settings**, **Accounts**, and **Utilities** options.

**IMPORTANT:** Hewlett Packard Enterprise recommends setting up a password recovery question and answer after initial configuration. If the Crypto Officer password is lost and a recovery question and answer have not been set, you will need to erase and reconfigure all Secure Encryption settings in order to reset the Crypto Officer password. For more information, see "Set or change the password recovery question (on page 39)."
Operations

Accessing Encryption Manager

Opening Encryption Manager
1. Start HPE SSA. For more information, see the HPE Smart Storage Administrator user guide.
2. Select a Secure Encryption-compatible controller.
3. Click Configure.

Logging into Encryption Manager
1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Click Encryption Login.
3. A new window appears. Select an account to log in with and enter the password in the field provided.

4. Click OK to continue.

Managing passwords

NOTE: Valid passwords must be 8 to 16 US-ASCII characters long and contain the following:
- At least one lowercase letter
- At least one uppercase letter
- At least one number
- At least one non-alphanumeric character, such as # or $

Set or change the Crypto Officer password

1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Log in as the Crypto Officer ("Logging into Encryption Manager" on page 37).
3. Under Accounts, locate Crypto Officer Password. Click Set/Change Crypto Officer Password.

5. Click **OK**.

### Set or change the password recovery question

1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Log in as the Crypto Officer ("Logging into Encryption Manager" on page 37).
3. Under **Accounts**, locate **Crypto Officer Password Recovery Parameters**. Click **Set/Change Password Recovery Question**.

A new window appears.

### Password Recovery Question

(What's this...?)

### Password Recovery Answer

(What's this...?)

4. Complete the following fields:
   a. **Password Recovery Question**: Enter a question to which only you know the answer.
   b. **Password Recovery Answer**: Enter the answer to the question entered above.

5. Click **OK**.

### Set or change user account password

**IMPORTANT**: If this is the first time setting the User password, you must be logged in as the Crypto Officer.
The User account is disabled by default until the Crypto Officer sets the User account password for the first time.

To set or change the User account password:
1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Log in to the Encryption Manager ("Logging into Encryption Manager" on page 37).
4. A new window appears. Enter and re-enter the new password in the New Password fields.
5. Click OK.

Set or change the controller password

A controller password causes all encrypted volumes on the controller to be kept offline at startup until the controller password is entered.

The "Set/Change Password" action enables the controller password feature and sets the initial password. After a password is set, re-executing this action replaces the existing controller password with a new one. This procedure can only be performed by the Crypto Officer. The controller password cannot be changed while the controller password feature is suspended or while the controller is locked. However, the controller password can be removed by the Crypto Officer and later reset.

To set or change the controller password:
1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Log in to Encryption Manager ("Logging into Encryption Manager" on page 37).
3. Under **Settings**, locate **Controller Password**. Click **Set/Change Controller Password**.

4. A new window appears. Enter and re-enter the new controller password in the **New Password** fields.

5. Click **OK**.

**Suspending the controller password**

If the controller password is suspended, then the controller does not prompt for a password at system startup, and volumes are allowed online if all keys are accessible. Once suspended, the controller password feature can be resumed without requiring a password reset.

To suspend the controller password:

1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Log in to Encryption Manager ("Logging into Encryption Manager" on page 37).
3. Under Settings, locate **Controller Password**. Click **Suspend Controller Password**.

4. A new window appears, asking if you want to suspend the controller password. Click **Yes** to continue.

**Resuming the controller password**

Resuming a suspended controller password re-enables password prompts at system startup.

To resume the controller password:
1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Log in to Encryption Manager ("Logging into Encryption Manager" on page 37).
3. Under **Settings**, locate **Controller Password**. Click **Resume Controller Password**.

4. A new window appears, asking if you want to resume the controller password. Click **Yes** to continue.

**Working with keys**

**Changing the Master Encryption Key**
IMPORTANT: Hewlett Packard Enterprise recommends that you keep a record of the Master Encryption Keys when encryption is configured in Local Mode. The local Master Encryption Key is not displayed by any available tool or firmware because it is considered a cryptographic secret by FIPS 140-2. Secure Encryption design follows the NIST architecture requirements and does not allow Hewlett Packard Enterprise to assist in the recovery of a lost Master Encryption Key.

To change the Master Encryption Key:
1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Log in to Encryption Manager ("Logging into Encryption Manager" on page 37).
3. Under Settings, locate Master Key. Click Change Master Key.

4. A new window appears. Enter the new Master Key in the field provided. When using Local Key Management mode, the input can be any set of printable characters. When using Remote Key Management mode, the input must be the same name as the key name in the remote key store.

5. Click OK.

Rekeying the Drive Encryption Keys

This procedure creates a new set of Drive Keys used for encrypting the volume keys on the controller. This task is available to all roles in the system.

To rekey the Drive Keys:
1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Log in to Encryption Manager ("Logging into Encryption Manager" on page 37).
3. Under Settings, locate Encrypted Physical Drive Count. Click Drive Key Rekey.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Enabled</td>
</tr>
<tr>
<td>Key Management Mode</td>
<td>Remote Key Management Mode</td>
</tr>
<tr>
<td>Master Key</td>
<td>Set</td>
</tr>
<tr>
<td>Allow New Plaintext Volumes</td>
<td>Allow</td>
</tr>
<tr>
<td>Controller Password</td>
<td>Not Set</td>
</tr>
<tr>
<td>Firmware Locked for Update</td>
<td>Unlocked</td>
</tr>
<tr>
<td>Controller Locked</td>
<td>Unlocked</td>
</tr>
<tr>
<td>Local Key Cache Enabled</td>
<td>No</td>
</tr>
<tr>
<td>Encrypted Physical Drive Count</td>
<td>5</td>
</tr>
</tbody>
</table>

4. A prompt appears, indicating new Drive Encryption Keys will be created for all physical drives. Click OK to continue.

### Rescanning keys

In Remote Mode, this procedure signals the controller to retrieve all encryption keys from the ESKM. This procedure resolves potentially locked volumes that could have been locked as a result of failure to initially retrieve the associated keys.

