

Remote Key Management Server Configuration for Drive Encryption

Contents

Document revision history	3
Enterprise Security Key Manager	4
Features of ESKM.....	4
ESKM and HPE Servers	4
Supported Key Managers	5
Supported Storage Controllers	5
Configuring HPE iLO 6 Remote Key Management Server Using CTM	5
Procedure	5
Creating a user	5
Creating a group.....	6
Assigning users to group and assigning privileges to a user	7
Configuration of Master Key.....	8
Configure the Remote Key Manager Server	9
Configuring HPE iLO 6 Remote Key Management Server Using Utimaco	16
Procedure	16
Configuration of user and Group for Utimaco	16
Configure the Remote Key Manager Server	16
Create Logical drives and verify for encrypted state	18
HPE iLO 7 Remote Key Management Server for Drive Encryption.....	19
Procedure for Drive Encryption.....	19
Procedure for Drive Decryption	21

Document revision history

Project name: iLO

Document status: Final

Document version	Date	Prepared / Modified by	Reviewed by	Approved by	Section and text revised
1	27/10/2025	Kamal Joshi			Initial version

Enterprise Security Key Manager

Enterprise Security Key Manager (ESKM) manages and safeguards encryption keys across environments. It integrates with HPE servers to provide comprehensive key management and encryption services.

Features of ESKM

- Provides centralized control over encryption key lifecycle management
- Ensures that sensitive data is protected and comply with security regulations
- Ensuring integration with various applications and services
- Enables enforcement of encryption policies and audit key usage
- Ensures streamlining of key management processes

ESKM and HPE Servers

- This section describes the benefits of ESKM within an HPE server environment.
- Centralized key management: ESKM acts as a centralized repository for encryption keys allowing HPE servers to retrieve and manage keys from a single source. This centralization simplifies key management and ensures consistent application of encryption policies across the server infrastructure.
- Integration with HPE security features: ESKM integrates with HPE's built-in security features, such as HPE's Trusted Platform Module (TPM), HPE StoreOnce, and enhances data protection. The integration ensures the encryption keys used by the security features are securely managed and rotated as per the standards.
- Secure key storage and retrieval: ESKM securely stores encryption keys and provides a secure mechanism for HPE servers to retrieve the keys when needed. This ensures that sensitive data processed or stored on HPE servers is always encrypted with the required keys.
- Key lifecycle management: ESKM manages the entire lifecycle of encryption keys, including creation, distribution, rotation, and retirement. This lifecycle management is crucial for maintaining the security and integrity of encrypted data on HPE servers.
- Compliance and auditing: ESKM provides detailed auditing capabilities that track key usage and access. This helps organizations using HPE servers to comply with regulatory requirements and internal security policies by offering transparent reporting and monitoring.
- Seamless integration: ESKM integrates with HPE server management tools and APIs which allows automated key management and simplified configuration. This integration helps streamline operations and ensures that the encryption key management is aligned with the server's overall security strategy.
- By leveraging ESKM with HPE servers, organizations can enhance their data security posture, ensure effective key management, and maintain compliance with security standards and regulations.

Supported Key Managers

HPE iLO supports the following key managers:

- Utimaco Enterprise Secure Key Manager (ESKM) 8.53 and later
- Thales CipherTrust Manager 2.2.0, K170v (virtual) and K570 (physical) appliances
- Thales TCT KeySecure for Government G350v (previously known as SafeNet AT KeySecure G350v 8.6.0)
- Thales KeySecure K150v (previously known as SafeNet KeySecure 150v 8.12.0)

Note: If iLO is in CNSA security mode, key manager is not supported for Utimaco.

Supported Storage Controllers

- HPE SR932i-p Controller
- HPE NS204i-u SED Boot Device
- HPE MR416i-p and HPE MR416i-o Controller
- Intel® VROC (Supports only Remote Key Management)

Configuring HPE iLO 6 Remote Key Management Server Using CTM

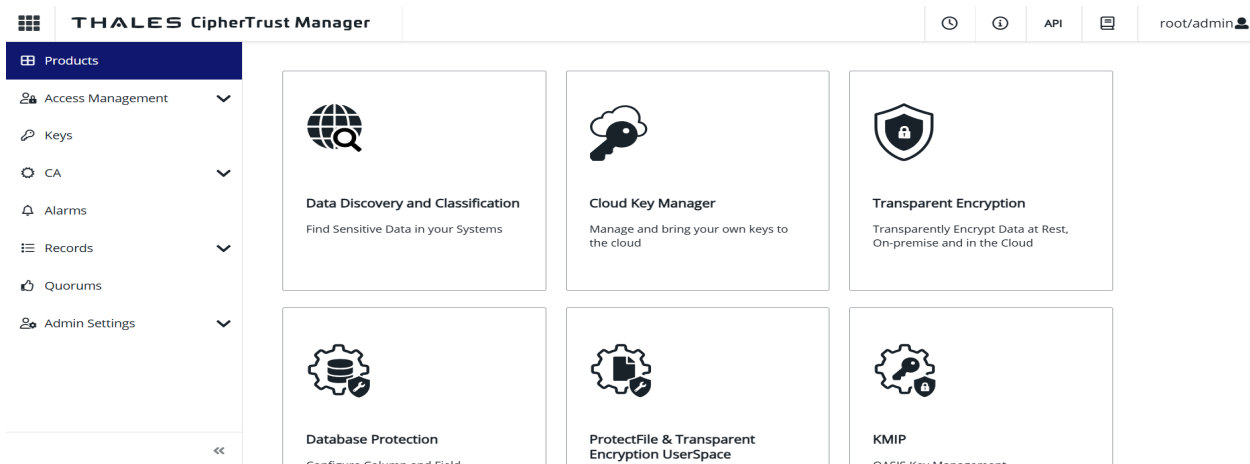
Hewlett Packard Enterprise recommends using CTM version 2.19.0 or later. Before configuring HPE iLO 6 Remote Key Management Server using CTM, the following steps must be completed:

Procedure

1. [Creating a user](#)
2. [Creating a group](#)
3. [Assigning user to group and assigning privileges to a user](#)

Creating a user

1. Click Access Management in the navigation tree



2. Click Users. The Users page appears
3. Click Add User

The screenshot shows the THALES CipherTrust Manager interface. The top navigation bar includes the product name and user information (root/admin). The left sidebar shows the 'Access Management' menu with 'Users' selected. The main area is titled 'Users' and contains a search bar and an 'Add User' button. Below this is a table of users:

Username	Full Name	Email	Source	Created	Updated	ID	Last
admin	admin	admin@local	local	Monday, August 18th 2025, 1:40:42 pm	Wednesday, September 3rd 2025, 3:13:47 pm	local 37cc7ab8-b7f7-40ct	We Sep 20, 2025

4. Enter username and Password

The 'Add User' form contains the following fields and options:

- Connection Type:** Radio buttons for Local Account (selected), OIDC, and LDAP.
- Allowed Client Type:** Checkboxes for Unregistered, Public, and Confidential (all checked).
- Full Name:** Text input field with placeholder 'name'.
- Username:** Text input field with placeholder 'username'.
- Email:** Text input field with placeholder 'email'.
- Password Policy:** Dropdown menu with 'Global' selected.
- Password:** Text input field with placeholder 'password'.
- Password Match:** Text input field with placeholder 'passwordMatch'.
- Validation Rules:**
 - Length is between 8 and 30 characters
 - Has at least 1 uppercase(s)
 - Has at least 1 lowercase(s)
 - Has at least 1 number(s)
 - Has at least 1 special character(s)
- Account Settings:**
 - Require user to reset password on next login
 - Set Account Expiration Date
 - Allow user to login using CipherTrust web app
 - Allow user to login using password
 - Allow user to login using certificate
 - Require user to login using Two-Factor Authentication

Creating a group

1. Click Access Management > Groups in the navigation tree. The Groups page appears.
2. Click Create New Group
3. Click Add Group

THALES CipherTrust Manager

Products

- Access Management
 - Users
 - Groups
 - Client Hub
 - Client Profiles
 - Connections
 - LDAP
 - OpenID Connect
 - Registration Tokens
- Keys
- CA
- Alarms
- Records
- Quorums
- Admin Settings

Groups

Name Search + Create New Group

Name	Defined By	No. of members	Description
admin	System	1	
All Clients	System		
Application Data Protection Admins	System		
Application Data Protection Clients	System		
Audit Admins	System		
Aug28	User		
Backup Admins	System		
CA Admins	System		

Create New Group

1 General Info 2 Assign Members 3 Review

Please Review
Before adding the group, review all details. Once the group is added, certain features will no longer be editable.

GENERAL INFO [Edit](#)

Name

Description

ASSIGN MEMBERS [Edit](#)

Name	User ID
<input type="text" value="ilo-5ced8c317400"/>	<input type="text" value="local fc923d55-561b-441d-8796-ae522542c672"/>

Back **Add Group**

Assigning users to group and assigning privileges to a user

1. Click Access Management > Groups in the navigation tree. The Groups page appears
2. Click Add Member
3. Enter Group Membership details. Use the Search Members option to search and add the following require three groups
 - CA Admins
 - Key Users
 - User Admins

THALES CipherTrust Manager root/admin

Products

- Access Management
- Users
- Groups
- Client Hub
- Client Profiles
- Connections
- LDAP
- OpenID Connect
- Registration Tokens
- Keys
- CA
- Alarms
- Records
- Quorums
- Admin Settings

< Groups

test_group

No. of members: 1 Description: _____

[Expand All](#)

GENERAL INFO +

MEMBERS -

Search members

1 Result | 1 Member [+ Add Member](#)

Name	User ID	
ilo-5ced8c317400	local fc923d55-561b-441d-8796-ae522542c672	...

1 Member 10 per page

THALES CipherTrust Manager root/admin

Products

- Access Management
- Users
- Groups
- Client Hub
- Client Profiles
- Connections
- LDAP
- OpenID Connect
- Registration Tokens
- Keys
- CA
- Alarms
- Records
- Quorums
- Admin Settings

Full Name	ilo-5ced8c317400	Created	04 Sep 2025, 13:17	Last Login	04 Sep 2025, 16:07
Email	ilo-5ced8c317400@local	Updated	04 Sep 2025, 16:07	Logins	16
Source	local	ID	local fc...2542c672	Last Failed Login	N/A
				Expires At	

[Expand All](#)

GENERAL INFO +

GROUP MEMBERSHIPS -

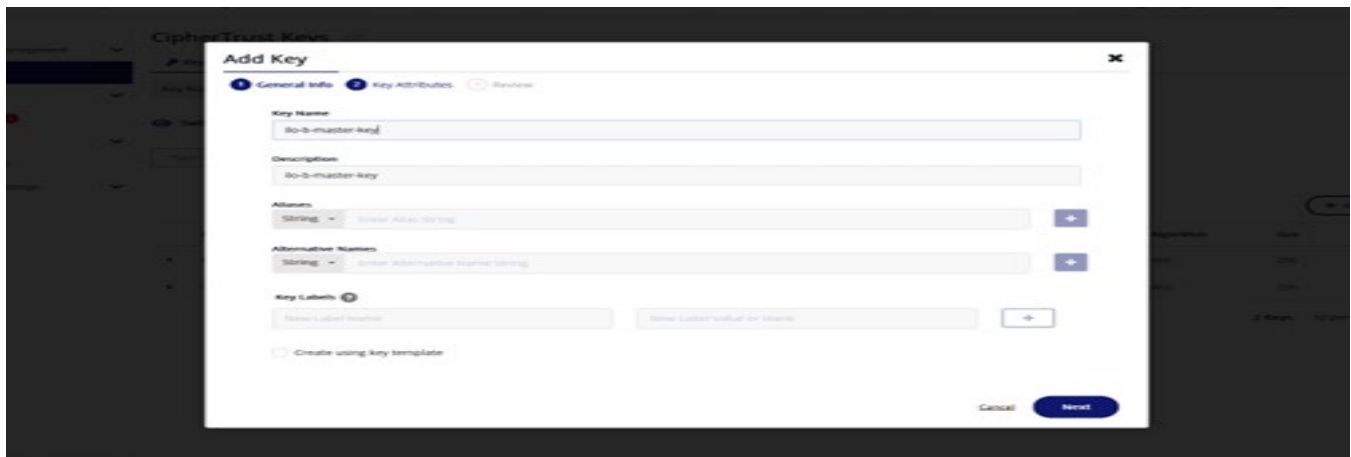
Search groups

3 Results | 3 Groups [+ Add Group](#)

Name	Description	
CA Admins		...
Key Users		...
User Admins		...