To rescan keys:

1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Log in to Encryption Manager ("Logging into Encryption Manager" on page 37).

4. A new window appears, indicating iLO will retrieve keys from the ESKM. Click OK to continue.

### Enabling Encryption Key Manager Authentication

When enabled, Key Manager Authentication allows the firmware to bypass prompting the user for the controller password when it is able to contact a verified key manager.

The following encryption settings must be configured before enabling Key Manager Authentication:

- Secure Encryption must be configured to run in remote key management mode.
- The controller password must be set ("Set or change the controller password" on page 40).
- Local Key Cache must be enabled, with the "number of access attempts" count set at a value greater than 0 ("Enabling/disabling local key cache" on page 58).
- The Crypto Officer or an additional user must be logged in ("Logging into Encryption Manager" on page 37).
To enable Key Manager Authentication:
1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Under Controller Password, click Enable Key Manager Authentication.

3. A new window appears. To confirm enabling Encryption Key Manager Authentication, click Yes.

**Volatile keys**

Enabling a volatile key for the logical drive prevents the encrypted data encryption key from being stored on the physical drives. In the event of a power failure or a server reboot, the controller loses the key.

For Local Key Management Mode, there is no method available to recover the data encryption key or access the data on the logical drive.

For Remote Key Management Mode, the controller must retrieve the data encryption key from the ESKM before the data on the logical drive can be accessed.

To enable, back up, and retrieve a volatile key for a logical drive, see "Enabling volatile keys in Remote Key management mode (on page 47)."

**Enabling volatile keys in Local Key Management Mode**

1. Start HPE SSA. For more information, see the HPE Smart Storage Administrator user guide.
2. Select a Secure Encryption-compatible controller.
3. Under **Controller Devices**, select **Arrays**.

4. Select a logical drive.

5. Under **Actions**, select **Encryption Volatile Key**. A new window appears.
6. Select **Enabled** or **Disabled**, and click **OK** to continue.

7. A warning window appears. Click **Yes** to continue.

8. A summary page appears, confirming that volatile keys are enabled. Click **Finish** to continue.
   A banner appears over the main menu, indicating that volatile keys are enabled for specific controllers. This banner will remain until volatile keys are disabled.

---

**Enabling volatile keys in Remote Key Management Mode**

1. Start HPE SSA. For more information, see the HPE Smart Storage Administrator user guide.
2. Select a Secure Encryption-compatible controller.
3. Under **Controller Devices**, select **Arrays**.

4. Select a logical drive.

5. Under **Actions**, select **Encryption Volatile Key**. A new window appears.
6. Select **Enabled**, and then click **OK** to continue.

![Encryption Volatile Key](image)

**Encryption Volatile Key** *(What's this...?)*

- Enabled
- Disabled

**Data Key Action** *(What's this...?)*

- Backup the Key to Remote Key Manager

7. A warning window appears. Click **Yes** to continue.
8. A summary page appears, confirming that volatile keys are enabled. Click **Finish** to continue.

A banner appears over the main menu, indicating that volatile keys are enabled for specific controllers. This banner will remain until volatile keys are disabled.
9. The keys are being backed up to the ESKM at this time. Click **Refresh** to update the **Logical Drive Details** summary listed on the right hand side of the screen. When the backup is complete, the summary will display **Yes** for **Data Key Backed Up**.

![Logical Drive Details]

- Status: OK
- Logical Drive Encryption: Encrypted
- Encryption Data Key Volatile: Yes
- Data Key Backed Up: Yes
- Drive Type: Data
- Size: 30.00 GiB (32.21 GB)
- RAID Level: RAID 1
- Legacy Disk Geometry (C/H/S): 7710 / 255 / 32
- Strip Size / Full Stripe Size: 256 KiB / 256 KiB
- Drive Unique ID: 600508B1001C85D80FB62A202E359756
- Logical Drive Label: 042E5A0P00000XRH5Y08M1663
- Disk Name: `\\PhysicalDrive2 (Disk2)`
10. To disable Data Key Backup, click Data Key Action.

11. A new window appears. Click OK to continue.

12. A summary page appears. Click Finish to continue.

Creating a plaintext volume

**IMPORTANT:** The controller only allows the creation of new plaintext volumes if it has been configured to do so by the Crypto Officer. Refer to the Encryption Manager screen to determine if plaintext volume creation is enabled on the controller.

To create a plaintext volume:

1. Start HPE SSA. For more information, see the HPE Smart Storage Administrator user guide.
2. Under **Controller Devices**, click on **Unassigned Drives**.

3. Select drives.
4. Click **Create Array**. A new window appears.

![Create Plaintext Volume](image)

5. Complete the following fields:
   a. **Create Plaintext Volume**: Select **Yes**.
   b. **My Account**: Select the account to log in with.
   c. **Password**: Enter the account password.
6. Complete remaining fields as necessary.
7. Click **Create Logical Drive**.
8. **Array Details**, **Logical Drives**, **Physical Drives** and **Device Path** specifications appear. Click **Finish** to complete.
Converting plaintext volumes into encrypted volumes

**NOTE:** In order to preserve existing data, the controller must read and rewrite the entire volume in order to complete the conversion process. Conversion may take some time to complete, especially if there is competing drive activity from the host system.

To convert plaintext volumes into encrypted volumes:

1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Log in to Encryption Manager ("Logging into Encryption Manager" on page 37).
3. Under **Controller Devices**, click **Arrays**.
4. Select the plaintext volume.
5. Under Actions, click **Convert Plaintext Data to Encrypted Data**.

![Actions](image)  

### Actions

- **Migrate RAID/Strip Size**  
  Modifies the current RAID or strip size for a logical drive. Changes the space as well as allowing for fine tuning of performance on the RAID.

- **Delete Logical Drive**  
  Deletes a logical drive. Any data contained on the logical drive will be lost. If the drive is part of an array, the array will be deleted as well.

- **Convert Plaintext Data to Encrypted Data**  
  Allows users to convert plaintext volume to encrypted volume.

A new window appears.

![Preserve Existing Data](image)  

### Preserve Existing Data (What’s this...?)

- **Yes**. Data will be preserved but conversion will take longer.
- **No**. Discard existing data.

6. Select one of the following:
   
   a. To preserve existing data, select **Yes**.
   
   b. To discard existing data, select **No**. If selected, a warning prompt appears after clicking OK, confirming your selection. Click **OK** to continue past the warning.

7. Click **OK**. A new window appears, listing the **Logical Drive Details**, **Logical Drive Acceleration Method**, and **Device Path** details.

8. Click **Finish**.

### Changing key management modes

1. Open Encryption Manager ("Opening Encryption Manager" on page 37).

2. Log in to Encryption Manager ("Logging into Encryption Manager" on page 37).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Status</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Enabled</td>
<td>Disable Encryption</td>
</tr>
<tr>
<td>Key Management Mode</td>
<td>Remote Key Management Mode</td>
<td>Change</td>
</tr>
<tr>
<td>Master Key</td>
<td>Set</td>
<td>Change Master Key</td>
</tr>
<tr>
<td>Allow New Plaintext Volumes</td>
<td>Allow</td>
<td>Disallow Plaintext Volumes</td>
</tr>
<tr>
<td>Controller Password</td>
<td>Not Set</td>
<td>Set/Change Controller Password</td>
</tr>
<tr>
<td>Firmware Locked for Update</td>
<td>Unlocked</td>
<td>Lock Firmware</td>
</tr>
<tr>
<td>Controller Locked</td>
<td>Unlocked</td>
<td></td>
</tr>
<tr>
<td>Local Key Cache Enabled</td>
<td>No</td>
<td>Set/Change Local Key Cache</td>
</tr>
<tr>
<td>Encrypted Physical Drive Count</td>
<td>5</td>
<td>Drive Key Rekey</td>
</tr>
</tbody>
</table>

4. A new window appears with the key management mode selected. Enter the Master Encryption Key in the field provided.

5. Click OK.

6. A warning appears, prompting the user to record the Master Encryption Key. Click Yes to continue.

Enabling/disabling plaintext volumes

**IMPORTANT:** Plaintext volumes are unencrypted. The option of allowing or disabling the creation of plaintext volumes depends on the following:

- The type of data to be stored on the plaintext volume
- The level of security you want or need in the system

Hewlett Packard Enterprise recommends that you do not enable this option for systems requiring high security or containing highly sensitive data.

To change plaintext volumes permissions after initial configuration:

1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Log in as the Crypto Officer ("Logging into Encryption Manager" on page 37).
3. Under **Settings**, locate **Allow New Plaintext Volumes**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Current Setting</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Enabled</td>
<td>Disable Encryption</td>
</tr>
<tr>
<td>Key Management Mode</td>
<td>Remote Key Management Mode</td>
<td>Change</td>
</tr>
<tr>
<td>Master Key</td>
<td>Set</td>
<td>Change Master Key</td>
</tr>
<tr>
<td>Allow New Plaintext Volumes</td>
<td>Allow</td>
<td>Disallow Plaintext Volumes</td>
</tr>
<tr>
<td>Controller Password</td>
<td>Not Set</td>
<td>Set/Change Controller Password</td>
</tr>
<tr>
<td>Firmware Locked for Update</td>
<td>Unlocked</td>
<td>Lock Firmware</td>
</tr>
<tr>
<td>Controller Locked</td>
<td>Unlocked</td>
<td></td>
</tr>
<tr>
<td>Local Key Cache Enabled</td>
<td>No</td>
<td>Set/Change Local Key Cache</td>
</tr>
<tr>
<td>Encrypted Physical Drive Count</td>
<td>5</td>
<td>Drive Key Rekey</td>
</tr>
</tbody>
</table>

4. Do one of the following:
   a. If encryption is disabled, click **Allow Plaintext Volumes**.
   b. If encryption is enabled, click **Disallow Plaintext Volumes**.

5. A prompt appears, asking you to confirm the change. Click **Yes** to continue.

---

**Enabling/disabling the firmware lock**

The firmware lock prevents the updating of firmware on the controller and is disabled by default. For security purposes, Hewlett Packard Enterprise recommends enabling the firmware lock function.

To change the firmware lock setting:

1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Log in to Encryption Manager ("Logging into Encryption Manager" on page 37).
3. Under **Settings**, locate **Firmware Locked for Update**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Current Setting</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Enabled</td>
<td>Disable Encryption</td>
</tr>
<tr>
<td>Key Management Mode</td>
<td>Remote Key Management Mode</td>
<td>Change</td>
</tr>
<tr>
<td>Master Key</td>
<td>Set</td>
<td>Change Master Key</td>
</tr>
<tr>
<td>Allow New Plaintext Volumes</td>
<td>Allow</td>
<td>Disallow Plaintext Volumes</td>
</tr>
<tr>
<td>Controller Password</td>
<td>Not Set</td>
<td>Set/Change Controller Password</td>
</tr>
<tr>
<td>Firmware Locked for Update</td>
<td>Unlocked</td>
<td>Lock Firmware</td>
</tr>
<tr>
<td>Controller Locked</td>
<td>Unlocked</td>
<td></td>
</tr>
<tr>
<td>Local Key Cache Enabled</td>
<td>No</td>
<td>Set/Change Local Key Cache</td>
</tr>
<tr>
<td>Encrypted Physical Drive Count</td>
<td>5</td>
<td>Drive Key Rekey</td>
</tr>
</tbody>
</table>

4. Do one of the following:
   a. If unlocked, click **Lock Firmware**.
   b. If locked, click **Unlock Firmware**.

5. A prompt appears, asking you to confirm the change. Click **Yes** to proceed.
Enabling/disabling local key cache

Local Key Cache enables the user to store the keys required to decrypt the volume keys in persistent memory on the controller. When configured for Remote Key Management Mode, the controller normally retrieves the keys from the ESKM at boot time. By storing the key values in the controller, logical drive data can be encrypted and decrypted without the network presence of the ESKM.