Configuration of Master Key

1. Add Master Key in ESKM



2. Configure Master Key as shown below and click Next

Add Key

1 General Info 2 **Key Attributes** 3 Review

Algorithm: AES Size: 256

Key Properties

- Generate KeyId for DSM Compatibility
- Versioned Key (NAE Property)
- Unique to Client (CTE Property)
- Deletable
- Exportable
- XTS/CBC CS1
- Set as Pre-active

Key Usage

- Sign
- Verify
- Encrypt
- Decrypt
- Generate MAC
- Verify MAC
- Wrap Key
- Unwrap Key
- FPE Encrypt
- FPE Decrypt
- Certificate Sign
- CRI Sign
- Translate Encrypt
- Translate Decrypt
- Translate Wrap
- Translate Unwrap
- Generate Cryptogram
- Validate Cryptogram
- Export Key
- Derive Key
- Content Commitment
- Key Agreement
- KMIP Mask Shorthand: 76

Back Next

Configure the Remote Key Manager Server

Administration - Key Manager

User Administration Directory Groups Boot Order Licensing **Key Manager** Language Firmware Verification

Key Manager Configuration settings have been saved.

Key Manager Servers

Primary Key Server Address	[Redacted]
Primary Key Server Port	9000
Secondary Key Server Address	N/A
Secondary Key Server Port	N/A
Require Redundancy	Disabled

Key Manager Configuration

Account Name	[Redacted]
Account Group	ilo_qa_ind_grp
Key Manager Local CA Certificate Name	[Not set]

(Optional) Configure the Remote Key Manager server details using Redfish

Use PATCH method using below URI to configure ESKM

"https://<iLOIP>/redfish/v1/Managers/<index>/SecurityService/ESKM/"

Payload:

```
{  
  "PrimaryKeyServerAddress": "",  
  "PrimaryKeyServerPort": ,  
  "SecondaryKeyServerAddress": "",  
  "SecondaryKeyServerPort": ,
```

```
"KeyManagerConfig": {  
  "AccountGroup": "",  
  "ESKMLocalCACertificateName": "",  
  "LoginName": "",  
  "Password": ""  
}  
}
```

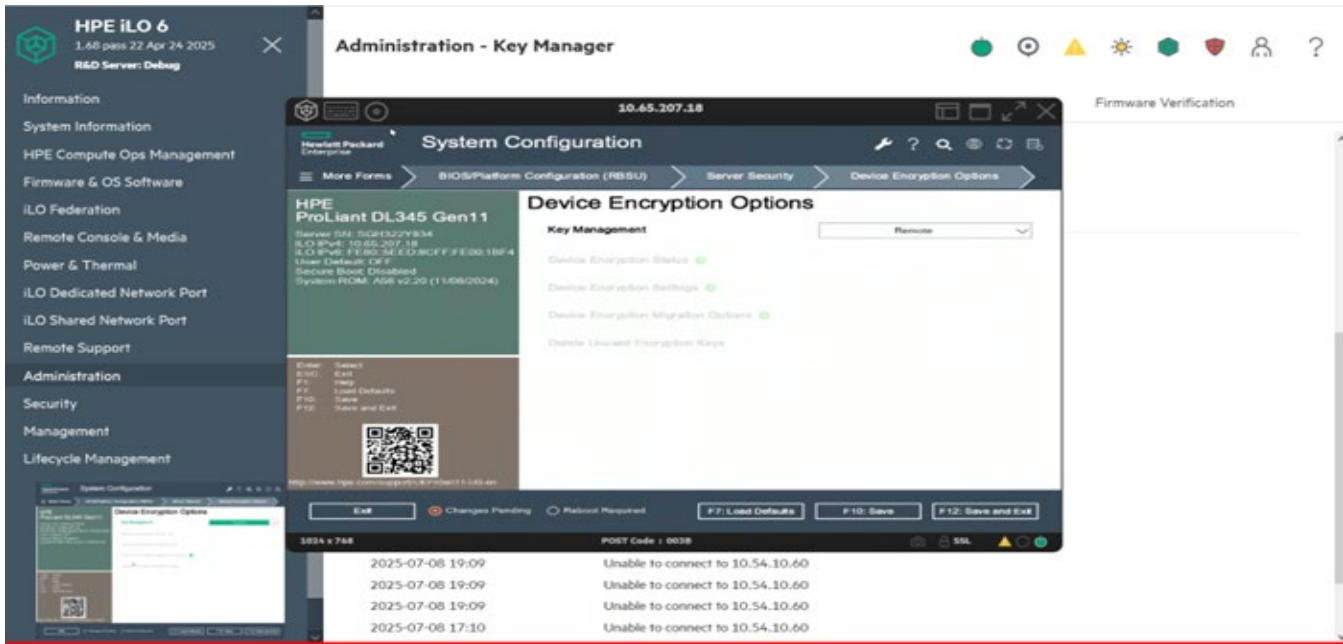
Perform GET operation on the below Redfish URI to see the Key manager config details

<https://<iLO IP>/redfish/v1/Managers/<index>/SecurityService/ESKM/>

1. Navigate to RBSU -> System Utilities -> System Configuration -> BIOS/Platform Configuration (RBSU) – Server Security ->Device Encryption Options



2. Change Key Management option to Remote



3. Click F10 to navigate to Intelligent Provisioning.
4. Launch the Smart Storage Administrator and enable Controller Encryption