1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Log in to Encryption Manager ("Logging into Encryption Manager" on page 37).
3. Under Settings, locate Local Key Cache Enabled. Click Set/Change Local Key Cache.

4. Do one of the following:
   - To disable, select No.
   - To enable, select Yes. If you select Yes, two new fields appear.

   **Enable Local Key Cache (What's this...?)**

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

   **Number of Access Attempts Before Deleting Local Key Cache**

   | 0   | Valid Range: 0 (No retry) - 10 attempts |

   **Retry Interval in Minutes (What's this...?)**

   | 1   | Valid Range: 1 - 15 minutes |

5. Complete the following fields:

   **IMPORTANT:** Hewlett Packard Enterprise recommends using the default settings for the number of access attempts. Only change this value if there is a concern that an unintended individual might remove the server from the environment. When the value is set to a value higher than "0", HPE Secure Encryption attempts to locate ESKM the configured number of times during boot. If all attempts fail, the local key cache is deleted prior to boot. All volumes encrypted will remain locked until the ESKM is reached and the required keys are retrieved and placed back into the local key cache.
Number of Access Attempts Before Deleting Local Key Cache - A value of "0" indicates HPE Secure Encryption will not check for the presence of a key manager, and the key cache will remain present on the controller. If the value is greater than "0", HPE Secure Encryption will attempt to contact the key manager the number of attempts specified. If any attempt is successful, the encrypted logical drive(s) will be unlocked using the keys in the local key cache. If all of the attempts are unsuccessful, then all of the encrypted logical drive(s) will remain locked and the keys in the local key cache are deleted.

Retry Interval in Minutes - The number of minutes between access attempts.

Click OK.

Importing drive sets in Local Key Management Mode

When the Master Encryption Key on an imported drive set is different from the Master Encryption Key on the receiving Smart Array Controller, the importing volumes remain offline until user intervention is taken. HPE SSA can be used to supply the Master Key name for the importing drives.

In Remote Key Management Mode, drives automatically import when the associated key is present on the ESKM. If keys are unable to be retrieved but are confirmed to be on the ESKM, it is possible they are assigned to a different group.

Importing drives with different Master Keys

Migrating drives to a non-encrypted controller results in the logical volumes associated with those drives remaining offline until encryption is enabled with the proper Master Encryption Key settings and mode for that volume.

If non-encrypted drives are migrated to an encrypting controller, the controller automatically brings the logical volumes associated with those physical drives online and makes them available for use.

To import drives with a different Master Key into a controller when using Local Key Management Mode:

1. Power down the server. For more information, see the documentation that ships with the server.
2. Attach drives. For more information, see the documentation that ships with the drives.
3. Power up the server. For more information, see the documentation that ships with the server.
4. Start HPE SSA. For more information, see the HPE Smart Storage Administrator user guide.
5. Under Array Controller(s), click the controller assigned to the new drives. Red alert message indicators will appear next to it.
6. Under Actions, click Configure.
7. From the side menu, click Encryption Manager.
8. Log in to Encryption Manager ("Logging into Encryption Manager" on page 37).
9. Under **Utilities**, click **Import Foreign Local Key**.

10. A new screen appears. Enter the new Master Encryption Key name assigned to the drives being imported in the **Master Key** field.

11. Click **OK**.

The drives will be incorporated, unlocked, and assigned the Master Encryption Key of the receiving controller.
Maintenance

Controllers

Clearing the controller

To clear all logical drives and arrays on controllers:
1. Start HPE SSA. For more information, see the HPE Smart Storage Administrator user guide.
2. Select the controller to be cleared.
4. A new window appears, confirming your request to clear the controller's configuration. To continue, click Clear.
5. A new window appears, displaying controller settings and configuration. To continue, click Finish.

Replacing an encrypted controller

If some or all of the drives managed by the controller being replaced are encrypted, you must re-configure the replacement controller with the same settings and key management mode you used for the controller you are replacing. For more information, see the documentation that ships with the controller.

In Local Key Management Mode, you must provide the correct Master Encryption Key name that matches the one used for the attached drives.

In Remote Key Management Mode, any valid Master Encryption Key name will work, since the Master Encryption Key names are part of the drive configuration information stored on each drive.

Replacing a server while retaining the controller

If you retain the same controller and physical disks, then there are no encryption-related tasks to complete.

If Remote Key Management Mode is in use, the previous iLO configuration for key management must be applied to the new server.

For more information on configuring iLO, see "Configuring iLO (on page 31)."

For more information on locating the group name, see "Locating groups associated with a drive (on page 62)."

Preconfiguring replacement components

It is possible to configure replacement controllers ahead of time for encryption. After installing the Smart Array Controller, enable encryption on the controller. For more information, see "Configuration (on page 13)."

After the server is powered down, the controller can be physically removed and set aside for later use.
Flashing firmware

If the firmware lock function is enabled, the firmware lock on the controller must be unlocked before attempting to flash the controller. To disable the firmware lock function, see "Enabling/disabling the firmware lock (on page 57)."

Drives

Replacing a physical drive

No Secure Encryption-related steps are associated with this procedure. To replace a drive, see the server maintenance and service guide.

Groups

Locating groups associated with a drive

Use one of the following methods to locate the group name associated with a drive.

- Query by drive serial number (on page 62)
- Query by previous server name (on page 65)

Query by drive serial number

1. Log in to the ESKM ("Logging in to the ESKM" on page 17).
2. Click the Security tab.

The following screen appears.

4. Click Add.
The following screen appears.

5. Complete the following fields:
   a. Query Name
   b. Query Type
   c. Description

6. Click Next.
   The Key Policy and Configuration screen appears.

7. If you want to save this query, enter a name in the Query Name field.

8. Under Choose Keys Where, do the following:
   a. Field 1: Select Key Name from the drop down menu.
   b. Field 2: Select Contains from the drop down menu.
c. Field 3: Enter the serial number of one of the drives in the server.

9. If you assigned a name to this query, click **Save and Run Query**. Otherwise, click **Run Query without Saving**.

10. Click on the key. A new screen appears, listing the **Key Properties**.

11. Click **Permissions** to view the group name.

---

**Query by previous server name**

1. Log in to the ESKM ("Logging in to the ESKM" on page 17).
2. Click the **Security** tab.

3. Under **Keys**, click **Query Keys**.
The following screen appears.

4. Click **Add**.
   The following screen appears.

```
Security > Keys > Query Keys

Key and Policy Configuration

Saved Queries

<table>
<thead>
<tr>
<th>Query Name</th>
<th>Query Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[All ESKM Keys]</td>
<td>ESKM</td>
<td>Built-in query that displays all ESKM keys.</td>
</tr>
<tr>
<td>[All KMIP Keys]</td>
<td>KMIP</td>
<td>Built-in query that displays all KMIP keys.</td>
</tr>
<tr>
<td>[All]</td>
<td>All</td>
<td>Built-in query that displays all ESKM and KMIP keys.</td>
</tr>
</tbody>
</table>

Add  Modify  Delete  Copy  Run
```

5. Complete the following fields:
   a. Query Name
   b. Query Type
   c. Description

6. Click **Next**.
The **Key Policy and Configuration** screen appears.

7. If you want to save this query, enter a name in the **Query Name** field.

8. Under **Choose Keys Where**, do the following:
   a. Field 1: Select **Custom: Server_Name** from the drop down menu.
   b. Field 2: Select **Equals** from the drop down menu.
   c. Field 3: Enter the previous server name associated with the drive.

9. If you assigned a name to this query, click **Save and Run Query**. Otherwise, click **Run Query without Saving**.
10. Click on the key. A new screen appears, listing the **Key Properties**.
11. Click the Permissions tab to view the group name.

Displaying log information

The event log displays events for all controllers in the system and does not differentiate between events produced by different controllers.

When operating Secure Encryption in Remote Mode, you can access the ESKM events log for information on key retrieval and exchange, including the following:

- Connection status
- Master Encryption Key retrieval
- Drive Key retrieval
- Drive Key save requests
- Drive Key deletion

To view the event log:
1. Log in to iLO using your server's credentials.
2. From the left side panel, expand the **Administration** menu.

<table>
<thead>
<tr>
<th>Expand All</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶ Information</td>
</tr>
<tr>
<td>▶ iLO Federation</td>
</tr>
<tr>
<td>▶ Remote Console</td>
</tr>
<tr>
<td>▶ Virtual Media</td>
</tr>
<tr>
<td>▶ Power Management</td>
</tr>
<tr>
<td>▶ Network</td>
</tr>
<tr>
<td>▶ Remote Support</td>
</tr>
<tr>
<td>▶ Administration</td>
</tr>
<tr>
<td>‣ Firmware</td>
</tr>
<tr>
<td>‣ Licensing</td>
</tr>
<tr>
<td>‣ User Administration</td>
</tr>
<tr>
<td>‣ Access Settings</td>
</tr>
<tr>
<td>‣ Security</td>
</tr>
<tr>
<td>‣ Management</td>
</tr>
<tr>
<td><strong>Key Manager</strong></td>
</tr>
<tr>
<td>‣ iLO Federation</td>
</tr>
</tbody>
</table>
3. Click **Key Manager**. The **Enterprise Secure Key Manager Events** appears at the bottom of the screen.

Navigating away from the page and returning or clicking **Test ESKM Connections** refreshes the list of events.

**Running queries**

To run a query:
1. Log in to the ESKM ("Logging in to the ESKM" on page 17).
2. Click the **Security** tab.
3. From the left side panel, expand the **Keys** menu and click **Query Keys**.

A new screen appears.

4. Under **Create Query**, complete the following:
   a. If you want to save the query for future use, fill in the following fields:
      - **Query Name**
      - **Description**
b. In the **Choose Keys Where** field, structure queries that combine any or all of the following criteria:

- Key Name
- Owner
- Group Name
- Algorithm
- Creation Date
- Latest Key Version Date
- Any Key Version Date
- Versioned Key
- Not Versioned Key
- Exportable
- Not Exportable
- Deletable
- Not Deletable
- Access Time
- Controller identification criteria
- Custom criteria

c. Structure the report by displaying the following columns:

- Key Name
- Owner
- Exportable
- Deletable
- Algorithm
- Creation Date
- Versioned Key
- Custom attributes

d. When you have finished structuring the query, click one of the following buttons:

- **Save and Run Query**
- **Save Query**
- **Run Query without saving**

The report appears with the selected criteria.
Troubleshooting

Common issues

Lost or forgotten Crypto Officer password

1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Under Accounts, locate Crypto Officer Password. Click Recover Crypto Officer Password.

A new window appears.

3. Do the following:
   a. Answer the security question in the Password Recovery Answer field.
   b. Enter and then re-enter a new password in the New Password fields.
4. Click OK.

Lost or forgotten controller password

The controller password is used to protect data in the event of a storage system theft. Once enabled, the controller will not unlock encrypted volumes until the correct controller password has been provided. If the controller password is lost or forgotten, the controller will remain locked and all encrypted volumes will be offline and inaccessible.

If the OS logical drive is encrypted, offline HPE SSA will be required to perform the steps below. For more information, see the HPE Smart Storage Administrator user guide.
To clear the controller password:

1. Open Encryption Manager ("Opening Encryption Manager" on page 37).
2. Log in as the Crypto Officer ("Logging into Encryption Manager" on page 37).
3. Under **Settings**, locate **Controller Password**. Click **Remove Controller Password**.