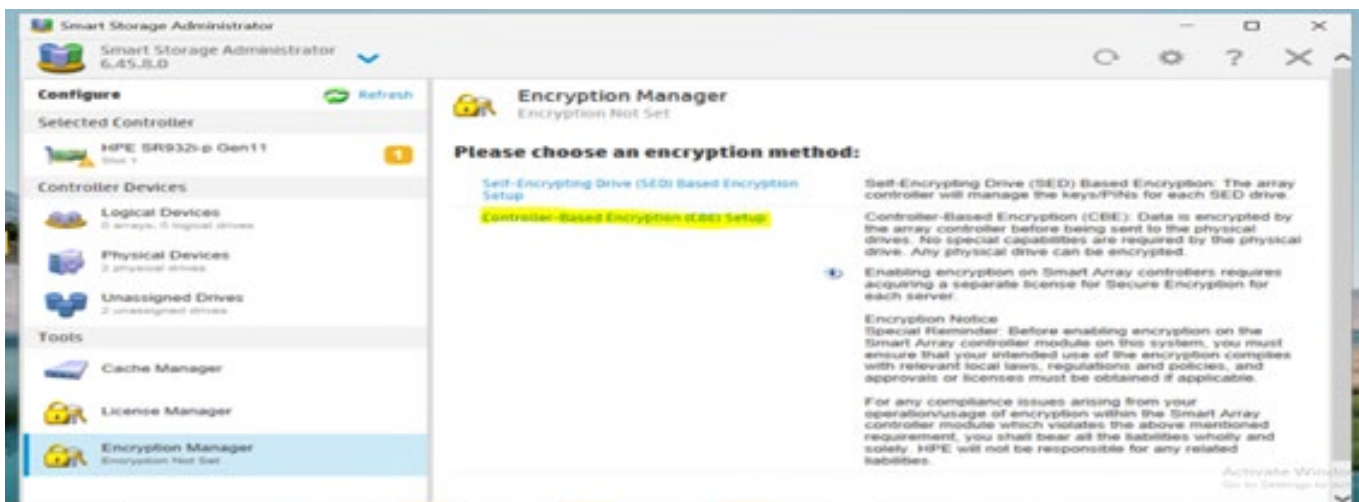
Note:

- If the boot devices do not need to be encrypted, then skip to step 10
- From BIOS: This option is needed if boot devices are RAID logical drives and those logical drives need to be encrypted.
- Create a logical drive and install OS on logical drive. This logical drive can be encrypted from OS



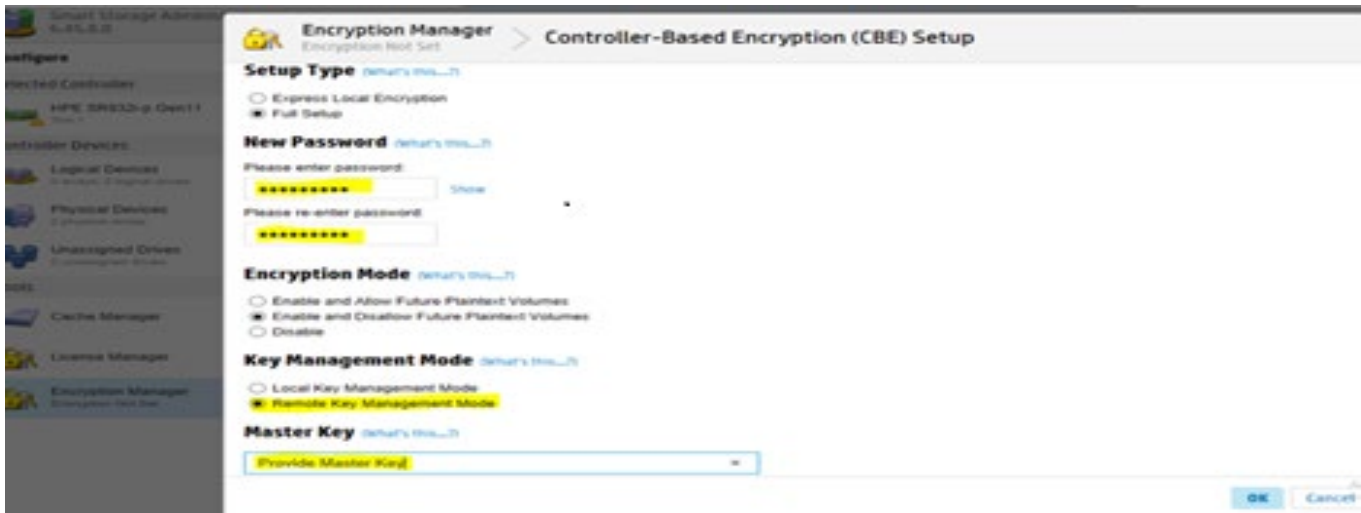


- From OS after installing Smart Storage Administrator (SSA) utility, select configure->Choose encryption method as "Controller based encryption."

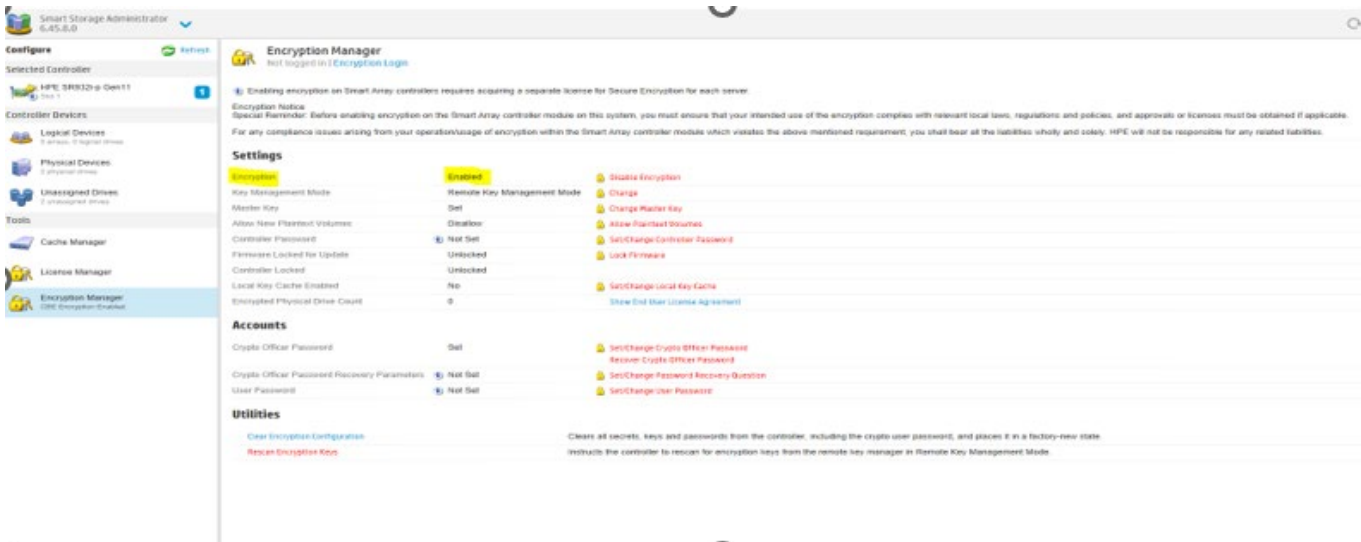


Note:

Provide the Password and the Master Key which is configured in Step 3 in Controller Based encryption setup page. Reboot the server after accepting the license and finishing the setup



6. After rebooting verify the Encryption state.

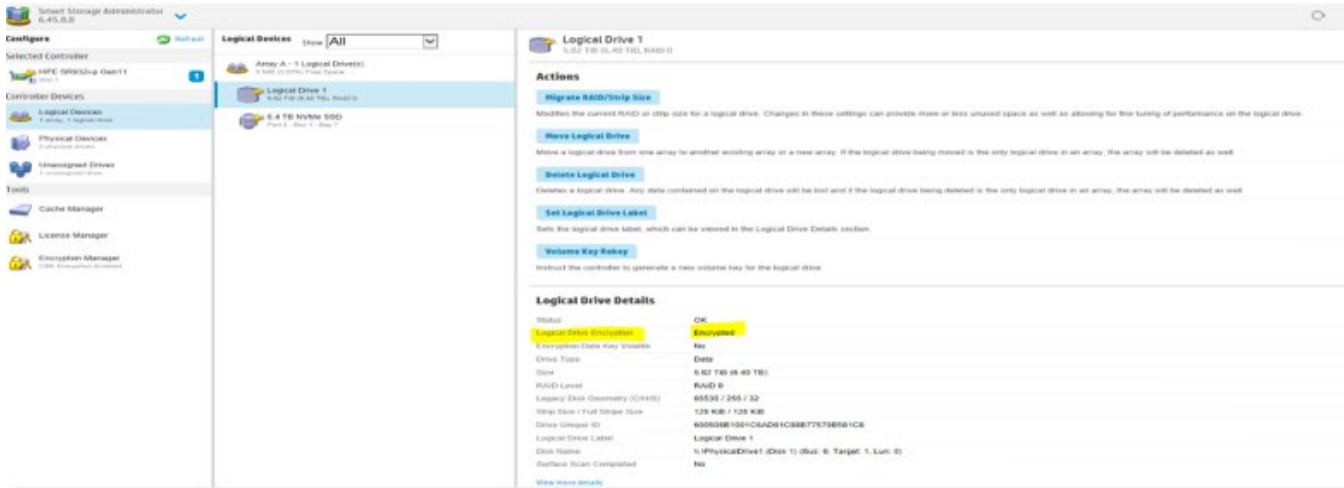


7. Click the Unassigned Drives in the navigation tree.

8. Select the desired drive(s) and create a logical array.



9. Click Logical Devices and verify that the created logical drive is encrypted.



10. Verify Key Manager Events in iLO GUI



11. (Optional) Verify Key Manager Events using Redfish:

Perform GET operation on the below Redfish URI to see the Key manager events

<https://<iLO IP>/redfish/v1/Managers/<index>/SecurityService/ESKM/>

Example Response

```

"KeyManagerConfig": {
  "AccountGroup": "ilo_sec_qa_grp",
  "AccountName": "ilo-5ced8c36076c",
  "ESKMLocalCACertificateName": "",
  "ImportedCertificateIssuer": "",
  "ImportedCertificateSubject": "",
  "RemotePassword": null
},
"KeyServerRedundancyReq": false,
"PrimaryKeyServerAddress": "10.10.10.10",
"PrimaryKeyServerPort": 9000,
"SecondaryKeyServerAddress": null,
"SecondaryKeyServerPort": null

```

12. Verify Logical drive Encryption status from the Storage page in iLO GUI.

System Information - Storage Information

Summary Processors Memory Network Device Inventory **Storage**

Storage Summary

Entity	Count	Health Summary
Storage Controllers	1	OK
Volumes	2	OK
Storage Enclosures	2	OK
Drives	3	OK

Volumes

Name	Status	Capacity	RAID Type	Drives	Spares
Logical Drive 1	Enabled	6.4 TB	RAID0	1	0
SR Volume 177	Enabled	6.4 TB	None	1	0

Logical Drive 1

Drives

Logical Drive 1 Details

@Redfish.WritableProperties	DisplayName,IOPerfModeEnab
Id	1
Name	Logical Drive 1
Status-Health	OK
Status-State	Enabled
Status-Conditions	
Identifiers.DurableName	600508B1001C6AD81C88B7
Identifiers.DurableNameFormat	NAA
Encryption	True
EncryptionTypes	ControllerAssisted
CapacityBytes	6401219190784
BlockSizeBytes	512
OptimumIOSizeBytes	131072
StripSizeBytes	131072
DisplayName	Logical Drive 1
DisplayName@Redfish.AllowablePattern	"[#53&()*+,-./w;@{}~@{}]"
IOPerfModeEnabled	True
ReadCachePolicy	Off

13. (Optional) Verify Logical drive Encryption status using Redfish:

Perform GET operation on the below Redfish URI to see the drive encryption status

<https://<iLO IP>/redfish/v1/Systems/<index>/Storage/<controller ID>/Volumes/<index>>

Example Response:

```

"Conditions": [],
},
"Identifiers": [
  {
    "DurableName": "600508B1001C6AD81C88B77570B581C8",
    "DurableNameFormat": "NAA"
  }
],
"Encrypted": true,
"EncryptionTypes": [
  "ControllerAssisted"
],

```

Configuring HPE iLO 6 Remote Key Management Server Using Utimaco

System Summary

Product:	Enterprise Secure Key Manager L1
Unit ID:	
Hardware Platform:	KVM Virtual Platform
Software Version:	8.53.0 (VESKM 8.53)
Date:	06/06/2025
Time:	12:06:23
Time Zone:	India Time
System Uptime:	16 days, 23:05:32
Licenses:	0
Licenses in Use:	

Procedure

1. [Configuration of user and Group for Utimaco](#)
2. [Master Key Configuration](#)
3. [Configure the Remote Key Manager Server](#)
4. [Create Logical drives and verify for encrypted state](#)

Configuration of user and Group for Utimaco

Create a group and add iLO-Mac user to the respective group. For iLO users, license type is "Server" and the users which are configured whose license type should be KMS.