4. A window appears, asking you to confirm that you want to remove the controller password. Click **Yes**.
5. Click on **Change Master Key** and enter the Master Encryption Key used for encryption. For more information, see "Changing the Master Encryption Key (on page 42)."
6. Enable Secure Encryption, then reboot the server.

Volumes appear online and are available.

**Lost or forgotten Master Key**

⚠ **CAUTION:** Hewlett Packard Enterprise strongly recommends storing a backup of the Master Encryption Key in a secure location. In some instances it is possible that a missing key will render your data inaccessible. If operating Secure Encryption in Remote Key Management Mode, Hewlett Packard Enterprise strongly recommends that you back up the ESKM regularly.

**Local mode**

If operating Secure Encryption in Local Mode, securing the Master Encryption Key value is critical to accessing the encrypted logical drive data. If the controller requires replacement or if the physical drives are moved to another controller, a matching Master Key is required to gain access to the data. Master Keys are not recoverable if lost. If the Master Key is lost or forgotten, you must perform a data restore operation from the backup media to regain access to the data.

**Remote mode**

Locating the key using the ESKM

To locate a lost or forgotten Master Encryption Key using the ESKM:

1. Log in to the ESKM ("Logging in to the ESKM" on page 17).
2. Click the **Security** tab.

3. From the left side panel, expand the **Keys** menu and click **Keys**.

4. The **Key and Policy Configuration page** displays a list of all keys. Scroll through the list to locate the Master Key.

5. If you remember specific attributes about the Master Key, run a key query ("Running queries" on page 72).

If you cannot locate the Master Key name, it may have been accidentally deleted from the ESKM. You may be able to locate the key by using an ESKM backup.

**Locating the key using iLO**

iLO utilizes an event log listing recent key activity. If the lost or forgotten key was recently modified, it might appear in the event log.

To locate a lost or forgotten Master Encryption Key using iLO:

1. Log in to iLO using your server’s credentials.
2. From the left side panel, expand the **Administration** menu.
3. Click **Key Manager**. The **Enterprise Secure Key Manager Events** appears at the bottom of the screen. Review the event log for the missing key.

Forgotten which Master key goes with which drive

Recovery of the Master Encryption Key name corresponding to a specific set of drives is possible when operating Secure Encryption in Remote Key Management Mode.

To recover the Master Encryption Key name:

1. Log in to the ESKM ("Logging in to the ESKM" on page 17).
2. Run a key query with the following search parameters ("Running queries" on page 72):
   a. **Choose Keys Where** drop down menu: select **Custom: Server_Name**. Two new fields appear.
   b. In the second drop down menu, select **Equals**.
   c. In the third field, enter the name of the server to be associated with the Master Encryption Key.
   d. Under **Custom Attributes**, select **Master_Key**.

Logical drives remain offline

If cryptographic information is missing, logical drives remain offline after system start. General causes include a missing, incorrect, or inaccessible key. Restoring the cryptographic information to match the attached drives results in the appropriate access to the logical drive.

Possible causes

- Encryption is not enabled.
- The matching Master Encryption Key is missing or incorrect.
- The controller password was enabled but is not entered or is incorrect.

Possible causes (Remote Mode only)

- Network connectivity issues are occurring between iLO and the ESKM.
- iLO is not configured properly.
- The Drive Keys are missing from the ESKM.
• The Drive Encryption Keys and iLO groups are mismatched.
   To view a diagnostic report, see the HPE Smart Storage Administrator user guide.

Master key not exporting

This issue occurs only in Remote Key Management Mode. The problem appears as either a locked controller or as locked volumes.

Possible causes

• A network problem prevents key retrieval from the ESKM.
• Lost or incorrect iLO configuration
• Missing or incorrectly configured Master Encryption Key

Possible Resolutions

• Troubleshoot the network connection between iLO and the ESKM. For more information, see "Testing the connection between iLO and the ESKM (on page 80)."
• Ensure the Master Encryption Key exists. For more information, see "Locate the key using the ESKM ("Locating the key using the ESKM" on page 76)."
• Ensure the Master Encryption Key is in the correct group. If the Master Encryption Key is incorrectly assigned, see "Placing a key in a group (on page 26)."

Testing the connection between iLO and the ESKM

iLO connects and manages key exchanges between the controller and ESKM. If you suspect iLO has lost its connection to the ESKM, you can test the connection in iLO.

To test the connection between iLO and the ESKM:
1. Log into iLO using your server's credentials.
2. From the left side panel, expand the **Administration** menu and then click **Key Manager**.
The following screen appears.

### Enterprise Secure Key Manager

**Key Manager Servers**

- **Primary Key Server**
  - Address
  - Port
- **Secondary Key Server**
  - Address
  - Port
- **Require Redundancy**
  - Apply

**Key Manager Configuration**

- **iLO Account on ESKM**
  - Name: iio-1402ec485bee
  - Group
- **ESKM Local CA Certificate Name**
  - This is the name of the Local CA in ESKM that is used to sign the ESKM server certificate. iLO will retrieve this certificate from the ESKM server.
- **Imported Certificate Details**
  - Issuer: Not Present
  - Subject: Not Present
- **ESKM Administrator Account**
  - Login Name
  - Password
  - Update ESKM

#### Test ESKM Connections

3. **Under Key Manager Configuration**, click Test ESKM Connections:
   - If iLO is connected to the ESKM, a green checkmark appears indicating the key managers are accessible.
   - If the connection has been lost, you will need to re-configure iLO to communicate with the ESKM. For more information, see "Connecting iLO to ESKM" on page 31."

### Potential errors encountered

The following table describes errors that might be encountered when configuring or operating Secure Encryption.
<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote key manager communication failure</td>
<td>Slot X Encryption Failure – Communication issue prevents drive keys from being retrieved. Encrypted logical drives are offline. System may not boot.</td>
<td>To troubleshoot, see the Key Manager page in iLO interface.</td>
</tr>
<tr>
<td>Incorrect or missing Master Key on Remote key manager</td>
<td>Slot X Encryption Failure – Master Encryption Key is incorrect or not retrieved from ESKM. Encrypted logical drives may be offline. System may not boot.</td>
<td>Correct the problem on the ESKM.</td>
</tr>
<tr>
<td>Volume Key decryption failure</td>
<td>Invalid Drive Encryption Keys on ESKM. Encrypted logical drives may be offline. System may not boot.</td>
<td>Restore the correct version of the Drive Encryption Key on the ESKM.</td>
</tr>
<tr>
<td>Unable to establish communication with controller</td>
<td>Communication issue prevents keys from being retrieved. Dependent encrypted logical drives are offline. System may not boot.</td>
<td>Reset the controller by rebooting the server.</td>
</tr>
<tr>
<td>Missing local Master Key</td>
<td>Imported encrypted logical drives are offline; the matching local Master Encryption Key is required. System may not boot.</td>
<td>Use HPE Smart Storage Administrator to enter the local Master Encryption Key.</td>
</tr>
<tr>
<td>Controller password failure</td>
<td>All encrypted local drives are offline due to failure to enter proper controller password.</td>
<td>Reboot the server and enter the proper controller password, or unlock the controller using HPE Smart Storage Administrator.</td>
</tr>
<tr>
<td>Controller encryption not enabled</td>
<td>Encrypted logical drives are present but encryption is not yet enabled. Encrypted logical drives are offline.</td>
<td>Use HPE Smart Storage Administrator to enable encryption.</td>
</tr>
<tr>
<td>Encryption parameters not set</td>
<td>Encryption is enabled for the controller but the Master Encryption Key name is not set.</td>
<td>Use Encryption Manager to set the Master Key name for the controller and reboot.</td>
</tr>
<tr>
<td>Controller/logical drive encryption type mismatch</td>
<td>Key management mode mismatch between controller and drives. Dependent encrypted drives offline.</td>
<td>Use Encryption Manager to match key management modes. For more information, see &quot;Importing drives with different Master Keys (on page 59)&quot;.</td>
</tr>
<tr>
<td>Encryption failure - unsupported system ROM detected</td>
<td>Unsupported system ROM detected. Encrypted logical drives may be offline. System may not boot.</td>
<td>Update the system ROM to a version supporting encryption.</td>
</tr>
<tr>
<td>Encrypted logical drives on non-encrypting controller</td>
<td>Encrypted logical drives are offline. Encryption feature is not available on this controller.</td>
<td>Move drives to a controller with encryption support or delete the logical drives.</td>
</tr>
<tr>
<td>Encryption failure - unsupported iLO firmware detected</td>
<td>Unsupported iLO firmware detected. Encrypted drive may be offline. System may not boot.</td>
<td>Update iLO firmware to a version supporting encryption.</td>
</tr>
<tr>
<td>NVRAM failure</td>
<td>Non-volatile storage corrupted. Critical Security Parameters erased per policy. Encrypted drives are offline.</td>
<td>Use HPE Smart Storage Administrator to reestablish CSPs.</td>
</tr>
<tr>
<td>Encryption engine self-test failure</td>
<td>Encryption engine hardware failure. Encrypted logical drives are offline until the problem is corrected.</td>
<td>Replace the controller to bring encrypted drives online.</td>
</tr>
</tbody>
</table>
## Troubleshooting 84

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to create a plaintext volume</td>
<td>While logged into the system, you are unable to create a plaintext volume.</td>
<td>Verify that Encryption Manager has been set to allow the creation of future plaintext volumes.</td>
</tr>
</tbody>
</table>

### Clearing the encryption configuration

**IMPORTANT:** Clearing all encryption settings clears all secrets, keys, and passwords from the controller. Secure Encryption will be returned to a factory-new state.

To clear all encryption settings:

1. Clear the controller ("Clearing the controller" on page 61).

**IMPORTANT:** Clearing the controller is not necessary if there are no encrypted drives present or if HPE Smart Storage Administrator is operating in an offline mode.

2. Log in to Encryption Manager ("Logging into Encryption Manager" on page 37).

3. Under **Utilities**, click **Clear Encryption Configuration**.

4. A prompt appears, indicating all encryption settings will be cleared from the controller. To continue, click **Clear**.
Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website (http://www.hpe.com/assistance).
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website (http://www.hpe.com/support/hpesc).

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center Get connected with updates page (http://www.hpe.com/support/e-updates)
  - Software Depot website (http://www.hpe.com/support/softwaredepot)

**IMPORTANT:** Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

- Hewlett Packard Enterprise Information Library (http://www.hpe.com/info/enterprise/docs)
- Hewlett Packard Enterprise Support Center (http://www.hpe.com/support/hpesc)
- Contact Hewlett Packard Enterprise Worldwide (http://www.hpe.com/assistance)
Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product’s service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the Insight Remote Support website (http://www.hpe.com/info/insightremotesupport/docs).
Appendix

Encryption algorithms

In keeping with the encryption standards outlined in FIPS 140-2 (http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf), controllers utilizing Secure Encryption are designed to meet FIPS-140-2 Level 2 requirements by implementing both physical security and cryptographic methods in protecting data-at-rest. Specifically, Secure Encryption satisfies the cryptographic requirements established in FIPS 140-2 by using NIST-approved algorithms in protecting both data and encryption keys. For more information, see the Cryptographic Algorithm Validation Program website (http://csrc.nist.gov/groups/STM/cavp/standards.html).