Username	KMP-Enabled	User Administration Permission	Change Password Permission	License Type	Last Access Time
das	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	KMS	2025-04-28 20:27:12
ilo-Sced9c001b64	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Server	2025-04-03 21:15:46
ilo-Sced9c001b64	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Server	2025-04-28 20:27:12
ilo-Sced9c001b64	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Server	2025-04-28 15:15:17
ilo-b47af1a7b192	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Server	2025-04-28 16:17:49
raiesh	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	KMS	2025-04-10 03:30:42

Master Key Configuration

Key Properties

Key Name:

Key Type:

Owner Username:

Algorithm:

Creation Date: 2025-03-14 15:40:24

Versioned Key Bytes:

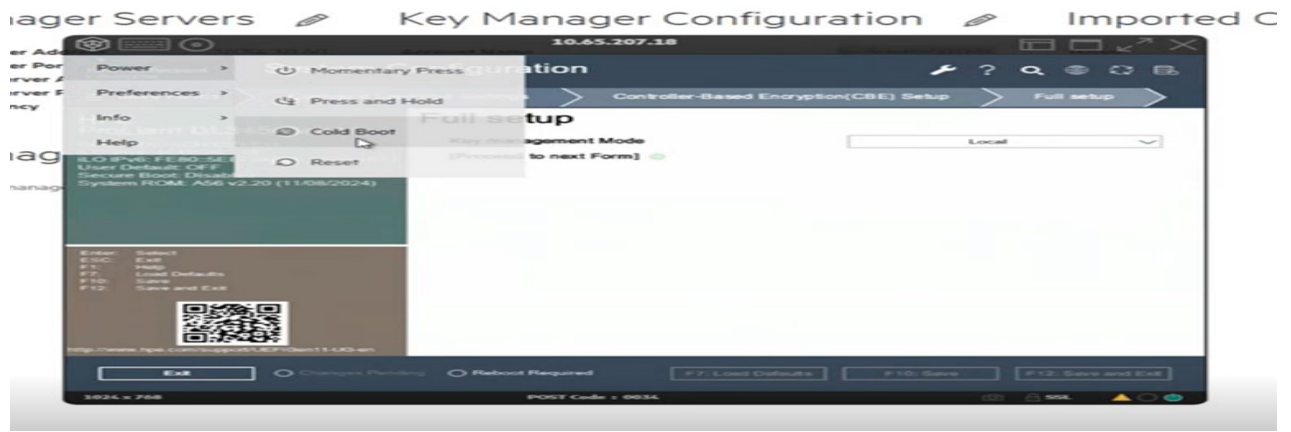
Deletable:

Exportable:

FIPS Security Level: 1

Configure the Remote Key Manager Server

1. Perform cold boot from RBSU for changes to take effect.



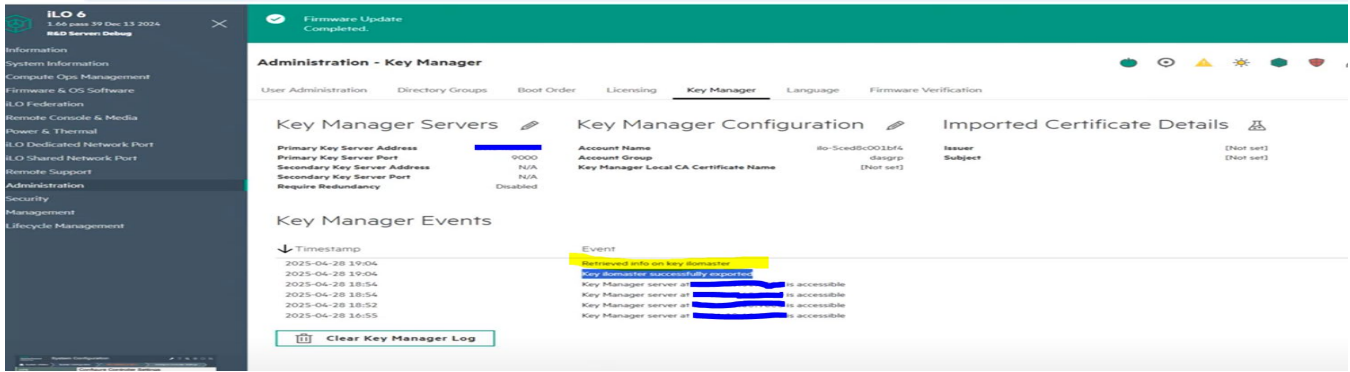
2. Click Remote option from RBSU



3. Configure and provide master key.

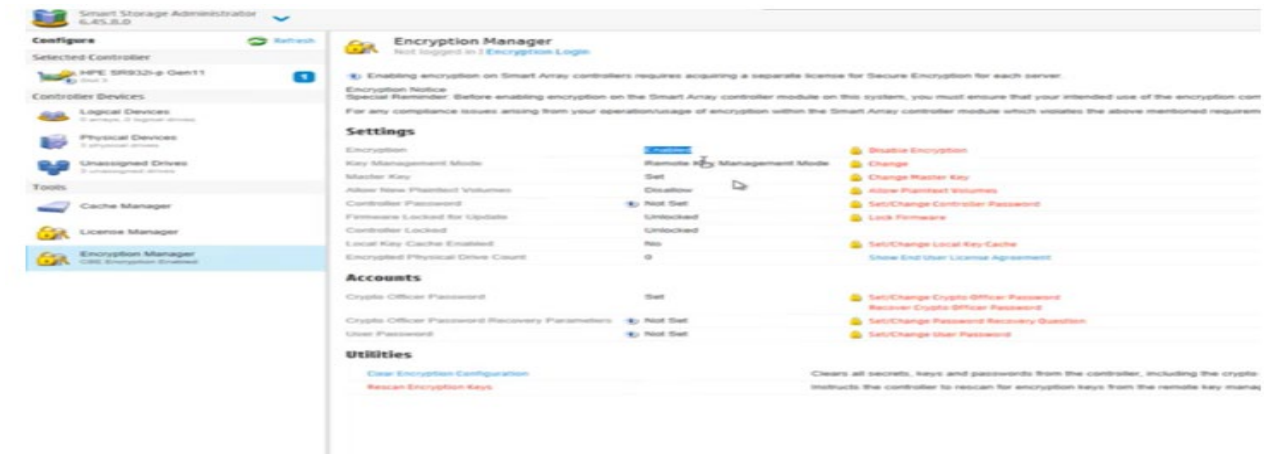


4. Check for Key Manager Events for configured Master Key in Key manager configuration

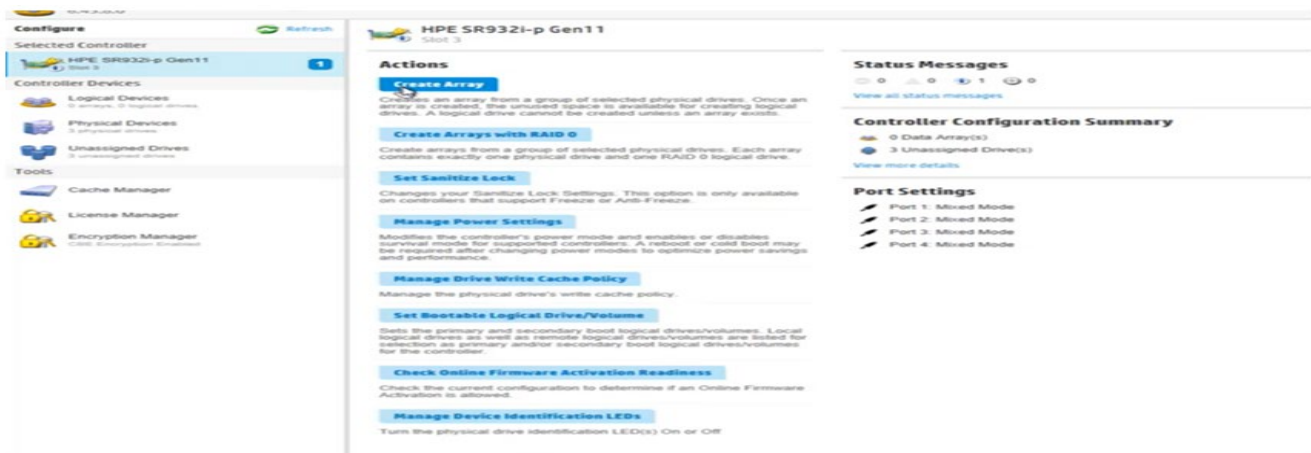


Create Logical drives and verify for encrypted state

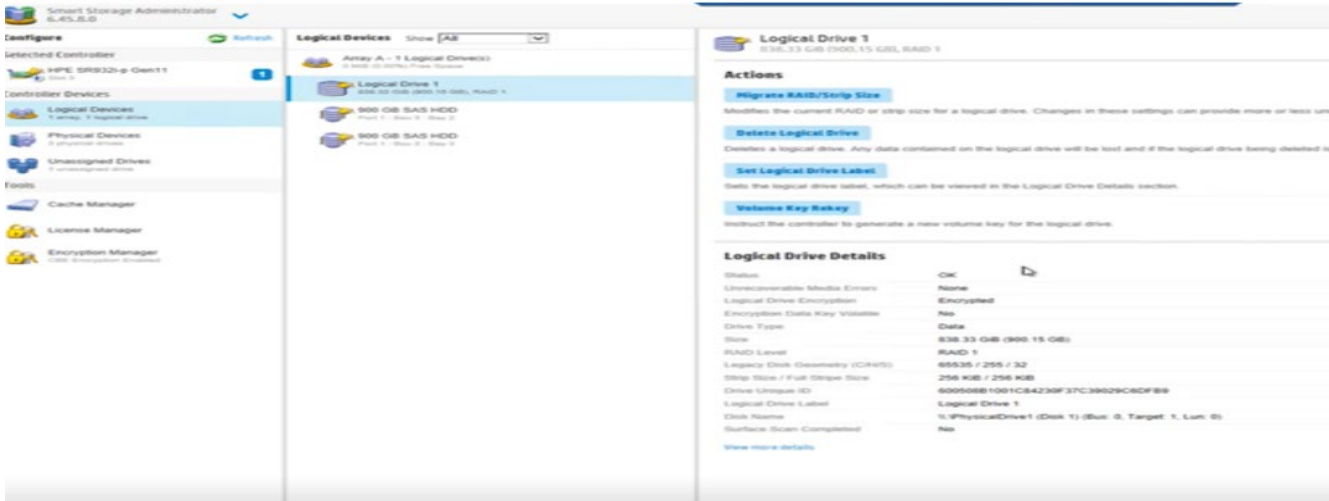
1. Reboot system and check encryption status