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XTS-AES 256-bit</td>
<td>The XTS algorithm is used to encrypt data on the drive platter as described in NIST special publication SP 800-38E.</td>
</tr>
<tr>
<td>AES-ECB</td>
<td>The AES algorithm is used to perform symmetric key encryption.</td>
</tr>
<tr>
<td>SHA-256</td>
<td>The SHA secure hashing algorithms are described in FIPS 180-4.</td>
</tr>
<tr>
<td>HMAC</td>
<td>The HMAC algorithm is described in the FIPS 198-1 standard.</td>
</tr>
<tr>
<td>PBKDF2</td>
<td>The PBKDF2 algorithm derives cryptographic keying material from user-provided passwords. The algorithm is described in NIST special publication SP 800-132.</td>
</tr>
<tr>
<td>DRBG</td>
<td>An implementation of the SP800-90A algorithm is used to produce random bit sequences.</td>
</tr>
</tbody>
</table>
ACU
Array Configuration Utility

Controller key
A key created by the controller and permanently saved to the Remote Key Manager after being wrapped by the Master Encryption Key. This key is used on a temporary basis to alleviate potential bottlenecks to the Remote Key Manager during volume creation/change events. Use of a Controller Key is on a temporary basis only and is ultimately transitioned via a rekey operation to the appropriate Drive Encryption Key.

Controller-secured region
The section of a device where data and Critical Security Parameters can exist in an unencrypted format. This boundary must be secured against tampering as acquiring this sensitive data may result in unauthorized access to data.

Critical Security Parameters (CSPs)
An industry standard term referring to security related information such as keys, passwords, and so forth, whose disclosure would compromise an encrypted system.

Crypto officer
Personnel who have permission to access the full range of encryption functions available on the controller. This includes turning encryption on and off, resetting keys, importing Master Encryption Keys, and so forth.

Drive array
The group of physical drives containing a logical volume.

Drive encryption key
Key generated by the Smart Array controller for each physical drive that contains at least one encrypted logical drive. The Drive Encryption Key for each physical drive is used to encrypt (wrap) the Volume Encryption Keys for all of the logical drives resident on that physical drive.

Drive key caching
In Remote mode, the Drive Encryption Keys are typically stored on the Remote Key Manager. However, it is possible to enable the controller to cache all of these Drive Encryption Keys necessary to decrypt attached logical drives within the controller-secured region. This option is available to the user through HPE SSA.

Encrypted data
Data that has been encrypted through the use of an encryption key.

ESKM
Enterprise Secure Key Manager
FIPS
Federal Information Processing Standard

HIPAA
Health Insurance Portability and Accountability Act

HITECH
Health Information Technology for Economic and Clinical Health

HPE SSA
HPE Smart Storage Administrator

iLO 4
Integrated Lights-Out 4

Local Master Encryption Key
The equivalent of a Master Encryption Key in Local mode. The Local Master Encryption Key name is stored in non-volatile memory within the controller-secured region and used to generate a Local Master Encryption Key for wrapping the Drive Encryption Keys.

Master Encryption Key
A two-part key established on the Remote Key Manager. This key consists of both a name and a value. The name consists of a maximum of 64 characters and is used to uniquely identify this key to all controllers within a given Security Domain. The Master Encryption Key value is a 256-bit quantity used by controllers to wrap Drive Encryption and Controller Keys for secure storage on the controller and import into the Remote Key Manager.

NIST
National Institute of Standards and Technology

NVRAM
nonvolatile memory

PCI-DSS
Payment Card Industry Data Security Standard

Plaintext
Data in unencrypted form.

Remote Key Manager
A server used to store, backup and retrieve keys for a group of controllers in a data center.

Volume encryption key
The key used in conjunction with hardware-based algorithms to perform the encryption of data resident on logical volumes.
Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (mailto:docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.
Index

A
access 37
algorithms, supported 87

B
backing up data 11
before you contact Hewlett Packard Enterprise 85

C
common problems 75
components 6
configuration 5, 11, 13, 17, 31
configuration overview 17
configuration, troubleshooting 84
configuring the ESKM 17
contacting Hewlett Packard Enterprise 85
controller 7, 10, 34, 42, 61, 75, 80
controller configuration 15, 34, 61
controller, replacing 61
crypto officer 38, 75

D
deployment scenarios 12
drive 59, 62, 79
drives, removing 62

E
crypt 7, 11, 87
error messages 82
errors 75, 82
ESKM 9, 10, 12, 17, 19, 21, 24, 26, 59, 62, 72, 76, 79, 80
ESKM, configuring 17, 31

F
factory defaults, resetting 84
features, overview 7
features, standard 7
firmware 57, 62
firmware lock 57
firmware update 57

G
groups 12, 19, 21, 26, 59, 62
groups, adding 19
groups, managing 21, 29, 62
GUI tasks 37
GUI, accessing 37

H
Hewlett Packard Enterprise website 85
Hewlett Packard Enterprise, contacting 85
HPE Smart Storage Administrator (HPE SSA) 6
HPE SSA (HPE Smart Storage Administrator) 6

I
iLO (Integrated Lights-Out) 9, 31
implementation 11
importing drives 59

K
key manager 9, 10, 17, 62, 72, 76, 80
Key Manager Authentication 44
keys 24, 26, 29, 42, 76
keys, creating 24, 42
keys, deleting 42
keys, managing 42, 43, 44, 76, 79, 80

L
license 10
license, iLO 10
Local Key Management Mode 13, 15, 76
logging in 17
logical drive 79
logical drive, troubleshooting 79

M
maintenance 61
Master key 24, 26, 29, 42, 59, 79, 80
minimum requirements 6, 12

O
operations 37
overview 5

P
password recovery, administrator 39, 75
password, changing 38, 39
passwords 38, 39, 42, 75
phone numbers 85
plaintext volume 51, 54, 56
preconfiguring replacement components  61
preparation procedures       37
product overview      5

Q
queries, executing  26, 62, 65, 72, 76, 79

R
Remote Key Management Mode  34, 76
replacement components, preconfiguring  61
replacing the controller  61

S
security domain  12
security settings  11
server, replacing  61
settings  11
settings, password  11
setup  11
Smart Array  10
Smart Array options  10
SmartCache  9
support and other resources  85
supported servers  75

T
technical support  85
telephone numbers  85
troubleshooting  75

U
user account, adding  17
user account, modifying  21, 38, 39

V
volatile keys  45, 47
volume  51, 54, 56

W
website, HPE  85