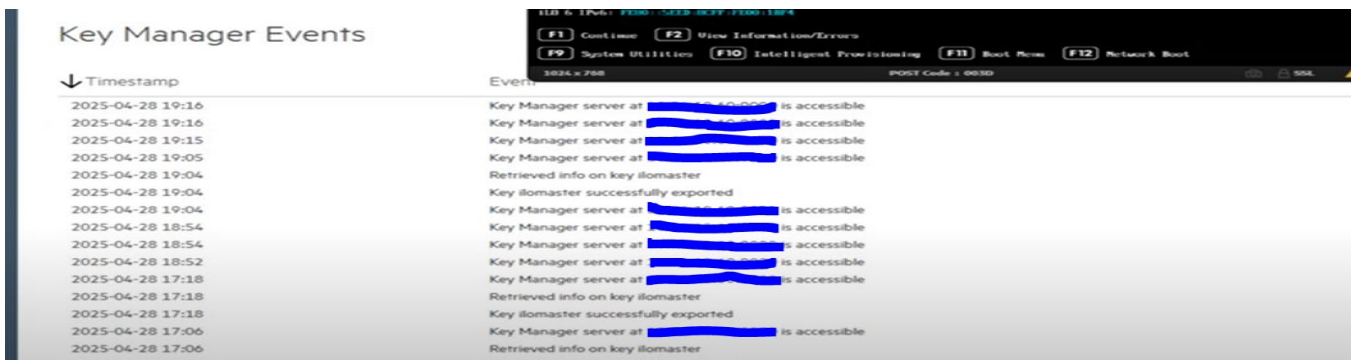
2. Create logical Drives



3. Check whether logical devices are displayed as encrypted.



4. Perform Cold boot of host and check keymgr events



HPE iLO 7 Remote Key Management Server for Drive Encryption and Decryption

Procedure for Drive Encryption

1. Configure the Remote Key Manager using iLO 7 GUI



2. Navigate to RBSU -> Device Encryption Status and verify no drives are encrypted



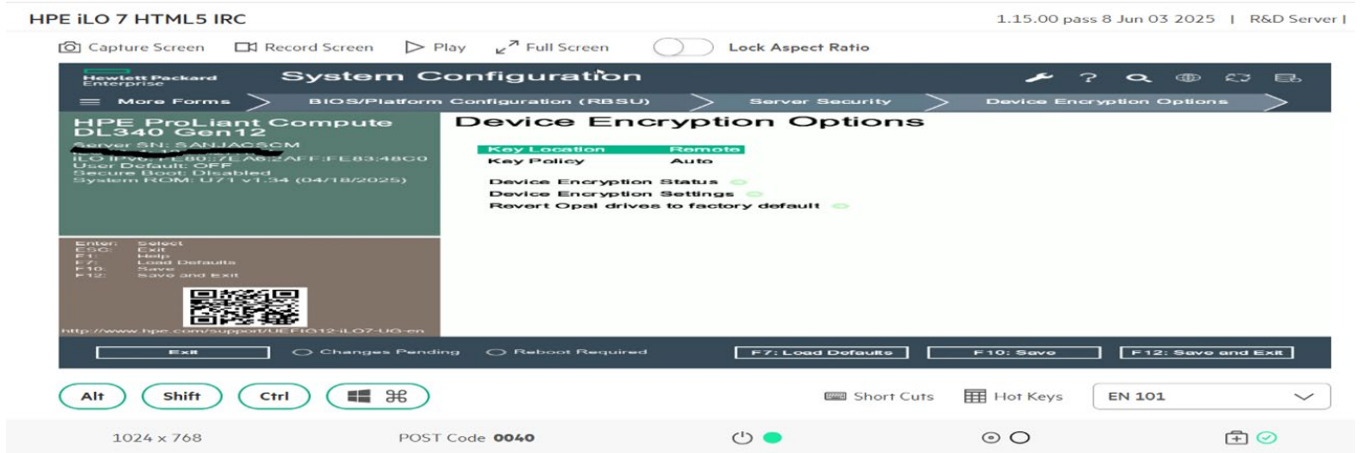
- (Optional) Configure the Remote Key Manager using in Redfish:
Apply patch operation to set keylocation to Remote

PATCH:- /redfish/v1/Managers/1/SecurityService

```
{
  "KeyLocation": "Remote",
}
```

Verify keylocation is updated to Remote using redfish GET URI
GET : /redfish/v1/Managers/1/SecurityService

- Navigate to RBSU → Server Security → Device Encryption Options → Unencrypted Device,
- Select drive and enable encryption operation



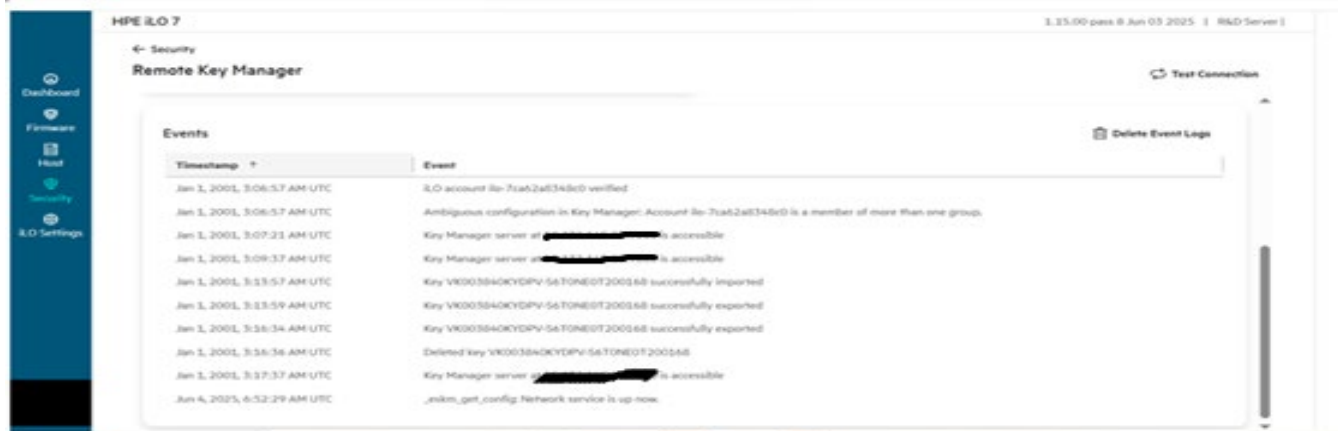


Procedure for Drive Decryption

1. Go to Encrypted Devices. Select the device and disable encryption option and start operation



2. Verify keymgr events after encryption and decryption operation. After encryption, imported events will be logged. After decryption export event will be logged as shown below:



Similar verification can be checked from IML logs also.

HPE iLO 7 1.15.00 pass 8 Jun 03 2025 | R&D Server |

← iLO Settings / Troubleshoot

Integrated Management Log

Search Actions ▾

8 Items								
	ID ↓	Severity	Class	Description	Last Update	Count	Category	
<input type="checkbox"/>	8	i Informational	UEFI	Encryption for Self Encrypted Drive (SED) at location : [NVMe drive Box 1 Bay 7] is disabled.	Jan 1, 2001, 3:16:36 AM UTC	1	Firmware, Maintenance	
<input type="checkbox"/>	7	i Informational	UEFI	Encryption for Self Encrypted Drive (SED) at location : [NVMe drive Box 1 Bay 7] is enabled.	Jan 1, 2001, 3:14:01 AM UTC	1	Firmware, Maintenance	
<input type="checkbox"/>	6	▲ Caution	UEFI	PCIe Slot 15 failed to train at Gen 4 speed and x16 width.	Jun 4, 2025, 9:36:03 AM UTC	1	Hardware, Configuration	
<input type="checkbox"/>	5	▲ Caution	UEFI	UEFI Non-Volatile Variable Store Corruption Detected. If enabled, Secure Boot security settings may be lost.	Jun 4, 2025, 9:35:37 AM UTC	1	Firmware	

Visit HPE.com

[Chat now](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Intel is a trademark of Intel Corporation or its subsidiaries in the U.S. and/or other countries. All third-party marks are property of their respective owners.

a00154574enw

HEWLETT PACKARD ENTERPRISE

hpe.com

